



Department
for Education

Data protection: a toolkit for schools

Open Beta: Version 1.0

August 2018



Contents

Summary	3
About this guidance: status and version control	3
Reference materials used within this document	4
Foreword by Neil McIvor, Chief Data Officer, DfE	5
Structure and purpose of the toolkit	6
Step 1: Raising awareness	8
Step 2: Creating a high level data map	12
Step 3: Turn your data map into a data asset register	15
Step 4: Documenting the reasons for processing data	19
Step 5: Documenting how long you need to retain information	28
Step 6: Reassurance and risks	34
Step 7: Decide on your Data Protection Officer role	42
Step 8: Communicate with data subjects	45
Step 9: Operationalise Data Protection, and keep it living	48
Annex	52
Annex 1.1 Explaining the language around data protection	52
Annex 2.1 Table for identifying personal information to support the initial data map	57
Annex 3.1 ICT Policy Agreement - Example	58
Annex 3.2 Example letter to parent/carer for record checking and consent	62
Annex 4.1 The possible lawful basis and conditions of processing for personal data	64
Annex 5.1 An Emerging Data Retention Strategy for the sector	66
Annex 6.1 Example Data Protection Impact Assessment template	77
Annex 7.1 GDPR, Schools and Contracts – Guidance Notes	79
Annex 7.2 Generic National Schools and Colleges Contract Template	83
Annex 8.1 Data Protection Advisory Visit Report	85
Annex 9.1 School Data Breach – Case Study	93
Annex 10.1 Safeguarding Myth-Busting	96
Annex 11.1 Agreement to vary the National Contracts	97
Annex 12.1 Lead Contributors	100

Summary

About this guidance: status and version control

Version: Open Beta, Version 1.0: date of release: 30 August 2018

This document has been released as an open beta version. This means that while we are confident the document adds value in achieving its aims of supporting schools to better manage data protection and to implement the new elements of data protection associated with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018; we will maintain it as a 'living document' which can be updated continually to accommodate relevant changes.

As an open beta, this document should be:

- tested continually by schools for readability and ease of use
- viewed and reviewed by a wide range of stakeholders who are interested in ensuring that schools deal with data protection robustly and efficiently

Feedback obtained during those processes will help iterate and improve the toolkit.

Alongside the publication of the first beta version of this document, we ran an informal consultation exercise from April 23 until 1 June 2018. The feedback gathered during this period has been used to inform most updates and improvements in this revised version. This is a 'living document' therefore; we anticipate there will be further opportunities for improvement in future.

This document is long because it includes a number of case studies and annexes that the schools that have contributed to the toolkit have found useful. It is intended that schools may choose to read the bits most relevant to their own level of maturity in managing data protection.

If you wish to comment on the content of this document then please provide feedback to data.modernisation@education.gov.uk with the subject heading "GDPR toolkit feedback". If your comments refer to specific content in the document, please reference the page number(s) to identify the area to which you are referring. We may not be able to provide individual responses to feedback; but all feedback will be read, considered, and used to inform future updates where appropriate.

Reference materials used within this document

In order to help schools to access supporting materials efficiently, a number of links are provided to materials created by public and commercial bodies, and case studies are provided from a range of volunteer organisations.

Any links to materials produced by commercial organisations are only done so after satisfying the following criteria:

- The material is assessed as being informative and correct.
- The material is assessed as adding value by a panel of school leaders working on data management.
- The commercial organisation that produces it may be referenced within the material, but the material must be free from any sales material or promotional material related to services offered.
- Access to the resource must be freely given without the need to register or provide contact details.

By referencing any open source external material, the Department for Education (DfE) is in no way endorsing or recommending any additional services or solutions provided by third party organisations. Schools are of course free to undertake their own searches for open-source material that can help them to fulfil their statutory duties.

As well as those organisations providing information links, a number of other organisations helped us in developing the content of this initial toolkit. The key people and organisations involved are outlined in **Annex 12.1**.

If, as an organisation, you have material that you feel would support schools in managing data protection, **and satisfies the above criteria**, please provide details to the consultation email address (data.modernisation@education.gov.uk), with a view to it being considered for inclusion in subsequent versions of this document.

Foreword by Neil McIvor, Chief Data Officer, DfE

Data plays a key role in our modern education system by providing opportunities to monitor effectively the progress of learners, enabling robust evaluation of methods, promoting evidence-based practice, and providing opportunities for huge efficiency improvements in school operations.

The use of data across our sector and beyond has developed significantly in recent years. It is therefore right that the law, processes and capabilities required for effective **custodianship** of children's data were updated to meet the growing demands imposed by modern data protection challenges.

The new data protection legislation that **came into effect in May 2018 provides both challenges and opportunities**. Understanding, aligning and complying with the new law is a challenge for all organisations, big or small. It does, however, provide an opportunity to refresh our policies and procedures relating to the safe stewardship of data. The new legislation is generating momentum around auditing where organisations are, identifying risks, and developing coherent plans to manage them down. It also places a firm emphasis on citizens being informed on the use of data and their associated rights. If our sector is to be entrusted to hold sensitive data about children across the country and exploit the benefits modern data technologies enable us, **then the new challenges** are to be welcomed.

In aiming to support schools with the changes, it is clear that there is no one voice or lens in our sector who could have written an excellent guidance document in isolation. That is why I am delighted to see the high degree of collaboration among schools, local authorities (LAs), multi-academy trusts (MATs), and the supplier community who have helped develop this working document.

We would really value your comments and feedback going forward so that we can continue to work with users to iterate and improve it.

Yours,

A handwritten signature in black ink, appearing to read 'ND McI', followed by a long, horizontal, slightly wavy line.

Neil McIvor, Chief Data Officer, Department for Education

Structure and purpose of the toolkit

Much of the best practice associated with the General Data Protection Regulation (GDPR) and Data Protection Act 2018 is based on the Data Protection Act 1998. That said, GDPR and the Data Protection Act 2018 introduce new elements and provide an opportunity for organisations to review their current data protection and privacy practices.

Schools will be at different stages in preparation for legislative change on data protection. The use of data and related technologies varies significantly across our schools, and this toolkit is intended to support schools in developing the policies and processes that are right for them. It has been developed by the Department for Education (DfE) working in collaboration with schools, multi-academy trusts (MATs), local authorities (LAs), system suppliers, GDPR support providers, the National Cyber Security Centre and the Information Commissioners Office (ICO).

The document provides 9 steps that, we think, can help schools efficiently develop the culture, processes and documentation required to be compliant with the strengthened legislation and effectively manage the risks associated with data management.

The 9 steps outline a suggested sequence of activities that will enable schools to identify and monitor the use of personal data, undertake the necessary processes for auditing and assessing risk, and assist with compiling policies to ensure schools can sustain compliance. Each step is structured to provide the intended outcomes of each step, a suggested 'how to' approach, top tips, case studies, and links to the most relevant resources for that step that have been identified to date.

It is important to note that **this document provides tips and guidance only**. It is intended to support schools draw out areas of risk. Where the term 'school' is used, multi-academy trust could equally apply where relevant, as the legal entity with the responsibility for data protection for their schools. **It does not constitute formal legal guidance, and as a data controller in its own right, a school is ultimately responsible for its own data protection procedures and compliance with legislation.**

Schools (and/or MATs) are data controllers in their own right and therefore should ensure they have appropriate registration with the ICO. For more information about registering with the ICO, please visit [their website](#).

Some education providers who are required to send data to the department have regarded the department as their data processor. This is not the case. In relation to data collected by the department from education providers, the department is usually **a data controller in common** (as defined under GDPR and data protection legislation) with the education providers, which means that **we each have responsibility for the data we process for our own purposes.**

The information processed by education providers remains their responsibility regardless of the IT systems the data is processed/held on until the point at which the data is transferred to the department.

Step 1: Raising awareness

Intended outcomes:

1. Raise awareness across **all** staff within the school who come into contact with personal data (noting that personal data can relate to pupils, staff, parents and potentially others). Making the link between data protection and child protection can be an effective way to 'make it real' for staff, although data protection is much broader than that.
2. Ensure that a broad range of staff across the school community are engaged with the work, to articulate and demonstrate the totality of personal data that is processed (as defined by DPA 2018) by the school, and to be engaged in the risk management. This includes an awareness that risks to personal data security can come from online threats like a cyber-attack.
3. Governors and trustees **are aware that responsibility for compliance with data protection legislation lies with them** and that they are kept informed about all key issues arising for the schools from the legislative changes and understand how to effectively monitor and review compliance working closely with the appointed DPO.
4. The language associated with data protection, and the enhanced legislation, is demystified.

How to approach this step:

Within a school, there are all sorts of job roles that utilise personal data for a variety of reasons. Some staff will be responsible for ensuring they simply use it responsibly, others will be making significant decisions about what data is used, how it is processed and stored and who it is shared with and how. As such, it is likely that a 'one size fits all' approach to staff training will not work.

From talking with schools, we believe an effective approach is to think about **3 levels of raising awareness:**

1. **All staff** should be aware of what personal data actually is, what 'processing' means in the broadest form, and what their duties in handling personal information are. They should be aware of the processes by which they are permitted to use that information, and be **clear of the scope of the permitted usage of that data**. They should be engaged with the **risks around data getting into the wrong hands**, and their responsibilities regarding responding to a **data breach**. The job roles that might warrant this level of training include catering staff, welfare supervisors, library staff, cleaners, first aiders etc.
2. **Those who can influence how data is used, processed and secured**. By this, we mean any staff in school who may have the authority to create and store data,

enter data into applications/software or decide if/when they will process certain data. They may also have responsibilities for how paper documents are handled within the school environment. This likely covers all teaching staff as a minimum.

As well as the awareness work, they should have the chance to **review the high-level data maps** suggested in [step 2](#), and be given an opportunity to contribute the different perspectives that they offer compared with senior leaders or data leads. They should also be engaged with things like **ensuring there is a legitimate lawful basis and, if relevant, a condition for processing** the information they utilise, and that **storage of data is minimised** to that required to perform the necessary tasks. They should be engaged in **discussions about identification and mitigation of risks**, and know the governance arrangements that oversees the management of risks. In addition, as more schools process and store personal data by electronic means, schools will want to produce user-friendly security policies and staff training to help reduce the risk of a data breach. The job roles that warrant this level of training may include, but are not limited to, higher level teaching assistants, teaching staff, office staff, site administrators, information and communications technology (ICT) staff and technical support staff. Everyone can help prevent data loss by following basic cyber security steps.

3. **Senior leaders and executive level, and those who manage the ‘data ecosystem’.** By this, we mean those in school who are responsible and accountable for making choices around the use of technology and its security, deciding on what and how the data is shared, and setting school policies around the use of data and technology. As well as the senior leadership team (SLT), it may well be network managers or business managers. These people need to be **sufficiently aware of the content of GDPR and the Data Protection Act, so that they can assure governors that the school has the right things in place to be compliant.** As a data controller the school has a responsibility to ensure that there is accountability, and transparency throughout the whole data ecosystem and that the principles of data minimisation and privacy by design are adhered to by all parties, and that any contracts with data processors cover the relevant areas of data protection. This level of training is aimed at those who are accountable for those responsibilities on a day-to-day basis.

Job roles warranting this level of training include, but may not be limited to, all SLT members, curriculum leads, business managers, ICT leads and data managers and MAT executive teams.

In addition to staff training, **awareness for governors and MAT trustees** should focus on the following areas:

- That the ultimate responsibility and accountability for compliance sits with governors and trustees. **Data Protection will, on an ongoing basis, require resourcing and**

governors/trustees will be an important support mechanism for the DPO in performing his or her role

- Making sure their school has good network security to keep the personal data they hold protected. This should also include having a business continuity plan in place that has cyber resilience as a consideration.
- That the new legislation moves schools from being required to 'comply' with data protection, to being required to 'demonstrate' compliance with legislation.
- To actively demonstrate compliance, schools need to document all their assets containing personal data and ensure they are being appropriately managed and secure.
- Appraising and scrutinising the performance of the school leadership/executive in the area of data protection
- Preparation requires a thorough 'audit' or 'housekeeping' exercise on current data processes that should already be in place in relation to the Data Protection Act. In particular, it is likely that data retention policies need more consideration.
- Following the data audit, an assessment of risks to data protection that will be considered by the school to be high or medium should be maintained. Schools should clearly identify what these risks are and how they are being addressed. This could include identifying any shortcomings in the school's network security infrastructure and keeping IT security policies up to date. This should be documented as evidence towards compliance.
- Schools need to review how they communicate their use of data with pupils/parents, and the rights of data subjects, with clear explanations regarding the strengthened rights (including Subject Access Requests (SARs)). Schools need to have agreed procedures for dealing with SARs.
- A need to appoint a Data Protection Officer who has the ear of governors (and vice versa) and is somewhat independent from but can work closely with the management structure that develops and maintains data policies. ([Step 7 has more information](#)).
- A review of data protection policies in light of any changes to procedures and processes arising from the data audit and risk management.
- Reviewing data protection is an ongoing process requiring the whole school to be continually mindful of their responsibilities. Formally scheduling an annual review of current practice through an internal or external audit may be something schools wish to consider.

Top tips:

- Link data protection to safeguarding children (and child protection) when trying to get people engaged. In this way, all staff see that data protection matters in the context of pupil welfare. However, the rights of individuals are also key and start people thinking about gaps in current practice.

- Once SLT have developed a high-level data map (as described in [step 2](#)), test and iterate it during training with staff. They will identify new things and it will help entrench a sense of ownership.

Case studies

- In training, it may be useful to use ‘real life’ case studies to explore how your school ensures that its personal data is safe. “School CCTV hacked” or “Children’s Services Data Breach” are 2 search terms that might find articles that provide food for thought and help make training/risk management feel real.

Relevant resources:

- [Annex 1.1](#) explains the key terms and language used to describe data protection and within this document.
- There are several posts on the [DfE teaching blog related to GDPR](#).
- An [introductory GDPR video](#) on the DfE YouTube Channel.
- This 2m 30 second [video by GDPR in Schools \(GDPRiS\)](#) can help to set the scene as part of training with staff. A [print out summary](#) is also available on their website.
- The [National Cyber Security Centre website has guidance](#) in this area and will publishing more advice covering the topics discussed above in the coming months.
- [Children and the GDPR](#) provides more detailed, practical guidance for UK organisations who are processing children’s personal data under the GDPR. Also, refer to [Step 4](#) on processing children’s personal data.
- [Annex 3.1](#) - From Oxford Diocesan Schools Trust: Example of an ICT Policy, setting out responsibilities and parameters for ICT (including data protection), to be signed by all staff in a school

Step 2: Creating a high level data map

Intended outcomes:

1. Build up an overview of all the places personal data are stored and used in the school (your school's "data ecosystem").
2. Create something that can be discussed and tested with staff to identify any gaps in the initial 'overview' and build confidence that everything is captured.
3. Create an overview that can be aligned to more detailed documentation about data assets.
4. Create a picture that helps communicate personal data use with pupils/parents, a requirement of the new legislation discussed in [step 8](#).

How to approach this step:

One approach many schools are taking is to begin with a session to complete these 3 columns of a table:

1. Data sent to the school from someone else (for example, a local authority admissions team).
2. Data created within the school.
3. Data passed on from the school to someone else (a subsequent school for a pupil, the local authority, DfE or a supplier).

Consider the types of personal data your school records and uses. The data can be categorised as follows:

- admissions
- core management information systems (MIS)
- any 'data integrator software' you may use to connect your MIS with other systems
- curriculum tools
- payment systems
- virtual learning environments
- catering management, including cashless catering
- safeguarding, potentially including CCTV
- trips and transport
- uniform, equipment and photographs
- identity management systems (potentially using biometrics/fingerprinting)
- contract/communication systems
- social care and health interactions (for example, school nurse visits)
- statutory returns
- references and education settings you pass children on to
- workforce systems – such as job applications, current staff and former employees
- paper records
- other systems

A simple way to capture this information is by creating a table with the data types forming the row headings and the data flow considerations forming the column headings. An example is provided in [Annex 2.1](#)

Once you think you have captured all the data sets in use within the table, convert the table into a visual map of the data systems, and how the data flows into and out of the school. A visual map is engaging and user friendly, and will be useful in subsequent steps.

