Records Management and Data Security

The Data Protection Act 2018 is designed to protect the privacy of individuals. It requires that any personal information about an individual is processed securely and confidentially.
This includes both staff and pupils. How a school obtains, shares and uses information is critical, as personal data is sensitive and private.

Staff need to know and understand

- How to manage, keep and dispose of data
- The school's procedures in relation to pupil records, email, social media, taking photos in schools, mobile technology and the school website
- When they are allowed to share information with others and how to make sure it is kept secure when shared.

The school collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations. Once personal information about pupils, parents and teachers has been gathered, it must be kept secure.

All members of staff will have signed a code of conduct, which includes guidance on the management and security of data and information, as well as the use of email, social networks, mobile phones, taking photos in school.

Confidentiality

Working in the school environment means having access, in a variety of ways, to information that must be regarded as confidential. As a general rule, all information received in the course of employment or whilst being engaged by the school, no matter how it is received, should be regarded as sensitive and confidential. Employees should use their discretion regarding these matters, and should seek further advice from their line manager or the Headteacher, as appropriate.

All workers and volunteers must be aware that they may be obliged to disclose information relating to child protection issues and should make it clear to the individual either that confidentiality cannot be guaranteed and/or decline to receive the information and direct them to a more appropriate colleague.

Discussions outside work

Employees should have regard to potential difficulties which may arise as a result of discussions outside work. While it is natural to talk about work at home or socially, employees should be cautious about discussing specific and sensitive matters and should take steps to ensure that information is not passed on. Employees should be particularly aware that many people will have a direct interest in the School and even the closest of friends may inadvertently use information gleaned through casual discussion. In particular, employees need to understand the implications of discussions on social networking sites

Data Protection Officer

Our school's DPO is

Managing pupil records

The pupil record should be seen as the core record charting an individual pupil's progress through the Education System. The pupil record should accompany the pupil to every school they attend and should contain information that is accurate, objective and easy to access. The information that should be kept in the pupil record is listed in the Information Management Toolkit for Schools.

Recording information

Pupils have a right of access to their educational record and so do their parents under the Education (Pupil Information) (England) Regulations 2005. Under the Data Protection Act 1998 a pupil or their nominated representative has a right to see information held about them. This right exists until the point that the file is destroyed. Therefore, it is important to remember that all information should be accurately recorded, objective in nature and expressed in a professional manner.

Responsibility for the pupil record once the pupil leaves the school

The school which the pupil attended until statutory school leaving age is responsible for retaining the pupil record until the pupil reaches the age of 25 years.

Storage of pupil records

All pupil records should be kept securely at all times. Paper records, for example, should be kept in lockable storage areas with restricted access, and the contents should be secure within the file. Equally, electronic records should have appropriate security.
Access arrangements for pupil records should ensure that confidentiality is maintained whilst equally enabling information to be shared lawfully and appropriately, and to be accessible for those authorised to see it.

Data security measures

Both manual and digital records need to be secure. The level of security should reflect the potential harm that could result from the lost or misuse of the data. Memory sticks perhaps need to the most consideration as they are very easy to lose. Either avoid the use of memory sticks completely or ensure they are password protected and fully encrypted.

Employees have a responsibility to make sure sensitive information is used and stored securely. They should:

- make sure filing cabinets are kept locked when unattended;
- make sure sensitive information is not left on desks or the photocopier/fax/printer;
- make sure papers are not left lying around at home or in the car. If confidential materials or paperwork are taken away from the school, precautions must be taken to ensure they are not accessible to third parties;
- make sure appropriate steps are taken to keep track of files which are on loan or being worked on i.e. a record of the date sent and the recipient's name and position;
- make sure, if it is necessary to supply personal files through the external mail, these are sent recorded delivery;
- make sure copies of faxes and emails are stored securely;
- make sure steps are taken to ensure that private/confidential telephone calls/conversations are not overheard;

- make sure meetings where sensitive or confidential information is being discussed are held in a secure environment;
- make sure confidential paperwork is disposed of correctly either by shredding or using the confidential waste facility;
- make sure personal data is not used for training or demonstration purposes where fictional data can be used;
- make sure line managers comply with the procedures for the storage and sharing of information relating to individuals' performance management reviews.

Employees have a responsibility to make sure computer data is used and stored securely.
They should:

- make sure computer data is not left exposed to others' view when unattended, or when using computers for sensitive data where other employees may have sight of such data – screen savers should be used where appropriate ;
- make sure machines are switched off when leaving the office;
- passwords must not be disclosed to other colleagues unless authorised by an appropriate manager or required by the school;
- make sure sensitive data is not stored on public folders;
- staff should be familiar with the security of email/internet systems;
- make sure computer discs are wiped clean correctly before being reused;
- make sure any user IDs and passwords remain confidential unless express permission has been given by management to disclose them;
- computer files should be backed up regularly and not solely saved to the hard drive.