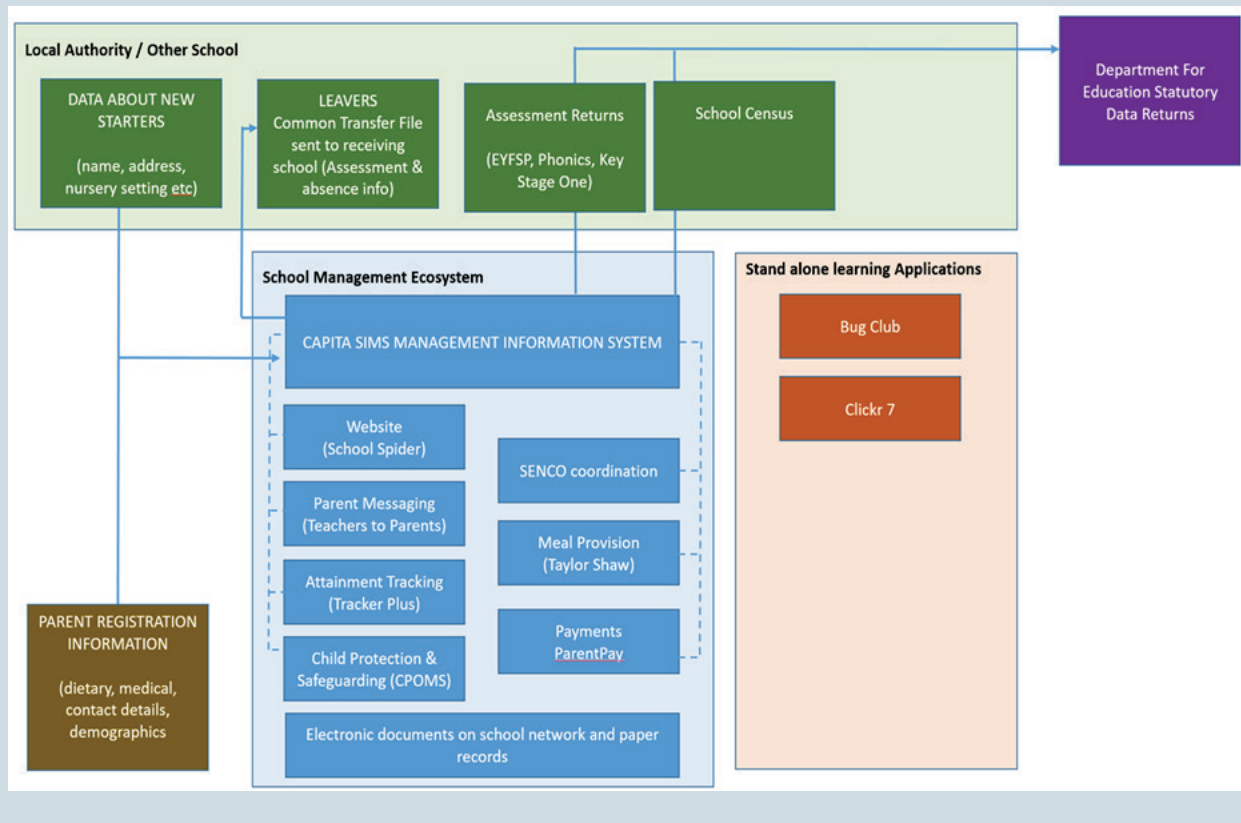
Top tips:

- Remember, the focus is **personal** data, which is information that identifies a living individual. Whilst you may want to do this for other data assets as well (for example, financial data assets) the priority is personal data in terms of responding to the new legislation.
- Invite a range of staff to document the data systems and stores associated with each data area. SLT or data managers might initiate the work, but it will be other teachers and school members who spot the gaps and will often have a more comprehensive understanding of paper records or use of learning applications that may not be on SLTs radar.
- Do you have 'middleware'/'data integrators' that extract data from your MIS to be used in other systems? Examples are Groupcall Xporter, Wonde, OvernetData, SalamanderSoft, Assembly/Ark UK group and Ruler. **If so, it is vitally important that you are aware of what information is being extracted from your MIS and how it is being used and/or shared with other systems.** If you don't know whether you use them or not, ask your MIS Provider. **It is critical that the school assesses how its liability may be affected by the actions of your third party suppliers and to mitigate risk it is important to exercise due diligence and ensure you have an up to date data processing agreement in place with them.**
- At this stage, it would be a good opportunity to take stock of the IT security policies that your staff currently follow both when you are sharing and storing personal data over networks.
- The data map you create is your 'as is' data map and will help you understand the range of personal data your school uses, how it is used and who it is shared with. **It does not mean that it is compliant with new legislation.** The work you will do in subsequent steps will build on this knowledge to pinpoint areas of weaknesses or potential issues with current practice that need to change.

Case study: Dobcroft Infant School, Sheffield: Pupil data

Dobcroft Infant School undertook a data mapping exercise at the outset of preparing for the new legislation.

Sharing it with teachers and staff proved extremely valuable in validating the map, identifying gaps, and being alive to issues with paper records.



Relevant resources:

- [Annex 2.1](#) includes an example of a table that can be used to support the work to capture all personal level data assets.
- This [video by GDPR in Schools \(GDPRiS\)](#) can be used to help set the scene and context of those setting out on the data mapping and data asset register work with a school. This is also available as a [mind map](#).

Step 3: Turn your data map into a data asset register

Intended outcomes:

1. Create the main framework around which schools can document the detail associated with each dataset.
2. Identify the areas of weakness/risk or gaps that will most likely begin the creation of a risk-management based approach to compliance.

How to approach this step:



- A data asset is a 'thing' that contains data. It could be a database, a system, a spreadsheet, or a set of paper records. It is worth taking time getting the level of detail right here. If you think of your school as a library, then data assets are the books. They are not the most detailed level of data you hold (that would be the words, sentences and chapters in those books), but rather they are distinct portions of your data estate that can be thought of as 'one asset'.
- The creation of data map is a useful starting point, but you need to start building up a rich picture of understanding your data assets. You need to create a data asset register.
- In simple terms, a data asset register is a long list of all the different data assets you have in your school, with some supplementary information about each of them. Different organisations will go down to different levels of detail here depending on their complexity and maturity. As a minimum, doing this for all assets that hold personal level data is required.

Your data map will contain a pictorial representation of your data assets. We recommend that at this stage:

1. You give each 'data asset' on your data map a reference number.
2. You create a row in a spreadsheet for each data asset you assigned a reference number.
3. You create the following column headings:

Theme	Column heading
Source	<ul style="list-style-type: none"> Source of data
Contents	<ul style="list-style-type: none"> Does it contain Personal Level Data (Y/N)? Does it contain GDPR Special Category Data (Y/N)? Other data considered sensitive in education (Y/N)?
Processing and role of the school	<ul style="list-style-type: none"> Is the school a data controller or data processor? If a controller, are there any joint controller relationships? What processing is done with the data – what is this data asset used for in school? What is the lawful basis (personal data) and condition for processing (special categories) that apply to that processing?
Controlling access and use	<ul style="list-style-type: none"> Is there any onward sharing? To whom? Is there an up to date data sharing agreement in place? Who has access to this data asset in school, and how do we control that to ensure only those with permission can see/use it? When using IT networks, is it possible to limit the number of users, grant the least amount of privilege required, and monitor their activity?
Data retention and destruction	<ul style="list-style-type: none"> What is the data retention period(s) for the different data in the data asset, and what is the justification for it? Is the capability to manage retention (that is, to delete records or anonymise them after X years) built into software? If no, what operational process is in place to ensure the intended retention period is implemented properly?
Communicating with data subjects and their rights	<ul style="list-style-type: none"> Do you rely on seeking active informed consent, and if so how is this managed? How are data subjects informed of their rights regarding access? How are data subjects informed of their rights regarding rectification of data? How are data subjects informed of their rights regarding erasure of data? How are data subjects informed of their rights regarding restricting certain types of data processing? How are data subjects informed of their rights regarding objecting to certain types of data processing? Is the process for Subject Access Requests, including getting data in a structured format known?

Theme	Column heading
Security and Breach	<ul style="list-style-type: none"> • What security measures are in place for inappropriate access or loss of a data asset? • Are data security policies in place and well understood by staff? • Has the school put in place up-to-date ICT security policies to prevent or deter personal data loss for incidents such as a cyber-attack, and do you review it within a defined period? • As part of your IT security policy, do you follow processes to secure the transfer of data between users and controllers? • Is there a process in place for handling a breach of a data asset including reporting it to the relevant authorities?
Automated Profiling	<ul style="list-style-type: none"> • Does the processing of the data involve any automated decision making, including profiling?
Offshore storage	<ul style="list-style-type: none"> • Is the data stored offshore? If so, where?

Top tips:

- Some of this information (where data is stored, the security measures and confirmation that there is no onward sharing) may be required via conversations with your suppliers. DfE has published [an open letter to encourage suppliers to support you with this task](#). Feel free to quote it to your supplier if you are experiencing resistance.
- Ensure that your 'data map', created in [step 2](#), and the data asset register remain in sync at all times. Use versioning control to ensure that they do, that way your data map can continue to be the easy way of visualising your data estate, and the data asset register can be the more detailed management tool, but you can use both with confidence so long as they are aligned.
- Spending a bit of time structuring your data asset register based on logical areas (for example, learning platforms, payment systems) will pay dividends in the long run in terms of 'staying organised' as you build things up, as you change systems over time and will help when putting together a risk register to assess the cyber security readiness of your school. Another benefit is that an inventory of all your systems, and network enabled electronic devices, can help improve your data security further down the line. For example, once you have identified all your systems and devices you can set up policies to keep them properly maintained by regularly updating and patching with the latest security updates.

- Depending on the size of your school, it may be important to develop a classification for your numbering. For example, A = Admissions data, B = Catering systems, C = Communication systems, and then you can develop your list with some structure:

A. Admissions Data:

A.001 – Admissions File from LA

A.002 – Admissions data from Feeder Schools

B. Catering Systems:

B.001 – Pupil ordering system

B.002 – Payment System

B.003 – Identification System

C. Communication Systems:

C.001 – Text messaging system to parents

C.002 – Email distribution list of alumni / ex pupils

Relevant resources:

- DfE has published [an open letter to encourage suppliers to support you](#) with this task. Feel free to quote it if you feel you need greater input from suppliers to help you complete your asset register in relation to system security, onward data sharing and any offshoring of data in particular.
- The [EduGeek website](#) is a popular place for data managers and technical colleagues grappling with data protection issues to collaborate and discuss issues associated with information management and data handling.
- The National Cyber Security Centre has [published guidance](#) that can help prevent personal data loss due to a cyber-attack. The principles contained in this [guide](#) can also help improve your school's cyber resilience from online threats.

Step 4: Documenting the reasons for processing data

Intended outcomes:

1. Become familiar with the conditions and lawful basis for processing that are most relevant to the activity of schools.
2. Understand the extra reasoning that is required to process special categories of data, which are tightly defined in the new legislation.
3. Understand that lawful bases are specific to processing data – that is, the purpose you are using it for.
4. Identify the areas that do not appear to be essential to undertake the task of safely and efficiently running a school, as these are the areas that specific consent from data subjects may need to be sought if not already obtained.

How to approach this step:

- Before setting out the lawful reasons for processing data, it is important to classify the data in the asset as items with differing sensitivity require different processing conditions.
- Remember that personal data is all the data that relates to an identified or identifiable living individual. GDPR identifies 2 types of personal data:

Special Category Personal Data – Some items of information about people are highly sensitive. GDPR specifically defines them as data relating to:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade-union membership
- health or sex life

Data relating to criminal offences is also afforded similar special protection.

Personal data – All other data items related to an individual are merely termed ‘personal data’. These are data items such as an attendance mark, an email address, or an examination result.

Understanding legal definitions can be quite complicated, (they are set out in full in [Annex 4.1](#)), but in all probability, the use of pupil data in a school that does not need consent from data subjects falls into two or three main areas provided for in law (workforce data may also be reliant upon being “necessary for a contract”). Focussing on these, with help from the ‘top tips’ at the end of this section, should help you move through this step relatively quickly.

The first question to ask yourself is:

“Am I required by law to process this data?”

DfE data returns, such as school census (not withstanding a few exceptions where parents are given the option to self-declare or refuse, refer to [census guidance](#)) and certain responsibilities to return data to the local authority, means you have a **legal obligation** as your lawful basis ([see Annex 4.1](#)) and your condition for processing the special category data within that is **processing is necessary for reasons of substantial public interest**. This is to comply with GDPR Articles 6 and 9 and the Data Protection Act 2018 Chapter 2(8)

If the answer to that first question is ‘no’, then the second question to ask is:

“Do I need to process this data in order to safely and effectively run my school?”

If the answer to that is yes, then the lawful basis of **public task** may well apply, and again, the **public task condition may well apply where the data items are special category data**. An appropriate condition from articles 6 and 9 of the GDPR need to be identified. **Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding**. Information that could be relevant to keeping a child safe should be shared so that informed decisions can be made about a child’s welfare.

The next area to explore thoroughly is the data processing that does not appear to be legally essential, nor needed to run your school safely and effectively. These are the areas where other conditions, particularly specific consent of the data subject, may need to apply. Article 4(11) of the GDPR defines consent as:

“...any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”

Examples here from school life might include:

- A. A school asks students for consent to use their photographs in a printed student magazine. Consent in these situations would be a genuine choice as long as students will not be denied education or services and could refuse the use of these photographs without any detriment.
- B. “Marketing” materials to pupils/parents. This might include ‘non-school’ material, for example, if a local holiday club pays you to email parents with details of the holiday club, that is not an essential part of running the school. Or it may include school material such as fundraising campaigns. Consent will definitely be required if such communications are carried out electronically, because of the Privacy and Electronic Communications Regulations (PECR) but if marketing is paper based,

the lawful basis of legitimate interests could possibly be considered, subject to the usual balancing tests.

- C. You should seek consent, from the data subject, for keeping and using personal data (like contact details) of former pupils for fundraising, marketing, and other non-essential activities that you may want to undertake long after they have left school.
- D. If you are retaining data as part of a collection to contribute to the National Archives, please be mindful that there is specific guidance on this outside of your general processing of data. Please contact the National Archives team for further details and find detailed guidance on how to develop and manage digital archives and the data protection implications on their [website](#).

Importantly, if relying on consent:

1. Consent must be voluntarily given; it must be specific, informed and unambiguous, and able to be refused with an alternative process on offer. People should know exactly what they are signing up to.
2. Individuals must be able to revoke consent at any point and procedures need to be in place to allow individuals to withdraw consent.
3. Parental consent will always expire when the child reaches the age at which they can consent for themselves (13 years old). You need therefore to review and refresh [children's consent](#) at appropriate milestones. Please read ICO guidance on how to [handle children's consent after they turn 13](#). ([ICO Guidance on Consent](#))

Top tips:

- It is important to capture the [lawful basis](#) and conditions for processing. It determines the answer to 'what am I allowed to process?'
On its own, justification for processing does not provide compliance. Just as important as the 'what?' is the, 'how do I process it responsibly?' So, whilst a lawful basis exists for processing that a child is looked after, a school also needs to consider: how many people have access to which data, do they really need that level of access, what degree of history is necessary, how the security of the data is handled as a result of system security and policies how that data is used within the school. The school should also check that they are being transparent with data subjects about this processing.
- Within education, we do process some sensitive information about children that is not set out in the legislation as a 'special category personal data'. Notably information about children's services interactions, free school meal status, pupil premium eligibility, elements of special educational need information, and some behaviour data. **We consider it best practice that when considering security**

and business processes about such data, that they are also treated with the same ‘high status’ as the special categories set out in law.

- **Remember that the reasons/conditions relate to the processing activity, not the data itself.** For example, the processing of a parent’s phone details might be ‘to text message urgent school information, and contact in case of an emergency relating to their child’. That is essential to run your school well as a public task. That does not justify passing their phone number on to someone who wants to market tutoring services in the local area. Conditions for processing should cover the data items within an area, the purpose, the people, and ensure that necessity and proportionality are considered at all times.
- If you are relying on legal obligations as your condition for processing, think about what happens after you have fulfilled that legal obligation. For example, if you want to retain gender data on year 6 students after the summer school census, and the legal obligation is no longer relevant as the data has been sent to DfE, you need another lawful basis to rely in of you are to retain and use that data.
- Consent should not be relied upon for processing data essential for a school performing public tasks and for data in a learner’s Education Record. For example, you **do not** need parental consent to enter children for exams. If you are relying on consent, it must be easy to give and to withdraw. It should be voluntarily given without feeling forced to agree. If a data subject feels that they ‘must’ agree, or saying no is unduly awkward, then this is not a genuine consent process and a different lawful basis should be used.
- Article 7(2) of GDPR addresses pre-formulated written declarations of consent that also concern other matters. When consent is requested as part of a (paper) contract, the request for consent should be clearly distinguishable from the other matters. If the paper contract includes many aspects that are unrelated to the question of consent to the use of personal data, the issue of consent should be dealt with in a way that clearly stands out, or in a separate document. Likewise, if consent is requested by electronic means, the consent request has to be separate and distinct, it cannot simply be a paragraph within terms and conditions, pursuant to Recital 32.39
- Explicit consent should always be used for biometric data usage (and for that purpose only) – and if any one of the pupils or parents/carers do not wish to give consent, a genuine alternative must be offered. For example, stating “you can bring in a packed lunch” is not a reasonable alternative to a data subject not wishing to provide biometric data to support catering management. A pin number would be. This is set out in the Protection of Freedoms Act.

- You may find that more than one condition for processing applies. If so, it is good practice to document all that apply at this stage.

Safeguarding:

GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need.

The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent (DPA, Part 2,18; Schedule 8, 4)

When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file.

All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place.

The Working Together on Safeguarding Children statutory guidance states the following:

1. Effective sharing of information is essential for early identification of need, assessment, and service provision to keep children safe.
2. All professionals responsible for children should be proactive in sharing information as early as possible to help identify, assess and respond to risks or concerns about the safety and welfare of children, whether this is when problems are first emerging, or where a child is already known to local authority children's social care (e.g. they are being supported as a child in need or have a child protection plan). You should be alert to sharing important information about any adults with whom that child has contact, which may affect the child's safety or welfare.
3. Information sharing is also essential for the identification of patterns of behaviour when a child has gone missing, when multiple children appear associated to the same context or locations of risk, or in relation to children in the secure estate where there may be multiple local authorities involved in a child's care.
4. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare, and protect the safety, of children, which

must always be the paramount concern. To ensure effective safeguarding arrangements:

- you should have arrangements in place that set out clearly the processes and the principles for sharing information. The arrangement should cover how information will be shared within your own organisation/agency; and with others who may be involved in a child's life
 - all professionals responsible for children should not assume that someone else will pass on information that they think may be critical to keeping a child safe. If a member of staff has concerns about a child's welfare and considers that they may be a child in need or that the child has suffered or is likely to suffer significant harm, then they should share the information with local authority children's social care and/or the police. Staff should be particularly alert to the importance of sharing information when a child moves from one school to another, due to the risk that knowledge pertinent to keeping a child safe could be lost.
 - you should aim to gain consent to share information, but should be mindful of situations where to do so would place a child at increased risk of harm. Information may be shared without consent if you have good reasons to do so, and believe that the sharing the information will enhance the safeguarding of a child in a timely manner. When decisions are made to share or withhold information, you should record who has been given the information and why.
- Please refer to Annex 10.1 for a list of Safeguarding Myth-Busting points from the statutory guidance.

Case study: Ensuring data subjects have their rights respected when using biometric data – model policy provided by the Oxford Diocesan Trust (sourced from ‘The Key, in partnership with Forbes Solicitors and Emma Swann)

If and where the school uses pupils’ biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act, 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will seek written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school’s biometric system(s). If a biometric system is introduced, we will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners using cash at each transaction if they wish.

Parents/carers and pupils can object to participation in a school’s biometric system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil’s parent(s)/carer(s).

Where staff members or other adults use the school’s biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time and the school will delete any relevant data already captured.

Case study: Appropriate use of photography

Photographs are used in school for many different reasons. The different uses should be considered separately and potentially have different conditions for processing. For example:

- Photographs used in identity management may be essential for performing the public task of the school, but should be deleted once a child is no longer in that setting, as it is no longer needed for the purpose for which it was held.
- Photographs in the school environment relative to providing education may fall under the public task purposes, but after the child has left the school this argument becomes weak and may not be lawful; permission to retain beyond their time in school (if required) should be sought. For example, if the child is in a display showing a scientific experiment being done that you wish to retain as a learning resource for future years.
- Photographs used in promotion/marketing type material should seek specific informed consent, and only be used in line with the consent provided.

Relevant resources:

- The Information Commissioners Office (ICO) website provides more details about the [lawful basis for processing](#), and for special category data, [the conditions for processing](#). These are provided in [Annex 4.1](#).
- This [short video by GDPR in schools](#) provides a 3 minute commentary on the lawful basis relevant to schools.
- Find additional useful free advisory resources on the [GDPR in Schools website](#)
- Find more information about information sharing for safeguarding in the [statutory guidance](#)

ICO consent information:

- Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.
- If you process children's personal data, you should think about the need to protect them from the outset and design your systems and processes with this in mind.

- Compliance with the data protection principles, and in particular fairness, should be central to all your processing of children's personal data.
- If you are relying on consent as your lawful basis for processing, when offering an online service directly to a child, in the UK only children aged 13 or over are able provide their own consent.
- Where consent is the lawful basis for processing data for children under the age of 13, you must get consent from whoever holds parental responsibility for the child
- Where you are seeking consent from a child (13 or over), the consent must be written in a language they can understand

Step 5: Documenting how long you need to retain information

Intended outcomes:

1. Create a workable data retention policy that can be discussed and iterated with those who best understand your uses of data.
2. Understand that data retention is based on justification – if you can justify it, you can keep it.

How to approach this step:

- Schools need to be mindful that at present there isn't a 'sector wide data retention policy' guidance document. [Annex 5.1](#) is a very first iteration, but if one is to evolve, it will take greater engagement and consultation than has happened to date.
- It is important to understand that you cannot easily think about data retention at the most detailed level of individual data items – it is the context they are being applied that is relevant.
- Data retention does not have to be 'all or nothing' – as data becomes older, there are steps that schools can take to retain the power of pupil level data for analytical purposes, without the need to keep detail such as name and full address.
- The requirements for data retention as set out through legislation has not significantly changed through GDPR and examples of best practice already exist (for example, the [IRMS Schools Toolkit](#)), but many other aspects of data retention have changed due to how and why data is processed under GDPR and increased emphasis on data minimisation.
- The Data Protection Act 2018 adopts the General Data Protection Regulation (GDPR) principle of 'storage limitation', which requires that personal data should be kept for **no longer than is necessary** for the purpose for which the data are processed. The legislation does not impose specific limits or prescriptions on periods of retention for any data. It is important to put in place policies, as well as technical and organisational measures, to adequately prove (through evidence) that you adhere to, and comply with the 'storage limitation' principle.

Before tackling this, ensure you are comfortable with some of the simple terminology introduced in [Annex 1.1](#):

Term	Description	Example
Data subject	The person that the data relates to.	John Smith the pupil. Jane Smith the teacher.
Data item	A single piece of information about a data subject.	“Ethnicity = white British” “Attendance = 97%”
Data item group/element	A group of data items that are typically captured about the same activity or business process in school.	Behaviour management or catering.
System	A piece of software, computer package or manually managed asset that supports the administration of one or more areas of school life.	Capita SIMS, ParentPay, MyMaths.
System group	An umbrella term to describe the areas of school administration where systems that contain personal level data typically reside.	Core MIS, payments, curriculum tools.

These terms are important as we start to think about how long data is kept for. The focus should be on the time period that is ‘necessary and proportionate’.

Data items are extremely detailed, and to think them through it helps to group them together into data item groups. Similarly, with over 1,000 systems in use in the education sector, grouping into overarching themes can help provide focus.

When working with a group of people from schools, LAs, MATs and suppliers, we found grouping data items about pupils into the following areas was the most workable set of data item groups:

- admissions
- attainment
- attendance
- behaviour
- exclusions
- personal identifiers, contacts and pupil characteristics
- identity management/authentication
- catering and free school meal management
- trips and activities
- medical information and administration
- safeguarding and special educational needs

We used the [Common Basic Dataset](#) as the starter for creating the scope of what a school initially needs to focus on.

Once you have your list of data item groups, think about 4 periods of data retention:

1. One month after the event about which you create data is active, in order to ensure any 'loose ends' are tied up.
2. One year after the pupil to whom the data relates is at your school, in order to ensure smooth 'handover' activity related to the child is passed on to a subsequent school.
3. For 5 years after a pupil has left your school, to support longer term but detailed analysis of progress, attainment, support for different pupil groups etc. This is the area where 'blurring' of the data discussed below can gain most traction.
4. Long term, until the child is 25 years of age or older, for instances where detailed information about activities in school may form an important part of safeguarding for that individual.

When setting a data retention policy, consider the following questions:

- Why am I holding this data?
- Am I under legal duty to retain the information for a set period of time?' Consider legal duties that impose specific time periods for data retention
- Do I need to pass it on? Once I have passed it on, am I required to keep it? Do I still need to use it?
- What is the school's actual responsibility – is appropriate long-term retention actually someone else's job such as a receiving institution or local authority?
- What might Ofsted expect from me in terms of the length of time I can perform detailed reporting?
- As time goes on, can I delete some of the information – for example would aggregated data ('counts' of pupils that you might share with governors) or de-personalised data (individual rows, but with names and other identifiers removed) do the job just as well?
- "Because I always have done" is not a justification, but it may be a clue as to a justification. "Why might we have that policy?" Is a good question to ask.

A number of schools have collaborated with sharing thinking on data retention with us in creating this document, and their shared work is provided in [Annex 5.1](#). This is provided to stimulate thinking and discussion at a local level. As data controllers, schools should determine their own policies that work for them and their particular context.

Potential further work on retention

Based on the feedback we received, there are many concerns about data retention. To support schools fulfil their role, the department will explore the possibility of working collaboratively with schools to develop overarching data retention national guidelines, specifically in more sensitive areas like safeguarding, that can be adopted by all schools. If you want to participate in exploring the feasibility of this work, please send an email with the heading 'Schools Data Retention' to the following email address:




data.modernisation@education.gov.uk

A way to reduce sensitivity over time

When discussing data retention with colleagues across the sector, a common theme emerges. At some point in the pupil lifecycle, detailed fully named and personally identifiable data is needed. Before being comfortable deleting that data completely, there is usually a period where names or full addresses may not be needed, but individual level data still is. After that, there may well be a period where aggregated or summary statistics are all that is needed, and that retaining these for a long time was a good idea.

As we move through time and data becomes older (e.g. the years after a child leaves the school), schools may be able to take steps to remove some of the risks around personal level data by de-personalising it. That is, by taking the names and personal identifiers away, but retaining the data at individual level, schools can still undertake the longer-term analysis of trends or studying of impact on small pupil groups, but the underlying data being retained carries less risk than keeping all the personal identifiers within the data of interest.

This concept is hard to communicate, and to do so people increasingly talk about the 'blurring of a photograph'.

		
With pupil names and other identifiers, the data is instantly personal.	Typically, once the pupil has left, we need to ask if we still need identifiers like name or data of birth. Could 'term of birth do'? If so, that is good practice as it 'blurs' the data slightly.	Over time, can we retain aggregated summary statistics that are highly blurred? For example, the sort of data that might be shared with all governors.

This is an important concept; [GDPR requires data minimisation and data protection by design and default \(Article 25\)](#) – meaning data controllers and processors must implement appropriate technical and organisational measures, such as this 'blurring technique' (pseudonymisation), which are designed **to implement data-protection principles, such as data minimisation**. These techniques reduce risk, but do not negate the need for compliance with legislation.

Top tips:

- Anonymisation can be performed by simply replacing personal information with non-personal identifiers or aggregates where personal information is no longer required. For example, after a certain period from the day a child leaves school, you may replace the name with a random ID, the date of birth with year of birth and the postcode with locality or town name.
Example - Instead of keeping the records attached to the following information in your database: Name: John Smith; D.O.B: 18/06/2010; Address: 100 Smith Street, SW1P 3JR, London. You can anonymise that to: ID: Student 1004; Year of Birth: 2010; Address: Westminster. Provided you don't keep information linking John Smith to the ID 1004, the data associated with that record will not be easy to de-anonymise to personally identify John Smith. With pseudonymisation, you must retain a way to link the record back to John Smith. But, you must keep in mind that even such an approach will not be infallible. For example, if John Smith is the only child born in that year from that area, he could still be personally identifiable. That means you must exercise judgement and justify why you would want to keep that information.
- You cannot think about data retention/deletion at the data item or data item group level only. A good data retention policy needs to look at how long you retain data items within the different areas of administration of school life. "How long do we need to keep pupil names in our catering system?" and "how long do we need to keep pupil names in our safeguarding system?" are better questions, and may well generate different answers.
- We learned from discussion that within some areas of data, there is inconsistency in local practice in terms of data retention periods requested of schools, notably around safeguarding data. Follow your local best practice so long as it remains justifiable.

Relevant resources:

- In March 2018, DfE joined a number of schools, MATs, LA representatives and system suppliers to have a 'hack day' thinking about data retention. The combined data retention policy for a school from that thinking is set out in [Annex 5.1](#).
- DfE is aware that several schools make reference to the [IRMS Toolkit](#) when setting data retention periods. The IRMS is a not for profit organisation that supports the Information and Records Management Profession. As part of their current model they make some content available as open source.
- Annual Checklist for review of School Records incorporating Safe Data Destruction Log – Developed and used by The Oxford Diocesan Schools Trust (based on the IRMS document)

Step 6: Reassurance and risks

Intended outcomes:

1. Identify risks that emerge from the initial completion of your data asset register.
2. Assess what can be done to eliminate or reduce areas of medium/high risk and set action plans to do so.
3. Use Data Protection Impact Assessments as a part of your risk identification and mitigation procedures.

How to approach this step:

- A logical place to start identifying issues and risks is the data asset register outlined in [step 3](#). This will likely identify high-level issues. The most important things to look out for include:
 - Any “current activity” which does not map to a lawful basis and conditions for processing.
 - Do you have uncertainty about onward sharing? As a way to test this, could you demonstrate to a pupil which piece(s) of their personal data have been shared with whom, and when? If systems are moving data, they should be able to report on it. Do you think that you will be less likely to carry out safeguarding activities? If this is the case, it would be useful to re-assess how you are applying the law in this context.
 - Do you have an up to date data sharing agreement with organisations you are passing data on to?
 - Are your IT security policies up to date and is everyone handling personal data aware of your security policies and appropriately trained?
 - Do your systems allow you to implement **your** data retention policy? If not, then it is the system that should adapt to meet your needs, not your data retention policies being compromised to meet any limitations of a system.
 - Do people in your school know what the process is for reacting to a data breach? Have the processes (including IT response and recovery plans) for reacting been tested? Ensure sufficient time is given to the “here’s how we assess impact and minimise that impact” in your data protection policies.
- The data asset register does not flush out all risks and issues. However, regular reviews, use of external experts/advisors, and the involvement of the Data Protection Officer and data protection lead will all help here, as will the completion of Data Protection Impact Assessments.