Eight Things You Need to Know About E-mail

E-mail has replaced telephone calls and memos
As communicating by e-mail is quick and easy, many people have replaced telephone conversations and memos with e-mail discussions. However, the language in which e-mail is written is often less formal and more open to misinterpretation than a written memo or a formal letter. Remember that e-mail should be laid out and formulated to your school's standards for written communications.

E-mail is not always a secure medium to send confidential information
You need to think about information security when you send confidential information by e-mail. The consequences of an e-mail containing sensitive information being sent to an unauthorised person could be a civil penalty (up to £17.5 million) from the Information Commissioner or it could end up on the front page of a newspaper. In addition, a school might also be sued for damages by an aggrieved data subject. Confidential or sensitive information should only be sent by a secure encrypted e-mail system. Never put personal information (such as a pupil's name) in the subject line of an e-mail.

E-mail is disclosable under the access to information regimes
All school e-mail is disclosable under Freedom of Information and Data Protection legislation. Be aware that anything you write in an email could potentially be made public.

E-mail is not necessarily deleted immediately
E-mails can remain in a system for a period of time after you have deleted them. You must remember that although you may have deleted your copy of the e-mail, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 or under the Data Protection Act 2018.

E-mail can form a contractual obligation
Agreements entered into by e-mail can form a contract. You need to be aware of this if you enter into an agreement with anyone, especially external contractors. Individual members of staff should not enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so.

E-mail systems are commonly used to store information which should be stored somewhere else
All attachments in e-mail should be saved into any appropriate electronic filing system or printed out and placed on paper files.

Employers must be careful how they monitor e-mail
Any employer has a right to monitor the use of e-mail provided it has informed members of staff that it may do so. Monitoring the content of e-mail messages is a more sensitive matter and if you intend to do this you will need to be able to prove that you have the consent of staff. If you intend to monitor staff e-mail or telephone calls you should inform them how you intend to do this and who will carry out the monitoring.

E-mail is one of the most common causes of stress in the work-place
Whilst e-mail can be used to bully or harass people, it is more often the sheer volume of e-mail which causes individuals to feel that they have lost control of their e-mail and their workload. Regular filing and deletion can prevent this happening.

Personal social networking sites

All employees of the school, individuals engaged by the school or individuals acting on behalf of the school from third party organisations (including governors) should bear in mind that information they share through social networking applications, even if they are on private spaces, may still be the subject of actions for breach of contract, breach of copyright, defamation, breach of data protection, breach of confidentiality, intellectual property rights and other claims for damages. Employees must therefore not publish any content on such sites that is inappropriate or may lead to a claim, including but not limited to material of an illegal, sexual or offensive nature that may bring the school or the local authority into disrepute.

It is totally unacceptable for any employee to discuss pupils, parents, work colleagues or any other member of the school community on any type of social networking site.
Reports about oneself may also impact on the employment relationship for example if an employee is off sick but makes comments on a site to the contrary.

Retention of pupil records

The School has adopted the Information Management Toolkit for Schools created by the IRMS (Information and Records Management Society) and adheres to its principles and guidance, including the retention schedule for school records. A full copy of the Information Management Toolkit is available on the School website.

You are violating the Data Protection Act if you keep data for any longer than it is needed.

Safe destruction of records

All records containing personal information, or sensitive policy information should be made either unreadable or unreconstructable.

- Paper records should be shredded using a cross-cutting shredder
- CDs / DVDs / Floppy Disks should be cut into pieces
- Audio / Video Tapes and Fax Rolls should be dismantled and shredded
- Hard Disks should be dismantled and sanded

Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in with the regular waste or a skip unless there is no other alternative.

Additional guidance and further reading

- EPHA website – dedicated page https://essexprimaryheads.co.uk/info-and-documents/data-protection/
- Staff Code of Conduct
- Data Protection Policy
- Data protection Toolkit for Schools – DfE August 2018
- Data protection guide for schools – EPHA July 2017
- Information Commissioner's Office https://ico.org.uk/
- ICO Data Protection guide for schools
- ICO guide to taking photos in schools
- Information Management Toolkit for Schools 2019

This briefing paper relates to records management and data security – to develop the staff understanding of data protection issues, follow up with the additional 7-minute staff meetings:

- Information sharing
- Data Protection Principles