- A Data Protection Impact Assessment (DPIA) is a tool to help you identify and minimise data protection risks. Conducting a DPIA meets, in parts, an organisation's accountability obligations under GDPR, and is an integral part of the 'data protection by default and by design' approach. An effective DPIA helps you to identify and fix problems at an early stage, demonstrate compliance with your data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage, which might otherwise occur. In some cases, GDPR says you must carry out a DPIA, but they can be a useful tool in other cases too.

Top tips:

- **Minimisation** is a key thing to think about:
 - Think about the minimum amount **of personal data** that is needed to get the job done. If an external consultant is coming in to look at progress of pupils in primary schools, then if month of birth or term of birth would do the job, there is no justification for passing on date of birth.
 - Think also about the **minimum amount of people that need access to personal data**. People should only see the personal data they need to see to perform their role. If the number of people seeing the data is indefinite, then this should be made explicit to the data subject.
- Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (DPIA). A DPIA is a process designed to describe the data processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. In other words, a DPIA is a process for building and demonstrating compliance. A DPIA is required when the processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)). Examples of when you need to conduct a DPIA:
 - **Data concerning vulnerable data subjects** Vulnerable data subjects include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees, more vulnerable segments of the population requiring special protection
 - **Innovative use or applying new technological or organisational solutions**, like combining use of finger print and face recognition for improved physical access control, Certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.
 - **CCTV**

- DPIAs will need to be frequently reviewed and kept updated. For example, the activity which is subject to the DPIA may slightly change and present new risks as a result. Your school will also need to review all uses of personal data on a regular basis to check whether any activity has started to present high risks to individuals and therefore requires a DPIA.
- Many data breaches occur via 'innocent mistakes'/human error, and unintended misuse of technology. Ocean Learning Trust are one trust that has withdrawn use of memory sticks/flash drives completely as part of their process to mitigate risk. If you decide to use removable hardware containing personal data you should think about, and limit, who has access to removable media. You should scan all media before importing onto the corporate system and employ encryption, strong passwords and other means of protection.
- Unfortunately, data breaches also happen because of targeted actions by malicious actors and hackers who can be based both internally or externally to the school setting. Regularly reviewing your IT security policies and processes are a must and simple steps like: Regularly updating your software; Employing strong passwords; Using anti-virus software, using encryption, protecting external devices and not leaving your computers unlocked can all make a real difference in preventing IT based data breaches. Staff awareness training on data gathering techniques used by cyber attackers can also be of benefit.

The following case studies focus on some known areas of risk common to many schools.

Case study: Pupils and medical information

Many schools have pupil photographs and key medical conditions on the staff wall. At the onset of thinking about GDPR, one school was thinking, “We ask parents for consent, but that’s special category personal data, should we take it down?”

When thinking it through the school decided:

- Consent was actually the wrong basis for processing. Although well intentioned, the information is actually deemed essential for keeping certain children safe. As such, it’s part of fulfilling a public task, consent should not be used. But at the same time...
- Checks could be done to ensure that it was only relevant medical information (that is, that which a member of staff needed to know in order to keep the child safe) that was used in this way.
- Further steps could be taken to minimise the amount of people who could see that information by re-positioning it and ensuring that only the right people had access to that room – that the space is ‘well policed’.
- That, as part of ensuring parents are informed, whilst consent is not sought, a clear statement about what is held, why it is important for keeping the children safe, and what steps there are to look after that special category data was good practice.

Case study: Mark books and target setting – two ends of the digital spectrum, but both with risks to manage

The data map done in [step 2](#) will likely show a very diverse ecosystem. Most primary schools for example have many paper documents, including pupil workbooks and mark books. These are often very ‘visible’ in classrooms. Whilst some personal information will be needed within them, practices which appear to unnecessarily increase the amount of sensitive pupil data, such as pupil premium and looked after status being contained within them should be avoided.

At the other end of the spectrum, many schools use software packages to support pupil target setting and progress reporting. If this is done ‘blindly’, with software generating targets that go on to trigger various interventions depending upon that target, then it is arguable in the automated profiling territory, outlined in [step 3](#). Ensuring staff see the inputs, can check the outputs to ensure errors in processing are picked up, and can manually adjust targets where other factors not contained within the progressing algorithm are relevant, would all seem good steps to take.

Case study: Taking personal data home

“Can we take information home about pupils?” is a common question raised. This applies to both previous/current legislation and new legislation. An organisation must be clear on:

- What information? – Like many areas of data risk management, has the boundary about what is necessary to perform the required tasks been established?
- What devices and software? – Have you ensured they are secure when being worked on outside the school environment? Has the policy on working on own devices (if allowed at all) been refreshed and reviewed?
- What training/awareness? – Are you confident that people using the information have the right level of training to be alive to all of the different risks that may present if using personal data outside of the school environment? Staff should be very aware of the breach notification process and how to trigger this if working remotely.

If having done that sort of thinking, an organisation feels confident that the risks around personal data are being well managed even when used remotely, then the law does not prevent it from happening. It is for the organisation to assess the benefits of working in this way, and that risks are being appropriately mitigated.

Case study: Using IT intelligently to reduce risk: Queen Elizabeth's High School, Gainsborough

One of the risks Queen Elizabeth High School (QEHS), Gainsborough identified early was the potential for any member of staff generating ad-hoc reports in the management information system (MIS) downloading the data onto an unsecure memory stick or personal laptop. It is incredibly useful for staff to be able to download lists of student names, other personal data or exam scores in order to be able to manipulate the data to provide insights into the achievement of groups of students and thereby set the best learning activities for them. However, there was a high risk of data breach if the memory stick or laptop was lost and the data was not encrypted.

Their solution has several layers of security to it in order to control the risks, but without placing an undue administrative burden on the staff of the school. They have provided every member of staff with a memory stick encrypted using a free to use encryption tool. Each memory stick is assigned to a member of staff and logged. No other devices can be used to download files from any computer in the school. Within their GDPR policy and staff behaviour code they have made it clear that no other memory source is to be used and if the data is taken off-site it is not to be loaded onto unencrypted computers at home.

If a member of staff wants a particular data set they email a member of the office staff who has received training indicating what data they want, why they want it and for how long they will keep the data. All of this information is logged so that the school has a record of all data exports that have been undertaken.

The data is then extracted as a spreadsheet, zipped, password protected and placed in a secure area of the school network for a limited time in order for the member of staff to collect it. The password is emailed to the member of staff separately.

As a result, QEHS Gainsborough are confident we have controlled the risks sufficiently to allow staff to continue to use this data as they did before in order to enhance our support for the students whilst protecting the data sufficiently to meet the requirements of the GDPR.

Case study: Reducing the risks associated with hardware: Broadmead Lower School, Bedfordshire

Broadmead Lower was thinking about the information risks associated with their printing and photocopying, which uses rented hardware. All classrooms and the office staff are networked into one printer, which is very cost effective. However, GDPR prompted some fresh consideration of risks.

- **Internal breach risks** existed because others could access printing before the intended recipient collected it, particularly when printers jammed and the print completed the intended job subsequently. This was significantly reduced by each staff member having a code that is used to run jobs when they are there to collect them, rather than as soon as they click print.
- **External breach risks** the preparation for GDPR meant the school felt more informed to ask about the hard drive in the machines: what information is retained? How long for, why and who can access it? What do the rental company do with that data once the machine is taken away? What evidence should we seek to confirm data destruction? What other networking and remote access risks do we need to consider?

Head teacher Kim Hewlett reflects:

“We decided to formally ask these questions when selecting a new supplier. I worked with our IT support providers to ensure that the information we got back was plain English and understandable, and as a result we are confident we now have the best solution for mitigating risks associated with printing and photocopying in our busy school”.

Relevant resources:

- To ensure Data Sharing Agreements reflect best practice, it is worth looking at [the ICO Data Sharing Code of Practice](#). This includes a model data sharing agreement.
- Information about GDPR compliant contracts can be found on the [ICO website](#).
- [Annex 7.2](#) is an example of a GDPR-compliant contract template produced by The National Association of Independent Schools & Non-Maintained Special Schools (NASS) for their members.
- Although written about the Data Protection Act 1998, [the ICOs 'Bring Your Own Device'](#) guidance covers many of the risks and practical steps for schools to take when weighing up remote working of staff.
- GDPRiS has a useful document about the [things schools will want to know from suppliers](#) in order to demonstrate GDPR compliance.

- [Annex 6.1](#) contains a Data Protection Impact Assessment template provided by CBICT, an organisation that supports schools in central Bedfordshire.
- The ICO website contains good information about [when and how to best conduct Data Protection Impact Assessments](#) as part of identifying potential areas of risk.
- The National Cyber Security Centre has a range of guidance on its [website](#) that can help keep your systems and personal data secure from online threats.
- The European Commission has guidelines on [personal data breach](#) notification
- ICO guidance on data breaches can be found here: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

Step 7: Decide on your Data Protection Officer role

Intended outcomes:

1. Understand the role of the Data Protection Officer (DPO), and be clear that, as a data controller, each school must designate a named DPO in order to be comply with new legislation (note, this DPO can be named as a DPO for more than one school/organisation and may not be a direct employee of the school or organisation).
2. Understand the different options for a school appointing a DPO, so that schools can consider the best value and appropriate method for them.
3. Understand the DPO will be the point of contact for communications with the Information Commissioners Office (ICO).

How to approach this step:

The first step is to understand the responsibilities of the DPO, and the greater degree of separation between the DPO role and the 'data ecosystem manager' than has previously been the case under the Data Protection Act 1998.

Responsibilities of the Data Protection Officer

Currently, schools have leads on data protection but very often they either are, or work very closely with, the person who has established the ecosystem. The new legislation encourages a degree of separation between those in charge of the ecosystem, and the DPO role. The DPO needs to be:

- **Highly knowledgeable** about data protection, GDPR, the schools operations, technology and security
- Well placed to promote a **data protection culture** within a school

The DPO role involves advising school leadership and staff about their data obligations, monitoring compliance, including managing internal data protection activities, training, and conducting internal audits.

The DPO will also need to advise on when data protection impact assessments are required, and be available for data protection enquiries from parents and pupils. Additionally, they need to be able to report directly to the board and be **the point of contact for communication with the Information Commissioner**.

Options for appointing a Data Protection Officer

The second step is the need to consider the pros and cons of the different options for designating or appointing a DPO. There appear to be 4 options available to schools:

1. **Re-align responsibilities within your current team** – create the DPO role within your team that is sufficiently removed from those making technology or processing decisions.
2. **Collaborate** – share the DPO function between a group of schools, or share expertise by being the DPOs for each other's school.
3. **Contract** – it is possible to buy in the DPO function for your school or group of schools. The DPO should have expert knowledge of data protection law and practice, as well as significant knowledge of the education system and regulations.
4. **Seek volunteers from experts that may exist in the wider school community.** This might be possible, but note that as a volunteer their statutory responsibilities remain at the same expectation as a paid DPO. It would be a reasonably big commitment for that volunteer, and they would need to be able to clearly convey risks and views to senior managers.

Effective working with a Data Protection Officer (DPO)

The DPO should be involved, properly and in a timely manner, in all issues that relate to the protection of personal data.

It is crucial that the DPO, or his/her team, is involved from the earliest stage possible in all issues relating to data protection. In relation to data protection impact assessments, the GDPR explicitly provides for the early involvement of the DPO and schools should seek the advice of the DPO when carrying out impact assessments. Ensuring that the DPO is informed and consulted at the outset will facilitate compliance with the GDPR, promote a privacy by design approach and should therefore be standard procedure within the school's data governance. In addition, it is important that the DPO be seen as a discussion partner within the school and that he or she be part of the relevant working groups dealing with data processing activities within the organisation.

Top tips:

At the time of publication of this toolkit (August 2018) the ICO has no plans to accredit certification or carry out certification although the GDPR does allow this (find out more about [certification](#) on their website). That means there are no 'certified DPOs' with respect to GDPR in the UK. Keep this in mind when you make decisions about who you designate as a DPO or courses you send staff on.

The options above are all genuine. Think through what is best for your school – the case study below may be helpful. As yet, there does not appear to be a common approach, but

it appears a 'many schools to one DPO' model is emerging as the most common, whether that is provided by the local authority, or multi-academy trust.

Case study: Ark's Data Protection Officer Solution

Ark has appointed an Information Governance Manager to serve as a MAT-wide data protection officer. This role supports Ark's 36 schools, ventures, and central teams with developing data protection policies and processes and updating IT and data systems to enable their technical GDPR compliance. Training and support to designated data protection leads within each school will ensure that they can lead their schools in protecting staff, student and parent data.

To support cultural compliance, all staff will learn about GDPR and data protection as part of their annual induction, in the same way that they learn about safeguarding in schools and diversity in the workplace. Annual safeguarding audits will also be carried out at each school, to ensure that day-to-day processes across our schools meet the new data protection requirements.

Students will be required to give consent on the use of their data during secondary school, where consent is the condition in [Annex 4.1](#) being relied upon, which will help ensure that they are educated in their rights as data subjects, as well as how to protect their own data, as part of the e-safety and digital/ICT elements of the curriculum.

By centralising the role of DPO across our network, Ark are reducing the burden on individual schools and supporting them in sharing resources and learning from one another on how to comply with the new regulations.

Relevant resources

- The European Commission sets out some [guidelines on Data Protection Officers](#).

Step 8: Communicate with data subjects

Intended outcomes:

1. Be familiar with the full potential rights a data subject has, and the circumstances in which these do not all apply, that is to say exemptions exist.
2. Consider how best to **demonstrate** your compliance with new legislation, which is a key focus of the changes. Compliance alone is not enough.
3. Be aware of 'exemplar' privacy notices for communicating with parents/pupils, and the work DfE is doing to test these with parents and the ICO on behalf of schools.
4. Gain benefits from being open and transparent with data subjects, there is more to building trust than compliance alone.
5. Subject Access Requests: key changes and tips for handling within schools.

Here is the link to [ICO Childrens Data Guidance](#)

How to approach this step:

- Be clear on who are the schools data subjects. Of course pupils are data subjects, but so too are staff, parents/carers and ex-pupils.
- The first thing to be aware of is 'what are key subject's rights?'
 - the right to be informed
 - the right of access
 - the right to rectification
 - the right to erasure
 - the right to restrict processing
 - the right to data portability
 - the right to object
 - rights in relation to automated decision making and profiling.

The right to be informed is a key part of the strengthened legislation. There are a number of ways that data subjects can be informed. These include:

- When providing 'initial registration' information upon joining the school. This is a big opportunity to get the data relationship right from the first contact.
- When providing additional information/data at various points during the year.
- Through effective use of the school website.
- In the case of staff, at various points in the 'lifecycle' of an employee, such as applying for a role, accepting a role/signing a contract, annual appraisals, upon conclusion of a contract etc.

But what does 'being informed' actually mean? It means the data subject receives clear communications about:

- what information is being collected/processed about them
- why the data is collected (purpose)
- what the lawful basis for processing the data (where applicable)
- who/which organisations data is shared with and why (this could be categories of organisations)
- how the data is stored and how long for, and how security is ensured
- how to exercise their right of access to data
- how to exercise any other rights, such as restricting certain types of processing or rectifying data
- who to contact for queries

A Privacy Notice is one way of doing this, and some links to templates are provided in the resource section below.

The revised legislation requires that when the data subjects are children it should be written in a concise, clear and plain style. It should be age-appropriate and presented in a way that appeals to a young audience.

Data subjects have a **right to access** data. One way they can do this is through a **Subject Access Request**, which can be a request to see part or all of the data a school holds about their child.

Subject Access Requests can also come from other data subjects such as staff or former staff/pupils

Once they have seen that data, they may request it to be **rectified** if it is incorrect, and this is one area where subject is accessing their data can help organisations. Regular (secure) checking of one's own data can help with data cleaning and quality, which has other benefits to the school.

Finally, you should think about where some of these **rights are not going to apply due to other conditions set out in [Annex 4.1](#)**. For example, the right to erasure. Whilst the child is in your school, there may be data that you would not erase if requested. For example, if the parent asked you to delete all your children's informal assessment data, then it would hamper your ability to perform your public task.

Top tips:

- Subject Access Requests (SAR) are not new within the 2018 legislation. The timeframe for response has shortened slightly (to one month, with exceptions). Schools do worry, "what happens if we get a SAR just before the summer holiday?" Education is largely unique in this regard, and the data protection legislation applies to all organisations processing personal data in the country. To efficiently deal with SARs the following tips may help:

- Include your willingness to help data subjects access their data in your privacy notice. Explain to parents that most of the year you aim to do this in a timely manner, but during school holidays this may become more difficult.
- If you receive a SAR:
 - Have a conversation to see if the requestor is willing to clarify the scope of the data requested. A parent may only be interested in one small part of the data record, and would far rather get a quick response focussed on that scope rather than await a full SAR response.
 - Consider whether a SAR is complex. Whilst you still need to notify the data subject within 1 month if that is what you decide, it does allow you a further 2 months to produce the information. You must be willing to justify that decision and tell the requestor about that decision as soon as possible.
 - Check if this is an Educational Record request, as set out in The Education (Pupil Information) (England) Regulations 2005, as the timescales for doing so may be shorter.
- The revised legislation extends the need to inform data subjects about processing to children, not just their parents. Done well, this is a good thing, but it is wise to be cautious here. A communication that children don't fully understand could do more harm than good. (A child worrying why the school is collecting their test data and sending it off to the government for example). In particular, with younger children, it may be that introducing such conversations within wider e-safety and ICT lessons is more appropriate. This then allows teachers to use language that suits their particular children, and ensure understanding and a 'chance to ask questions' is provided alongside the learning.

Relevant resources:

- Further information about [the rights of individuals](#) is provided on the ICO website, and specifically [children's rights relating to their data](#).
- DfE provides a range of [model privacy notices](#) for schools to adopt as one part of a schools communication with data subjects. These are currently being tested with groups of parents, and may well iterate in future as parental testing is combined with ensuring any edits remain aligned with legislation by checking in with the ICO.
- The ICO have also set out the [minimum standards of privacy notices](#)
- This simple [5 minute video](#) prepared by GDPRiS provides parent-focussed information that may be helpful in raising awareness amongst data subjects. There is an A4 printed sheet and infographic on the [free resources](#) section of their website.
- The European Commission [have a pdf document online](#) that sets out a lot of principles and good practice/bad practice examples in relation to transparency.
- See [Annex 3.2](#) for an example of a letter to parents for record-checking and consent – produced by the Oxford Diocesan Schools Trust

Step 9: Operationalise Data Protection, and keep it living

Outcomes from this step:

1. Identify the range of policies required within a school that cover the procedures and processes for data protection.
2. Understand what a data breach is, and what to do about it.
3. Ensure that data protection and risk management is a core and regular part of decision-making and risk management practices within the school.

How to approach this step:

- The data that is processed, and the mechanisms through which your school undertake that processing, will evolve over time. The key things which need to be living documents to ensure they keep up with change are your:
 - data map/ecosystem drawing
 - data asset register
 - data protection impact assessment and risk management activity plan
- The Data Protection Officer will have views on how best to do this. It is about ensuring that the data protection principles outlined in your school's policies are embedded into processes within the organisation. For example:
 - Confirming that a new system has been recorded on the data map and data asset register should be an essential step before any procurement activity is concluded.
 - Each time data is shared outside the school, a 'check and send' culture to ensure that the data you are sharing, and who you are sharing it with, is logged centrally is good practice. Check that where appropriate a data sharing agreement exists and a record of the sharing is logged.
 - Ensuring the risk management work being undertaken feeds into overall risk registers and conversations with governors.
 - Ensuring that staff training is regular and appropriate.
 - Ensuring that you make the best use of 'key times' to communicate with data subjects, such as when first registering contact information.
- Operationalising the safe use of data on an ongoing basis requires a strong combination of safe people, safe technology, and safe processes. As such, ensuring that your school complies with the legislation requires looking across a wide number of policies that are used in schools today. Our working group has established the

following (non-exhaustive) list of policies, which together help play a part in ensuring good management practices when it comes to data:

- Fair Processing or Privacy Notice – Pupils
- Fair Processing or Privacy Notice – Employees
- Data Protection Policy
- Data Retention Policy/Schedule
- IT and Communications Systems Policy incorporating:
 - roles and responsibilities
 - e-Safety policy
 - IT security policy
 - responsible user agreements
 - social media policy
 - trust website requirements and monitoring
- Code of Conduct
- Child Protection Policy (we have asked the local safeguarding board to review this)
- Business Continuity Policy
- Acceptable Use Policy: Employees
- Acceptable Use Policy: Pupils
- Acceptable Use Policy: Governors
- Data Breach Policy

Top tips:

- In addition to the right policies, procedures, and processes; you must ensure all contracts and agreements (controller to controller or controller to processor) are compliant with data protection law. Refer to the 'Relevant Resources' section below and [Annex 7.1](#) and [Annex 7.2](#) for examples.
- Consider taking advantage of the ICO advisory audits. [According to the ICO](#), the audit provides an assessment of whether your school is following good data protection practice and will help you understand and meet your data protection obligations. The audit looks at whether a school has effective controls in place alongside fit for purpose policies and procedures to support data protection obligations. You will benefit from the data protection knowledge and experience of the ICO's audit team at no expense. The audit is an opportunity for staff to discuss relevant data protection issues with the members of the ICO's audit team to improve their knowledge and awareness.
[The ICO will produce an advisory report with recommendations on how to improve. See Annex 8.1 for an example of a report that was produced for an academy.](#)
- A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Some organisations may refer to this as a breach of confidentiality, integrity or availability, as this is how it is often referred to in many international

information and security standards. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach may be about more than just losing personal data. The initial steps should be to minimise and assess the impact, and a range of different steps then need to be taken depending upon the severity, as set out in the [ICO guidance](#).

- It is good practice to record and investigate every data breach, however small. An analogy here might be the 'accident log book'. Whilst a child grazing a knee may be minor in isolation, if each incident is reported and a trend around a piece of playground equipment is spotted, some remedial action might be appropriate. And so it is with data protection: if a particular system or process is identified as regularly having minor incidents by the Data Protection Officer, they and the school can mitigate the risk. They can only do this if a 'report it always' culture exists and is encouraged.

In the event of a serious data breach involving the personal data, for which the controller is responsible, the Data Protection Officer must report the breach to the Information Commissioner. A serious breach is a breach that interferes with the rights and freedoms of the data subject. Serious data breaches must be reported to the ICO within 72 hours of becoming aware of the breach, where feasible. **You should have the right policies and procedures in place for assessing the severity of data breaches and reporting them. Usually, this is done through the DPO, who is the primary contact for the ICO.**

Examples of a serious data breaches:

- **Losing or accidentally sharing data containing financial (banking) information about staff, especially if the information can be used fraudulently to cause financial damage to individuals.**
- **High risk example (i.e. notify data subject) – Whilst on a school trip, details are lost with the names, numbers and contact addresses of a class of pupils, but it also contains details of a looked after child who is at risk.**
- **Risk example (i.e. notify ICO within 72 hours) – MIS server is infected with ransomware and school is not able to retrieve data.**

See [Annex 9.1](#) for an example of a real school data breach, including the ICO response. This anonymised example is, however, not a serious data breach

Relevant resources:

- **Find out about ICO Data Protection Audits and how you can request one for your school: <https://ico.org.uk/for-organisations/resources-and-support/audits/>**
- **Find in [Annex 7.2](#) the national contract for placements in non-LA special schools. The last version was drafted in 2013, by The National Association of Independent Schools & Non-Maintained Special Schools (NASS), with help from local**

authorities, LGA and ADCS. NASS hosts it and it is available here:

<https://www.nassschools.org.uk/national-schools-contract/>

The contract is free for anyone to use - you don't have to be a NASS member. It was designed to be used by special schools as a contract to cover the local authority top-up element of high needs funding.

NASS commissioned a legal firm to draft a GDPR amendment clause, which is attached in [Annex 7.2](#). This can also be accessed on the NASS website:

<https://www.nassschools.org.uk/national-schools-contract/>

NASS prepared some guidance notes ([Annex 7.1](#)), initially for their schools, but have subsequently adapted these to contain more general information. The guidance is framed as what NASS calls a schedule 6 amendment. This reflects the structure of the national contract where any request to vary the existing terms and conditions can be set out in schedule 6 of the contract and agreed by both parties. Anyone not using the contract but wanting some brand wording on GDPR relationships between schools and LAs can cut and paste the majority of the wording, just removing references to clause numbers, which relate to the national contract.

- The ICO has guidance and templates to support schools undertake [Data Protection Impact Assessments](#). (NB: under consultation at the time of creating this version of the toolkit).
- The [ICO has a section on data breaches](#) and sets out what to do when. If you are unsure how best to handle a breach they offer a helpline service to support you assess the impact and appropriate steps.

Annex

Annex 1.1 Explaining the language around data protection

Term	Description	Example
Data subject	The person that the data relates to.	John Smith the pupil. Jane Smith the teacher.
Data item	A single piece of information about a data subject.	“Ethnicity = white British” “Attendance = 97%”
Data item group	A group of data items that are typically captured about the same activity or business process in school. These are also sometimes called data elements or data scope within the data community/sharing agreements schools have with suppliers.	Behaviour management, or catering.
Dataset	A collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer.	A database, table, number of related tables, a spreadsheet
System	A piece of software, computer package or manually managed asset that supports the administration of one or more areas of school life.	Capita SIMS, ParentPay, MyMaths.
System group	An umbrella term to describe the areas of school administration where systems that contain personal level data typically reside.	Core MIS, payments, curriculum tools.

Term	Description	Example
Personal data	Information relating to a natural identifiable person, whether directly or indirectly	John Smith was born on 01/01/1990. The head teacher's salary is £60,000.
Special category data	These are highly sensitive pieces of information about people. They are important because under GDPR they are afforded extra protection in terms of the reasons you need to have to access and process that information. In education, it would also be best practice to treat things like FSM, SEN, and CIN/CLA status as special category data.	Tightly defined as data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, health, trade-union membership, and health or sex life. Data relating to criminal offences is also afforded similar special protection.
(Data) Controller	The organisation who (either alone or in common with other people or organisations) determine the purpose for which, and the manner in which data are processed.	A school is usually the data controller, but they can also be a joint controller with their LA or DfE.
(Data) Processor	A person or organisation who process data on behalf of and on the orders of a controller.	A catering supplier the school uses.
Data audit/data asset register	The assessment of data and its quality, for a specific purpose. Other terms you might hear are data map or information asset log. In this context, we simply want the list of personal data assets that we hold, from which we can go on to place further important information alongside.	

Term	Description	Example
Lawful basis and conditions for processing	These are the specific reasons, set out in law, for which you can process personal data. There is one list for personal data (lawful basis article 6) and another list for processing special category data (article 9).	"The processing is necessary for administering justice, or for exercising statutory or governmental functions." Read the full list.
Data retention	How long you will hold information to do the processing job you need it for. At the end of a data retention period, processes should be in place to ensure it is properly disposed of.	"We keep parent's phone numbers until 1 month after they leave the school in case of any issues that need resolving (for example, payment or repayment of lunch money) and then it is deleted."
Privacy notice	This is a document that explains to the people you have data about ("data subjects") the data items you hold, what they are used for, who it is passed onto and why, and what rights they have.	DfE publish model privacy notices .
Subject Access Request (SAR)	This is where a person (data subject), requests access to the information you hold about them. Timescales for responding, as well as reasons why you must comply, or may refuse, are set out in law. A Subject Access Request is can be for all data about a subject or for specific information.	"I want to know the attendance data you hold about my son"
Data Protection Impact Assessment (DPIA)	This is a process to consider the implications of a change you are introducing on the privacy of individuals' data. Assessing privacy at the outset helps you plan	You would undertake one of these if introducing a new system to use

Term	Description	Example
	consultation/awareness/consent type options from the outset. "Privacy by design" is a term that is used in this space.	fingerprinting within catering provision.
Data breach	A personal data breach means the accidental or unlawful destruction, loss, alteration, disclosure, or access to, personal data. Breaches are either accidental or deliberate. It also means that a breach is more than just about losing personal data.	Sending a list of pupil names, attainment marks and dates of births to the wrong school.
Automated decision making/profiling	This is when machines/software make decisions based on rules generated by the machine/software, without human intervention, about someone. Typically, it is the significance of the decision that drives the caution and concern here. Read further information.	"Anyone recorded as attendance >99% will get a voucher for X"
Data Protection Officer (DPO)	<p>The GDPR requires data controllers to designate a Data Protection Officer (DPO) The DPO must be entrusted with the following:</p> <p>(a) informing and advising the controller (including processors and employees) of their data protection obligations</p> <p>(b) providing advice on data protection and monitoring compliance</p> <p>(c) co-operating with the Information Commissioner, acting as the contact point for</p>	<p>The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.</p> <p>A DPO can be an existing employee or externally appointed.</p> <p>Ideally, an effective DPO will have significant skills and knowledge of the education system and its regulations.</p> <p>When deciding on appointing or</p>

Term	Description	Example
	<p>issues relating to data protection.</p> <p>(e) monitoring compliance with policies of the controller in relation to the protection of personal data</p>	<p>designating a DPO, you must keep in mind that there are no 'certified DPOs' yet with respect to GDPR in the UK.</p>

Annex 2.1 Table for identifying personal information to support the initial data map

	Do we receive personal data?	Do we create personal data?	Do we send personal data?	Do we destroy personal data?
Admissions				
Core management information system				
Curriculum tools				
Payment systems				
Virtual learning environments				
Catering management				
Safeguarding				
Trips and transport				
Uniform, equipment and photographs				
Identity management systems				
Contact/communication systems				
Social care and health interactions				
Statutory returns				
References and education settings you pass children onto				
Workforce systems				
Paper records				
Other				

Annex 3.1 ICT Policy Agreement - Example

{SCHOOL LOGO}

Staff ICT Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone.

These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That the schools' ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff will have good access to ICT to enhance their work, to enhance learning opportunities for our young people and will, in return, expect staff to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that the young people receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

Safety for my professional and personal:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, tablets, etc.) out of school.

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to a member of the Senior Leadership team.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will only use my personal equipment to record these images if it is password protected.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school into disrepute.
- I will only communicate with young people and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- If the data on any device is breached I will report it to the Senior Leadership Team

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (iPads/PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I understand the importance of regularly backing up my work.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, racist material, adult pornography covered by the Obscene

Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself, or others, as outlined in the School Data Protection Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that the data protection policy requires that any staff or young person's data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law, or by school policy, to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- It is my responsibility to understand and comply with current copyright legislation.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school, and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff Name	
Signed	
Date	

Annex 3.2 Example letter to parent/carer for record checking and consent

Child's name:

Date:

Dear [parent/carer name],

Caring for your information

As you may be aware, new data protection rules came in from 25 May 2018 (called the General Data Protection Regulations or "GDPR"). As part of our ongoing process of meeting the new requirements and best practice, we would like to take the opportunity to do two things:

1. Checking the accuracy of your child's information

Firstly, we would like to check that the information we hold about your child, including emergency contact details, are fully up to date. Please see attached a print out of your child's information from our systems.

2. Seeking your consent

Secondly, at [school name], we use information about your child in a number of different ways, and we'd like your consent for some of the ways we use this personal data. We set these out in more detail below. If you are not happy for us to use information in the ways we list below, that's no problem – we will accommodate your preferences. Similarly, if you change your mind at any time, you can let us know by emailing [email address], calling the school on [phone number], or just popping in to the school office.

If you have any other questions, please do not hesitate to get in touch.

Yours sincerely

Head teacher

Please tick the relevant box(es) below, sign and return this form to school office by [date]

1. Checking the accuracy of your information:

Question	Tick ()
I have checked the print out of my child's information, including emergency contact information, and I confirm the details are correct (or where incorrect I have amended)	

2. My consent

Question	Tick ()
I am happy for the school to take photographs of my child, to use them on the school website and in the school prospectus	
I am happy to receive marketing materials and fundraising requests from the school and the parent teacher association (PTA)	

3. Signature

Signed by Parent/Carer	
Date	

Annex 4.1 The possible lawful basis and conditions of processing for personal data

The lawful basis for processing personal data

These are set out in Article 6 of the General Data Protection Regulation (GDPR). At least one of these must apply whenever you process personal data:

- a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- d) **Vital interests:** the processing is necessary to protect someone's life.
- e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests. This cannot apply if you are a public authority processing data to perform your official tasks. Public authorities will need to rely on official functions.

Where you are processing **special category data**, set out in Article 9 of GDPR, **as well as** one of the six lawful basis for processing, you must ensure that a **condition for processing** from the following list applies:

- a) **the data subject has given explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.
- b) processing is necessary for the purposes of **carrying out the obligations and exercising specific rights of the controller, or of the data subject, in the field of employment and social security and social protection law**, in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
- c) **processing is necessary to protect the vital interests of the data subject or of another natural person** where the data subject is physically or legally incapable of giving consent.
- d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a

political, philosophical, religious or trade union aim, and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes, and that the personal data are not disclosed outside that body without the consent of the data subjects.

- e) processing relates to personal data which are manifestly made public by the data subject.
- f) processing is necessary for the establishment, exercise or defense of legal claims, or whenever courts are acting in their judicial capacity.
- g) **processing is necessary for reasons of substantial public interest**, on the basis of Union or Member State law, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
- h) processing is necessary for the **purposes of preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law, or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.
- i) processing is necessary for **reasons of public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
- j) processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Schools will also need to know and rely upon the additional conditions for processing special category in Schedule One of the Data Protection Act.

Annex 5.1 An Emerging Data Retention Strategy for the sector

It is clear from work done so far that the sector is some way off having one 'standard' data retention set of standards. Whilst 'one policy' for the sector may never quite be achieved, most would recognise that there is benefit in greater harmony than we have at present within our sector.

This is an area of this document that is very much a 'work in progress'. **We would welcome feedback and how we can work up the thinking set out below into something that grows into an authoritative set of recommendations.**

For now, we recommend what is below to stimulate thinking and consideration of your local practice, but we do not recommend that any firm decisions are taken on the back of this guidance alone. It remains for each school, as a data controller, to set the data retention schedules that work for them and are justifiable.

We have introduced that data items aggregate into data item groups. Whilst thinking at data item group level allows us to have a sensible conversation, it should be noted that the data item group 'Personal identifiers, contacts and pupil characteristics' generally sits within all other data item groups:

Personal identifiers, contacts and pupil characteristics
Admissions
Attainment
Attendance
Behaviour
Exclusions
Identify management and authentication
Catering and free school meal management
Trips and activities
Medical information and administration
Safeguarding
Special educational needs

The following table sets out the emerging thinking from a sector working group discussing data retention in schools. This is provided as an illustration of the types of justification schools might want to consider. Further work is needed to test and iterate these justifications. Schools should continue to develop and own their own data retention policy based upon local justification and necessary task.

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
Admissions		X (admissions files)	X (admissions appeals)		<p>Admissions files</p> <p>Admissions data is used extensively from the period of the school receiving it up until the point where children enrol.</p> <p>It is then used for some validation and cross checking of enrolment details. Once enrolled, the child's records in the MIS become the core record.</p> <p>Data about children who enrolled but didn't get in is useful, but any intelligence gathered from it (for example, where in the city children are interested in our school, or the SEN make up) is aggregated within the first year to a level being non-personal, after that, the detailed data within the admission file could be deleted.</p> <p>It is important to retain detailed data for a year, any appeals for which richer data about other</p>

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
					<p>successful/unsuccessful appeals may be relevant typically happen in the first year.</p> <p>Information about admissions appeals</p> <p>When dealing with appeals, having a reasonable history of any other appeals in some detail can be needed to deal with the particular appeal. The information is needed alongside the admissions policies of the time.</p>
Attainment			X		<p>Formative assessment data is useful as a child is building towards a particular more formal assessment. Once the child leaves the school, it has little value in terms of retention.</p> <p>Summative attainment is the main outcome of what children 'attain' in school. It is important that future schools where pupils go on to learn can understand previous attainment. Whilst often that information is 'passed on' smoothly as children move phase, it is not always the case, and thus retaining the names alongside the main attainment</p>

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
					<p>data for 1 year after the pupil has left the school feels proportionate.</p> <p>Trend analysis is important, 3 to 5 years is often the 'trend' people look at, but longer may be relevant. Whilst this must be fully flexible in reporting small sub groups, and the data would wish to be retained at individual level, some personal data (for example, name) could be removed from the data to reduce sensitivity.</p> <p>After 3 to 5 years, then aggregated summaries that have no risk of identifying individuals are all that are typically needed to be retained.</p>
Attendance		X			<p>Attendance data probably resides in some 'operational' systems in schools, such as cashless catering. In these systems, the data should only be retained until the associated business processes have concluded (for example, payment of meals). The start of the next academic year once all bills are settled feels proportionate.</p>

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
					<p>Attendance is related to individual attainment and so being able to relate attendance to attainment whilst in our care is important. Keeping it in detailed, individual form for one year after the pupil leaves school support conversations about detailed attendance that may be needed to best support that child.</p> <p>After that period, non-identifiable summary statistics are all that is required to support longer-term trend analysis of attendance patterns.</p> <p>We noted another GDPR principle here that may apply to attendance. Under data minimisation, where 'paper records' capture attendance, this paper record duplicates the electronic version and is probably required once the paper has been transferred to a stable electronic format.</p>
Behaviour		X			<p>This is all relevant for managing children when with at your school. 1 year allows a period of 'handover' to next institution with conversations supported by rich data if relevant.</p>

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
Exclusions		X			Exclusion data should be 'passed on' to subsequent settings. That school then has responsibility for retaining the full history of the child. If a private setting or the school is unsure on where the child has gone, then the school should ensure the LA already has the exclusion data.
Identity management and authentication	X (images used for identity management)				
Catering and free school meal management		X (meal administration)	X (free school meal eligibility information)		<p>A short historic record of what a child has had may be useful in case of any food-related incidents at school, or parental queries about the types of meals their children are choosing. Keeping for up to one year also allows time to do accounting work associated with catering. Typically 'one month' may not be enough, but 'one year' feels enough.</p> <p>Due to the way school funding works, free school meal eligibility is a financial matter, and thus keeping this data for 6+1 feels appropriate. This 7-</p>

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
					year record also needs to be portable with the pupil, as historic dates can be used for funding.
Trips and activities	X (field file) X (educational visitors into school)		X (financial information related to trips)	X (major medical events)	<p>Financial information related to trips should be retained for 6 years + 1 for audit purposes. This would include enough child identifiers to be able to confirm contributions.</p> <p>A 'field file' is the information that is taken on a trip by a school. This can be destroyed following the trip, once any medicines administered on the trip have been entered onto the core system. If there is a minor medical incident on the trip (for example, a medical incident dealt with by staff in the way it would be dealt with 'within school'), then adding it into the core system would be done.</p> <p>If there is a major incident (for example, a medical incident that needed outside agency) then retaining the entire file until time that the youngest child becomes 25 would be appropriate.</p> <p>Permission to go on the trip slips will contain personal data, and destroying them after the trip</p>

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
					<p>unless any significant incident arises is appropriate, otherwise refer to the policies above.</p> <p>Schools sometimes share personal data with people providing 'educational visits' into school. There should be good policies in place to ensure that the sharing is proportionate and appropriately deleted afterwards.</p>
Medical information and administration	X (permission slips)	X (medical conditions and ongoing management)		X medical incidents (potentially)	<p>To support any handover work about effective management of medical conditions to a subsequent institution.</p> <p>Permission forms that parents sign should to be retained for the period that medication is given, and for 1 month afterwards if no issue is raised by child/parent. If no issue is raised in that time, that feels a reasonable window to assume all was administered satisfactorily. Adding this policy to the permission slip would seem prudent.</p> <p>Medical 'incidents' that have a behavioural or safeguarding angle (including the school's duty of care) should refer to the retention periods associated with those policies.</p>

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
Safeguarding				X	All data on the safeguarding file potentially forms part of an important story that may be needed retrospectively for many years. The elements of a pupil file (name, address) that are needed to identify children with certainty are needed to be retained along with those records.
Special educational needs					Refer to IRMS toolkit
Personal identifiers, contacts and personal characteristics	X (images used in identity systems) X (biometrics)	X (images used in displays in school)	X (postcodes) X (names) X (characteristics)		<p>Images are used for different reasons, and the reason should dictate the retention period. Images used purely for identification can be deleted when the child leaves the setting. Images used in displays etc. can be retained for educational purposes whilst the child is at the school. Other usages of images (for example, marketing) should be retained for and used in line with the active informed consent, captured at the outset of using the photograph.</p> <p>Biometric data (typically fingerprints used in things like catering) should be used and retained as set out in the active informed consent gained at the outset, but typically this should not be retained long</p>

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Long term need (pupil at school +5 years)	Very long term need (until pupil is aged 25 or older)	Justification
	X (house number and road)				<p>after the activity that requested its use has finished (for example, the child no longer attends the school to have a meal).</p> <p>As set out in other sections, names are needed for smooth handover to subsequent schools for up to one year.</p> <p>Postcode data is useful in analysing longer-term; performance trends or how catchment/pupil populations are shifting over time, but full address data (house number and road) is not required for that activity.</p> <p>Schools may well provide references for pupils for up to 3 years after they leave, and so retaining the name in the core pupil record is important (this doesn't mean it needs to be retained in all systems). Keeping names attached to safeguarding files for longer than this may be entirely appropriate – see safeguarding section.</p> <p>Characteristics form an essential part of trend analysis, and so retention is in line with those needs.</p>

When setting data retention policy, it is good practice to not only create the written 'plain English' justification, but also set it alongside the lawful basis for processing, set out in [step 4](#).

Data retention should also be communicated 'as a whole', so the data subject is as informed as possible. So, importantly, a school data retention document may describe exactly when a school destroys personal level data, but the school should take steps through privacy notices to ensure that the data subject is aware of where else the data has been sent, and ideally, signpost to the data retention policies associated with that sharing.

DfE is aware that several schools make reference to the [IRMS Toolkit](#) when setting data retention periods. The IRMS is a not for profit organisation that supports the Information and Records Management Profession. As part of their current model, they make some content available open source. The data retention element of that toolkit has many strengths, in particular the links with related legislation and the fact that it has evolved over time with significant input from people involved in the administration of education who are members of the IRMS.

Depending upon the feedback during the initial consultation period, it is probable that further work will be done to develop a consistent voice that supports schools by generating and sharing exemplar data retention policy.

Annex 6.1 Example Data Protection Impact Assessment template

Data set/system	Current practice	Impact of threat if occurs: 1=low 5=high	Likelihood: Low, medium, high	Response to risk	Action plan	Review date
Name the data set and/or system with personal level data	<p>What current practices exist (or not) that could either lead to the threat materialising or prevent the threat from materialising?</p> <p>For example, data entry, data management, transfer of data, collection of data, printing and storing information, handling data</p>	<p>Identify what potential threat could be realised. Is threat related to:</p> <ul style="list-style-type: none"> Privacy breach (data shared w/o consent or disclosed) Individual – in danger of harm/potential embarrassment /loss of confidentiality/ discrimination System failure or technical issues Non-compliance with GDPR through inadequate procedures/ non-consent/ negligence/ 	<p>As a result of practice, how likely is the identified threat a reality?</p> <p>Select from: Low Medium High</p>	<p>Transfer risk to third party/insurance</p> <p>Treat/mitigate Risk - reduce risk</p> <p>Tolerate/accept level of risk</p> <p>Terminate/remove risk</p>	<p>Where the likelihood of a threat is high or medium, identify the actions to address the threat and mitigate or minimise the risk if not eliminated</p> <p>What actions can be taken to minimise the risk or eliminate the risk altogether?</p> <p>In some cases, threats cannot be removed entirely in which case, can agree action to 'Accept risk – no further action necessary'</p> <p>Ensure actions have lead person identified, timelines and linked</p>	Depending on Action taken plan for a review

Data set/system	Current practice	Impact of threat if occurs: 1=low 5=high	Likelihood: Low, medium, high	Response to risk	Action plan	Review date
		disregard/ ignorance/data shared without consent/data loss			actions that impact upon the overall action to mitigate or eliminate the risk.	

Annex 7.1 GDPR, Schools and Contracts – Guidance Notes

Introduction

New data protection legislation, the General Data Protection Regulation (“GDPR”) came into effect on 25 May 2018. This is supplemented by a new UK Data Protection Act. Among the changes made by GDPR is a requirement to have more detailed contracts where one organisation processes personal data on behalf of another.

As GDPR comes into full effect, organisations are trying to upgrade their contracts with the people they either share data with or who process data on their behalf. GDPR has stricter requirements for these contracts and almost all existing arrangements will need to be updated to some extent. Schools are starting to see requests from local authorities and other public sector bodies.

This guide focuses on the National Schools and Colleges Contract (version 2.5) but many of the principles will be applicable to other contractual arrangements.

Terminology

The key distinction to bear in mind is between the “data controller” and the “data processor”. The data controller is the organisation which determines the reasons for which data will be processed and the manner in which this will be done. The data processor is a third party which processes data on behalf of a data controller, for example when providing outsourced services.

Personal data is information about a living individual. Schools will hold significant amounts of personal data about a variety of data subjects. The data subject is the individual person about whom personal data is held. The key focus is likely to be on data about learners but it is important to remember that schools will also hold personal data about parents, employees and non-employed staff, and contacts at the local authority such as social workers.

Data Transfers in a School Context

Typically, when looking at the relationship between a school and a local authority, the data sharing relationship is more co-operative than in a standard controller-processor relationship. The care and needs of the learner are critical, and this involves sharing a wide range of information both about the learner themselves and those individuals, such as school personnel, who they come into contact with. It may also involve data sharing among a wider group of organisations than simply the local authority and the school, for example involving health services and the Education Funding Authority.

The ICO’s guidance, in particular a report issued in 2012, is consistently clear that schools are data controllers, and that transfers to local authorities constitute data sharing between two data controllers rather than a processing relationship from a controller to a processor. Although the existing guidance reflects the DPA position and has not yet been updated for GDPR, the definitions of controller and processor have not changed and GDPR is unlikely to affect this position.

Some practical examples of controller to controller data sharing in this context which may be of use include:

- Information about pupils. Although the local authority clearly has a close interest in the pupils it places with a school, the school needs to use a significant amount of data for the purposes of the day to day running of the school and will do so as data controller. The National Schools and Colleges Contract confirms that a number of responsibilities lie with the school and the school will need to use personal data to perform these. In addition to day to day activities, the school is responsible for dealing with disciplinary issues, exclusions and complaints and although there will be some data sharing and co-operation, this is a process which the school will run for its purposes rather than because it has been instructed to do so by the local authority.
- Information about the school's personnel. The school will be the data controller in respect of this information when using it for HR related matters, such as recruitment, payroll, performance management and so on. However, the school will also have obligations to share this information with the local authority. For example under the National Schools and Colleges Contract, the school must notify the local authority if the head-teacher is absent for more than four weeks. This data is not collected solely because the local authority wants it – the school would hold it in any event e.g. for sick pay purposes.
- Another example relating to employees is in relation to employee vetting. A school has direct obligations under law to ensure that its staff are suitable. These are not simply contractual requirements carried out on behalf of the local authority. This means that data held or collected for the purpose of complying with these obligations will be data in respect of which the school is the data controller. Even where the local authority has a contractual right to review the school's record keeping in order to monitor compliance, this does not mean that the data is processed on the local authority's behalf.
- The school also has other directly enforceable legal obligations, and again data held in order to comply with these obligations will be data in respect of which the school is the data controller. These include requirements relating specifically to education such as those obligations listed in clause 4.2 of the National Schools and Colleges Contract, but also broader legal requirements such as health and safety. For example an accident book, or health and safety report, would be held or created for the school's own purposes to comply with these obligations.
- Data will also need to be shared in relation to safeguarding. This is likely to include information about school employees, non-employed staff or volunteer personnel as well as the learner or learners involved. Each party will have its own obligations in relation to safeguarding.

One exception to the general position that each party will act as a data controller and will simply share information with the other is information used by the local authority for the purposes of fulfilling its statutory obligations (for example the creation of the Educational Health and Care Plan). Even where the local authority is legally responsible for doing this, it will sometimes outsource the work to school staff. When using data for this purpose, the school may be the data processor of the local authority.

Current Position under the National Schools and Colleges Contract

The National Schools and Colleges Contract reflects the position outlined above. Clause 8.11 envisages that both parties will act as a data controller when performing the contract. It places an obligation on both parties to comply with their own data protection obligations as data controller. It also makes it clear at clause 8.9 that schools will have obligations in respect of data subject access requests, which is consistent with the school's position as data controller.

The contract does not currently contain any data processing provisions. Arguably there may be some situations in which data processing does take place as described above, and although these should be regarded as the exception to the rule, there is an argument for including a provision to cover what happens in this situation, unless this is to be picked up in a separate contract. However, even in this situation using a standard data processor clause without amendment is unlikely to be appropriate, not least because it will usually restrict the use of that data for the processor's own purposes.

Likely Requests

Approaches from third parties, including local authorities, are likely to take one of two forms – audit/assurance and requests for contract variation.

1. Audit/Assurance Questionnaires

GDPR includes stronger obligations around governance and due diligence. There is a greater expectation that due diligence will be carried out before either appointing data processors or entering into data sharing relationships, and that audits will be carried out during the contract term to monitor compliance.

It is therefore understandable that local authorities may ask for assurances around data use and the school's GDPR readiness at this stage. However, the questionnaires which are currently being used do not tend to be fit for purpose as they often assume that the recipient acts solely as a data processor and do not reflect the complexity of the data sharing arrangements which are in place.

Audit questionnaires are particularly problematic when the school is asked to confirm whether it will “only act on written instructions from the local authority” or that it does not use personal data for its own purposes. Unless the scope of the questionnaire is clearly limited to specific processing in respect of which the local authority is the data controller, it can be hard to answer this type of question with a yes/no answer.

It should also be borne in mind that an audit/assurance questionnaire alone will not satisfy GDPR requirements, which require a written contract to be put in place. Although some organisations may try to rely on a signature on the questionnaire it is not a formal contract and it is likely therefore to be the precursor to a request for a contract variation.

2. Contract Variation

As noted above, large organisations typically try to create a “standard” contract variation which is sent to everyone they have contracts with, without consideration

of the specific features of each relationship. These can take several forms, either a “Data Protection Addendum” which sits alongside the existing contract, a contract variation which expressly amends certain provisions, or a new contract which replaces the old contract in its entirety.

Rather than signing this sort of document, where the agreement to be varied is the National Schools and Colleges Contract, we have generated a template version of Schedule 6 to incorporate appropriate terms into the contract. More detailed comments on this are set out below.

For contracts which are not based on the National Schools and Colleges Contract it would be possible to adapt the wording in the template Schedule 6. However, advice should be taken in respect of the most appropriate way to build this in to the contract as each contract may require a slightly different approach.

We believe this Schedule 6 wording is preferable to alternatives for the following reasons:

- A blanket statement that the authority is a data controller and the school is a data processor is incorrect. The explanations set out above could be provided to the authority to make this point.
- An obligation that personal data is only processed in accordance with the instructions of the authority is problematic unless this is very clearly limited to specific data processing activities and does not prevent use of the same data for other purposes by the school.
- An obligation to return or destroy all copies of the personal data on termination may be problematic if the school would need to retain the same data for its own purposes as data controller.
- Restrictions on the use of sub-processors or the transfer of data outside the EEA should be limited so that they only apply to specific processing activities. They should not restrict the operations of the school when it acts as a data controller.

Annex 7.2 Generic National Schools and Colleges Contract Template

The Agreement to vary the National contracts template is based on the standard variation to the National Schools and Colleges Contract - Schedule 6 format. See Annex 11.1.

The GDPR specific wording has been included in box 1 of the template is as follows:

- Paragraph 1 incorporates a new definition of data protection legislation. Because there are a number of matters which need domestic implementation, and because GDPR will not be directly applicable in the UK after Brexit, it will be supplemented by additional domestic legislation which is currently being considered by Parliament. This definition incorporates that legislation and deals with Brexit.
- Paragraphs 2 and 4 replace the reference to the Data Protection Act 1998 with the new definition of Data Protection Legislation, with the intention of keeping the change as simple as possible.
- Paragraph 3 again replaces the Data Protection Act 1998 definition with the new defined term. It also removes the reference to “respective registrations”. The need to “register” details of an organisation’s processing with the Information Commissioner has been removed by GDPR so this reference has been replaced with a reference to ensuring that any disclosures are permitted by law (which is particularly important for public sector data sharing), and that appropriate transparency information has been given.

These four paragraphs constitute the minimum variation required to replace obsolete wording in the original contract so that it actually reads correctly in light of the legislation changes. These paragraphs do not significantly alter the responsibilities or liabilities of either party. For that we’ve suggested different ways that a school might use the optional clause described below.

Optional Clause

Having included paragraphs 1-4, an additional optional clause (paragraph 5) can then be added to Schedule 6. This adds more detail around the respective responsibilities of each party than is in the current version. The existing wording simply states that each party will fully comply while the optional wording sets out much more detail about specific compliance requirements.

This approach is a more significant variation, rather than simply updating the contract. The majority of the changes apply equally to both parties, rather than favouring one party over the other.

These optional clauses should be used where the local authority has indicated that it wants to incorporate data processor clauses or to upgrade the level of protection above and beyond what is in the existing contract.

In order to use this clause there are two options:

- Use the full clause (whole of paragraph 5); or
- Include some or all of clauses 8.15 to 8.18 but not clause 8.19.

Clause 8.19 should not be used as a standalone clause because in isolation it does not cover off the GDPR data processor requirements in full. However, it does cover off everything if used in conjunction with the other clauses and the provisions which are already in the contract. This clause would not be required if the authority accepts that the school does not act as a data processor for it, but will give it the protection it is looking for if it insists that processing does take place.

Clauses 8.15 to 8.18 include wording which is not mandatory in data sharing agreements, but which could be included as a matter of good practice. They give greater clarity about the steps which both parties are expected to take to ensure compliance with GDPR and to assist the other's compliance efforts.

- Clause 8.15 covers security. There is a direct obligation on data controllers to meet these standards in any event so the main impact of including this rather than relying on clause 8.11 is simply to give local authorities comfort that schools are doing the right things. In return schools ask for the same commitments from LAs
- Clauses 8.16 and 8.17 cover confidentiality and assistance with compliance. These would be required in contracts between data controllers and data processors and although they are not strictly speaking required here, they make sense in a data sharing context and again they will give comfort to legal departments who are expecting to see this wording.
- Clause 8.18 is a data security breach notification provision. Again this is a reciprocal provision. The notifications required by Schedules 1 and 4 of the National Schools and Colleges Contract are one way only and do not include security breaches. However, it is advisable to improve that position with this reciprocal provision more suitable for a data sharing scenario as both parties will be affected by the tight timescales for notifying both the regulator and affected individuals if a personal data breach takes place.

Clause 8.19 sets out the position if one party processes data on behalf of the other. Whilst this is expected to be the exception to the rule for all the reasons explained above, including some basic protection will give local authorities comfort that the issue is covered off. The clause only applies in respect of specific, agreed, processing activities and reflects the fact that the same data is likely to be used for each party's own purposes as well as the agreed data processing.

This clause does not cover the issues which have already been covered on a reciprocal basis in the other optional clauses. It also does not cover the audit rights required by GDPR because the authority's access rights are already picked up in clauses 8.3 and 8.5. If this clause is adapted for use in conjunction with other agreements, those agreements will need to be reviewed to see whether any additional wording is required.

Annex 8.1 Data Protection Advisory Visit Report

ICO Data Protection Advisory Visit Feedback

Green Park Academy,

Summer Term, 2018

Key findings & recommendations

Good practice

We noted some good practice as a result of our visit to Green Park Academy and were encouraged to learn that some steps to minimise data protection risks have already been taken. Examples worthy of note are:

- There is a designated member of staff to handle SAR's;
- There is culture of data protection responsibility across the school led by a GDPR team, with staff keen to realise GDPR compliance. This includes privacy awareness notices across the school;
- There is an ongoing training programme in place for all staff and governors;
- Staff and students sign an acceptable use policy;
- The assignment of role specific access to Green Park Academy systems and
- Green Park Academy use an external provider to destroy manual records and oversee this practice on site.

Development areas

During the day, we also noted procedures and practices where we believe there is an opportunity to improve on current arrangements. We have commented on these below and made some suggestions as to how they may be improved.

Observations	Suggestions
1. Fair Processing Although a privacy notice has been provided to parents, relating to children's rights, a privacy notice has not been provided directly to children. Under the General Data Protection Regulations (GDPR), children are entitled to the same	It is noted that Green Park Academy are intending to provide fair processing information to all students by September, and Green Park Academy are encouraged to ensure this is done as soon as is practicably possible. Green Park Academy should also provide fair processing

<p>right to fair processing information as adults.</p>	<p>information in an age-appropriate format for children. Further guidance on children and the GDPR is here. The Department for Education Privacy Notice Guidance can be found here.</p>
<p>2. Lawful Bases</p>	
<p>The lawful basis relied upon for processing is not clear for each data set (for example, a data set may be 'full name' or 'national insurance number'). The lawful basis is further not linked to the relevant purpose for processing.</p>	<p>Green Park Academy should ensure the single GDPR Article 6 condition being relied upon for each data set processed is clearly documented. Where more than one lawful basis is applicable to processing, Green Park Academy should select the most appropriate basis to rely upon. The ICO template for 'documentation' may aid Green Park Academy in identifying the appropriate lawful basis for each data set.</p> <p>Green Park Academy should be clear in their privacy notice about where they rely on each lawful basis for processing, and link this to the purpose for processing.</p>
<p>3. Special Category Data</p>	
<p>Where Green Park Academy collect special category data, a lawful basis for processing under Article 9 of the GDPR has not been identified. Processing such data is prohibited under the GDPR, except where a basis for processing under Article 9(2) is identified.</p>	<p>Green Park Academy should identify an appropriate basis for processing special category data under article 9(2) of the GDPR. Where an appropriate basis under Article 9(2) cannot be identified then processing of this data should not take place.</p>
<p>4. Retention Periods</p>	
<p>Under Article 14(2)(a) of the GDPR, Green Park Academy are responsible for ensuring their retention periods form part of their fair processing information.</p> <p>The privacy notice in place for student data indicates that retention periods are in line with the Information Management Toolkit for Schools, but does not define what those retention periods are. This means that data subjects may not be aware of the length of time that their data will be held.</p>	<p>To comply with their obligations under article 14(2)(a) of the GDPR, Green Park Academy should update their privacy notice to include either:</p> <ul style="list-style-type: none"> a) the retention period for each category of information, or; b) a link to the Green Park Academy retention schedule

5. Storage Limitation	
<p>Green Park Academy are considering retaining some student data indefinitely (such as name and date of birth). This would fall outside of the retention periods adopted and used by Green Park Academy, and may therefore not meet the school's requirement to provide fair and transparent processing information.</p> <p>Such indefinite processing also increases the risk of breaching Article S(l)(e) of the GDPR - The 'Storage Limitation' principle.</p>	<p>Information should not be held for longer than the Green Park Academy retention schedule as a standard practice. Where this practice does occur as an exception, the reason for processing information outside of retention schedules should be documented, a compelling purpose and lawful basis must be satisfied, and data subjects should be notified. If Green Park Academy are considering holding personal data indefinitely, the GDPR dictates that you can only do this for the purposes of:</p> <ul style="list-style-type: none"> • archiving purposes in the public interest; • scientific or historical research purposes; or • statistical purposes.
6. Right to Erasure	
<p>Under Article 17 of the GDPR individuals have the right to erasure of personal data in certain circumstances (sometimes known as the 'right to be forgotten'). A response to a request for erasure would need to be made within one month. Green Park Academy do not currently have a process in place to comply with this obligation should such a request be made.</p>	<p>Green Park Academy should create a formalised process for handling a request for erasure, and consider whether this process could form part of their data protection training programme.</p>
7. SAR Procedures	
<p>Although there is a SAR procedures document in place, there is no detailed guidance for staff in recognising a SAR.</p> <p>There was some confusion as to whether SAR requestors could be asked to put their request in writing. Under the GDPR, a SAR can be made either verbally or in writing (including via social media), and can be made to any part of the organisation.</p>	<p>Green Park Academy should ensure that all staff are able to effectively recognise a SAR by producing guidance for staff to understand how to handle such a request. This guidance should be included in the SAR procedures document.</p> <p>Green Park Academy should ensure that they have a process for handling a verbal SAR. Whilst it would be acceptable to invite requestors to complete a standard form, Green Park Academy cannot insist that requests are made in writing. It would be good practice for Green Park Academy to have a policy for recording details of the requests received, particularly those made by telephone or in person.</p>

8. SAR Reporting	
<p>Green Park Academy confirmed that where a SAR has exceeded the statutory time limit, this would be reported to the most senior level (governors). However, this process is not detailed in the SAR procedures document.</p>	<p>Green Park Academy should document the process for SAR reporting to governors in the SARs procedures document. This should include any SAR's that have exceeded the statutory time limit.</p>
9. Data Sharing	
<p>Green Park Academy do not have a clear process for dealing with one- off requests for data sharing, although it is noted that such requests would be handled through a designated safeguarding officer. There is also no evidence of a process outlining how data sharing agreements are handled. This could increase the likelihood of information being inappropriately disclosed to a third- party.</p>	<p>The process for handling one off requests for data sharing should be formally documented, along with the process for handling data sharing agreements. The ICO guidance on data sharing can be found here.</p>
10. Physical Security - Access to cabinets	
<p>Teachers have lockable cupboards in their classrooms. Keys are not stored on-site, but are taken home with the teacher. This is the same for non-teaching staff, as there are lockable cupboards in each office. It is noted that the facilities site team have master keys and are available at all times.</p>	<p>In order to improve key security and ensure accessibility at all times, staff should not take keys home with them. It would be advisable to use a key safe for the central storage of cabinet keys. If Green Park Academy choose to use a key safe in future, the code(s) should regularly be changed.</p>
11. Physical Security - Windows	
<p>Whilst on site we observed that office doors were locked when staff were not present. However, we also observed that windows were wide open, and part of the site has a flat roof next to office windows. This leaves the office at risk of intruders, and potentially places personal data at risk.</p>	<p>Green Park Academy should consider implementing appropriate measures to ensure that all accessible windows are secure. For example, through the use of window bracelet hinges.</p>
12. Removable Media	
<p>Green Park Academy are considering whether it would be appropriate to use encrypted USB devices, to allow staff to take information home to work on. There is currently a lack of end point control on USB ports in the school. USB devices could be used to download personal data, and this potentially puts the organisation at higher risk of a data</p>	<p>Using removable media to import/export personal or confidential data for the purposes of homeworking is not recommended. Green Park Academy should refer to the National Cyber Security Centre's guidance, with particular reference to sections 7, 9 and 10 of the 10 Steps to Cyber Security guidance.</p>

<p>protection breach. The use of USB devices also carries the risk of introducing a virus into the IT network.</p>	<p>Green Park Academy should consider the introduction of technical end point control to prevent unauthorised devices accessing the IT network.</p>
<p>13. Home Working</p>	
<p>Green Park Academy do not currently have a home/remote working policy. The acceptable use policy contains one point relating to remote working, but this is not sufficiently detailed to provide a good level of assurance for home/remote working security.</p>	<p>Green Park Academy should create a home/remote working guide to ensure that staff working remotely are doing so as securely as possible. This could form part of the overarching data protection policy and/or the acceptable use agreement.</p>
<p>14. Compliance Monitoring</p>	
<p>The Green Park Academy data protection policy mentions that monitoring is the responsibility of the Data Protection Officer (DPO). They do not currently document or carry out any compliance monitoring in relation to data protection.</p>	<p>Green Park Academy should consider conducting regular spot checks such as 'clear desk sweeps' and formally record the results of this activity, to monitor compliance with the policy. They could also consider regular data protection audits. Details of such monitoring should be set out in more detail in the data protection policy. Green Park Academy should consider sharing the results of this compliance monitoring with the governors and any other appropriate audience.</p>
<p>15. Version Control</p>	
<p>Policies are reviewed annually and there is ratification and approval by the governing body. However, it is not clear where or when policies have been updated.</p>	<p>Green Park Academy should introduce version control on their policies to ensure that it is clear where and when changes have been made. They could also include the author and reviewer name, and ensure the current version number is clear on the document.</p>
<p>16. Secure Printing</p>	
<p>Green Park Academy have secure 'follow me' printing installed at the school, but not all printers have this technology available. Printers that do not have this technology are located in locked offices but are on the Green Park Academy network. During our visit, it was reported that the default print selection for computers in the locked offices had on occasion been set to the wrong printer.</p>	<p>The decision not to install "follow me" printers across the school should be formally documented. Green Park Academy should consider and document further controls that can be put in place to reduce the risk of a data breach through unsecured printing.</p>

Green Park Academy reported that they had considered installing 'follow me' printing across the school, but that it was not deemed feasible due to cost.	
17. Clear Screens	
Screens lock automatically after 45 minutes and staff are required to lock their screens when they are left unattended, as part of their acceptable use agreement. Green Park Academy considered that setting the automatic lock at a time less than 45 minutes could disrupt classroom lessons.	Green Park Academy should consider whether they can alter the timings on the office based staff computers to lock after a shorter time period. This should be documented in the acceptable use policy.
18. Internet and E-mail Restrictions	
Rules governing the use of internet and e-mail are included in the acceptable use agreement signed by students, but is not included in the acceptable use agreement for staff.	Green Park Academy should consider adding internet and e-mail restrictions to the acceptable use agreement with staff, similar to that currently used for students.
19. Data Processors	
Green Park Academy have an external IT provider, the London Grid for Learning (LGfL), who act as a data processor, and host their servers on site. Green Park Academy use an external provider to destroy manual records and oversee this practice on site. They also use an external provider (EOS) to destroy electronic hardware. Green Park Academy have not visited the site of LGfL or EOS to audit practice in line with their obligations as a data processor. It is not clear that the right to audit has been included in the contracts with processors.	Green Park Academy could consider carrying out a visit to audit LGfL and EOS under the terms of their agreement, to seek assurance of processing practices. They should ensure this requirement is documented in the contract with all data processors.
20. Destruction	
Some records are destroyed in small volumes internally, with shredders available for staff. It was noted that most shredders were cross-shred, however one shredder used by some non-teaching staff was a straight-cut shredder and this is considered less secure. The information destroyed in this way is stored on-site before it is sent for recycling.	<p>Green Park Academy should consider reviewing their internal destruction processes to ensure all shredders used to destroy personal information are cross - shred.</p> <p>Green Park Academy could also consider how the information destroyed internally could be recycled more securely.</p>

21. Training

All staff have received data protection training specific to the requirements of GDPR, with further refresher training scheduled for September. The training covers records management and security guidance, but ICO auditors did not see evidence of breach reporting or requests for personal data training.

The DPO has attended training relevant to their role.

Green Park Academy have planned to carry out a self-assessment on data protection understanding in September, but had not considered other objective measures to assess whether staff have digested and understood the training provided.

Green Park Academy should consider incorporating breach reporting and requests for personal data into their training programme. They could also consider whether any staff would benefit from specialised training relevant to their role, for example, the DPO attending training on SAR handling.

Green Park Academy could also consider the use of an 'assessment' style follow-up to training to assess understanding, and keep a record of training attended. This could be reported to the governing body as part of ongoing monitoring. This was briefly discussed on site, and Green Park Academy were considering whether they could use 'survey monkey' to carry out such an assessment. It should be noted that survey monkey currently host data outside of the European Economic Area (EEA). Green Park Academy should ensure compliance with Chapter V of the GDPR - "International Transfers" - in this instance. The ICO guidance on international transfers can be found [here](#).

Useful resources

In addition to the ICO guidance provided elsewhere within this report, we would like to draw Green Park Academy's attention to the following which may be of assistance:

- a Guide to the GDPR;
- a GDPR FAQs document;
- a new advice service helpline for small organisations;
- a '12 steps to take now' graphic;
- Lawful basis interactive guidance tool;
- Getting it right: a brief guide to data protection for small businesses (pdf);
- Getting it right: small business checklist (pdf);
- Personal information online: small business checklist (pdf);
- A practical guide to IT security: ideal for the small business (pdf);
- A practical guide to IT security: ideal for the small business (Welsh language) (pdf);
- Training checklist for small and medium-sized organisations (pdf);
- Outsourcing - a guide for small and medium-sized businesses (pdf); and
- Collecting information about your customers: small business checklist (pdf).

We also recommend that Green Park Academy use our SME Data Protection Self-Assessment Toolkit to assess in more detail their compliance with data protection legislation and find out what they need to do to improve.

Finally

ICO staff were pleased to see that Green Park Academy are taking a proactive approach to developing an understanding of data protection concerns. We hope that the opportunity to discuss the various issues with us and the guidance provided within this report, will enable Green Park Academy to raise awareness about data protection matters and improve current practice, policies and procedures. Finally, to keep up to date with the work of the ICO, Green Park Academy may wish to subscribe to the ICO's eNewsletter.

Annex 9.1 School Data Breach – Case Study

Case Study – School Data Breach

A member of staff in a school sent an email in error to an unknown recipient which contained private information relating to another member of staff. The email address had been mis-spelt by the sender and forwarded to an incorrect address. No response was received from the recipient's address and there was nothing to indicate that the email had been read (the email was sent with a read receipt).

The member of staff responsible for sending the email immediately spotted the error and informed senior management. The intended recipient was also told about the matter and an apology made.

The breach was reported to the ICO within 24 hours.

ICO Response to Data Breach

I am writing further to your data security breach notification regarding the sending of an email contained personal data relating to a member of staff to an incorrect email address affecting one individual.

Thank you for the information you have provided. I have attached a copy of the information we have recorded about the incident. If you believe that any of the information we have recorded is incorrect you should tell us as soon as possible.

The requirements of the Data Protection Act 1998 (the DPA)

As you may be aware, the DPA requires that data controllers have in place appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Our Decision

We have considered the information you have provided and we have decided that no further action by the ICO is necessary on this occasion. This decision is based on the information we have recorded about the breach.

The reasons for our decision are as follows:

- You have advised that only one individual has been affected;
- The email is likely to contain some sensitive personal data and has the potential to cause damage or distress to the individual. The affected individual

has been informed of the incident and has expressed some concern in case the information should fall into the wrong hands. It is noted that in this instance, it is not known whether the email address used is active and whether the email has been read.

- A further email has been sent to the recipient to ask that the original email is deleted and to request confirmation of this, however no response has been received and the read receipt from the original email has not been activated at this time.
- The information has been potentially disclosed to one recipient and also relates to one individual, there is no evidence that the information has been further disseminated. In view of the above, the disclosure would not be considered to be significantly detrimental;
- You have advised that incorrect email address was used due to this being provided orally and the failure to check that the correct email address was being used; in this respect, the breach can be attributed to human error
- It is welcomed that you have identified that a checking process should be in place to verify the accuracy of email addresses that are being used; you have advised that this will no longer be done verbally
- You have advised that members of staff received mandatory data protection training as part of the induction process

However, we recommend that you investigate the causes of this incident to ensure that you understand how and why it occurred, and what steps you need to take to prevent it from happening again.

In particular, we recommend that you consider:

- Establishing an appropriate checking mechanism as soon as possible with a view to reducing a similar occurrence. Consideration should be given to the accuracy of the data being used, although it is noted that staff are asked to review contact details annually and immediately advise your organisation of any changes;
- Review the content of your DPA training to ensure that sufficient practical guidance is given to staff in how to comply with the DPA. Also consider your methods of control, delivery and monitoring of such training and of ensuring staff who deal with personal data complete this. This training should also be tailored to specific roles;
- The ICO recommends, as good practice, that refresher training is carried out annually. However, the ICO also recognises that some organisations may be restricted by available resources but would recommend that, in such cases, refresher training does not exceed two years.

Please note that we may make additional enquiries if we become aware of new information which affects the circumstances of this case.

Thank you for reporting the incident. Further information and guidance relating to data security breach management is available on our website at:

https://ico.org.uk/media/fororganisations/documents/1562/guidance_on_data_security_breach_management.pdf

Annex 10.1 Safeguarding Myth-Busting

Myth-busting guide to information sharing

Sharing information enables practitioners and agencies to identify and provide appropriate services that safeguard and promote the welfare of children. Below are common myths that may hinder effective information sharing.

Data protection legislation is a barrier to sharing information

No – the Data Protection Act 2018 and GDPR do not prohibit the collection and sharing of personal information, but rather provide a framework to ensure that personal information is shared appropriately. In particular, the Data Protection Act 2018 balances the rights of the information subject (the individual whom the information is about) and the possible need to share information about them.

Consent is always needed to share personal information

No – you do not necessarily need consent to share personal information. Wherever possible, you should seek consent and be open and honest with the individual from the outset as to why, what, how and with whom, their information will be shared. You should seek consent where an individual may not expect their information to be passed on. When you gain consent to share information, it must be explicit, and freely given. There may be some circumstances where it is not appropriate to seek consent, because the individual cannot give consent, or it is not reasonable to obtain consent, or because to gain consent would put a child's or young person's safety at risk.

Personal information collected by one organisation/agency cannot be disclosed to another

No – this is not the case, unless the information is to be used for a purpose incompatible with the purpose for which it was originally collected. In the case of children in need, or children at risk of significant harm, it is difficult to foresee circumstances where information law would be a barrier to sharing personal information with other practitioners.

The common law duty of confidence and the Human Rights Act 1998 prevent the sharing of personal information

No – this is not the case. In addition to the Data Protection Act 2018 and GDPR, practitioners need to balance the common law duty of confidence and the Human Rights Act 1998 against the effect on individuals or others of not sharing the information.

IT Systems are often a barrier to effective information sharing

No – IT systems, such as the Child Protection Information Sharing project (CP-IS), can be useful for information sharing. IT systems are most valuable when practitioners use the shared data to make more informed decisions about how to support and safeguard a child.

Annex 11.1 Agreement to vary the National Contracts

SCHEDULE 6

AGREEMENT TO VARY THE NATIONAL CONTRACTS

PARTIES TO THE AGREEMENT

THIS AGREEMENT is made on____(*insert date*) **BETWEEN**____("the Purchaser") and____("the Service Provider") and is supplemental to the National Contract dated____and made between the parties to this Agreement.

1. The Contract is varied as detailed below:

1. A new definition of "Data Protection Legislation" shall be included as follows:

"(i) unless and until the GDPR is no longer directly applicable in the UK, the General Data Protection Regulation ((EU) 2016/679) ("GDPR") and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998."

2. Clause 8.9 shall be amended to read:

"A policy of open access for Learners to their own records will be employed, subject to the relevant Regulations in Data Protection Legislation and the relevant Records Regulations."

3. Clause 8.11 shall be amended to read:

"Both parties may collect and maintain information which will be processed manually or by computer and used in accordance with their respective needs under the terms of the Data Protection Legislation. Both parties undertake to fully comply with the requirements and principles of Data Protection Legislation and information held by either party may be disclosed to other agencies where permitted by law and in accordance with any applicable transparency requirements."

4. Clause 9.2 shall be amended to read:

"Both parties will have a policy on confidentiality which accords with the principles of the Data Protection Legislation and will have mechanisms in place to ensure full compliance."

5. New clauses 8.15 to [8.19] shall be inserted as follows:

"8.15 Notwithstanding the generality of clause 8.11, each party shall ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate pseudonymising and encrypting personal data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to personal data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

8.16 Each party shall ensure that all personnel who have access to and/or process personal data for the purposes of this Agreement are obliged to keep the personal data confidential.

8.17 Each party shall give the other reasonable assistance, at the requesting party's cost, in responding to any request from a data subject and in ensuring compliance with its obligations under Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators.

8.18 Each party shall notify the other promptly on becoming aware of any breach of security relating to personal data received from or processed on behalf of the other party under this Agreement.

[8.19 Notwithstanding each party's obligations under clause 8.11, to the extent that the parties agree that one party (the "data processor") will process personal data on behalf of the other (the "data controller") in connection with this agreement, the data processor shall, in relation to any such processing:

8.19.1 carry out that processing only on the written instructions of the data controller;

8.19.2 at the written direction of the data controller, delete or return personal data

processed solely on behalf of the data controller (and copies of such personal data) on termination of the agreement unless required by law to store the personal data;

8.19.3 not transfer such personal data outside the European Economic Area for the purposes of the processing without the prior written consent of the authority; and

8.19.4 not appoint a third party processor of personal data in respect of such processing without the prior written consent of the Authority.]"

2. The Contract shall as from _____ be deemed to have been varied to give effect to this Agreement and subject to such variation shall continue in full force and effect.

3. Parties to the Agreement

PURCHASER:	<input type="text"/>		
Name:	<input type="text"/>		
Designation:	<input type="text"/>		
Signature:	<input type="text"/>	Dated:	<input type="text"/>
PROVIDER:	<input type="text"/>		
Name:	<input type="text"/>		
Designation:	<input type="text"/>		
Signature:	<input type="text"/>	Dated:	<input type="text"/>

This schedule is a generic schedule for use when applicable on either the National Residential, Fostering or Schools and Colleges Contract.

Annex 12.1 Lead Contributors

This toolkit has been put together as a result of significant contributions and collaboration between a number of individuals representing many perspectives. The Department for Education is particularly grateful to people from the following organisations for giving their support:

Organisation
Information Commissioner's Office
Oxford Diocesan Schools Trust
Ocean Learning Trust
Independent School's Bursars Association
Ninestiles Academy Trust
Ark Academy Trust
Hockliffe Lower School
Broadmead Lower School
Bedford Catholic Schools (SFAAT)
South West Grid for Learning
Dobcroft Infant School
Edith Cavell Primary School
Beaundesert Lower School
The Independent Schools Council
Queen Elizabeth High School, Lincs
Boston High School
Flitwick Lower School
Edith Cavell Primary School
Thomas Johnson Lower School
Defend Digital Me

Organisation
Lincolnshire County Council
Capita SIMS
GDPR in Schools (GDPRiS)
CBICT Ltd
Assembly
TheTrustBridge
Michelmores
National Association of Independent Schools & Non-Maintained Special Schools (NASS)
National Centre for Cyber Security
Information and Records Management Society



Department
for Education

© Crown copyright 2018

This publication (not including logos) is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

To view this licence:

visit www.nationalarchives.gov.uk/doc/open-government-licence/version/3

email psi@nationalarchives.gov.uk

write to Information Policy Team, The National Archives, Kew, London, TW9 4DU

About this publication:

enquiries www.education.gov.uk/contactus

download www.gov.uk/government/publications

Reference: DFE-00119-2018



Follow us on Twitter:
[@educationgovuk](https://twitter.com/educationgovuk)



Like us on Facebook:
facebook.com/educationgovuk