

INFORMATION SECURITY POLICY

1. Introduction

The school's investment in the acquisition, storage and use of electronic and paper based information exists primarily to help provide the effective delivery of its services. This information is held about a variety of people and it is essential that the availability and confidentiality of accurate relevant information is maintained in a secure and legal environment.

2. Objective

The information security objective is to ensure that the school's information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

3. Policy

The purpose of this policy is to protect the school's information assets from all threats, whether internal or external, deliberate or accidental.

The key aims of the policy are to ensure that :

- Information is protected from unauthorised access
- Confidentiality of personal or sensitive information is assured
- Integrity of information is maintained
- Information is disposed of in a timely, appropriate and secure manner
- Legislative requirements and school policy and practices are observed
- Information security training is available to all relevant staff
- Appropriate monitoring and reporting processes are put in place to identify and act upon breaches of information security

4. Supporting Framework

In order to achieve this, the school will develop and maintain information security standards. These will be based on, but will not necessarily correspond in depth with, the British Standard on Information Security ().

Procedures, working practices and protocols will be developed, either as detailed in ISO 27001:2005 or as required by educational needs, to support this policy. Examples of measures to achieve the above are physical security, virus control and the use of passwords for access control. The development of any new system will include information security analysis and requirements as part of the initial specification.

5. Responsibilities

The school's Headteacher has direct responsibility for maintaining this policy and providing advice and guidance on its implementation.

All staff are responsible for policy implementation and for ensuring that as staff they adhere to the standards.

6. Implementation

This policy will be made available to all parents, guardians, staff (whether permanent or temporary) and governors.

The following guidelines are taken from the LEA Corporate Handbook for Information Security (see appendix I).

7. General Security

It is important that unauthorised people are not permitted access to school information and that we protect against theft of both equipment and information. This means that we must pay attention to protecting our buildings against unauthorised access.

- Do not reveal pin numbers or building entry codes to people that you do not know or who cannot prove themselves to be employees.
- If you don't know who someone is and they are not wearing some form of identification, ask them why they are in the building.
- Do not position screens on reception desks where they could be seen by members of the public
- Do not be afraid to challenge people who you do not recognise if they are not wearing an identity badge
- Lock secure areas when you are not in the office
- Beware of people tailgating you into the building or through a security door
- Do not let anyone remove equipment or records unless you are certain who they are.

Visitors and contractors in School buildings should always sign in a visitors book.

8. Confidentiality

Pupil Information

- Individual Pupil record folders are available to staff of the school, pupil's own parent or guardian and to new school on transfer.
- IEP's/PEP's/PSP's/Child Looked After Plans written by and available to parent/guardian of child, teachers & LSAs at school, professional support agency staff (eg social worker, behaviour advisor, Educational Psychologist etc)
- Risk assessment on pupils. Available to SENCO, Headteacher, School Staff, Support Professionals and Parent or Guardian
- Accident or Incident Reports on behaviour. Notes taken should be given to Class Teacher, SENCO or Headteacher for secure storage in the behaviour files. Available under Freedom of Information Act to appropriate personnel/parent or guardian of the individual pupil. Some key information may be entered onto the child's SIMs record for school use only.
- Observation Notes. Observations of a class, group or specified individual should only be done under the direction of the class teacher/SENCO/Head Teacher. Clear guidance on length of observations/type of observations and purpose will be given. No names should be recorded, only an initial to identify people. Word by word transcripts are not necessary. Notes taken should be given to the teacher in charge for secure storage. The observations are only used as evidence for SEN applications or ongoing assessment and will be destroyed as soon as a summary report is written.

- Informal notes and assessments done by Teachers as temporary recordings rather than a permanent addition to pupil records remain confidential for the use of the class teacher, SENCO and Head teacher only.

SEN Records/Information

All SEN records/files are kept locked in a filing cabinet. SENCO & Head Teacher are the only staff with access to this. Records are shared with teachers, LSA's and parents as appropriate.

Discussions

Discussions with parents or other adults concerning pupils will usually be with the class teacher or in the presence of the class teacher unless it is with the SENCO or Advisory Professional. A LSA may be requested to talk to a parent who needs to give the school information regarding their child and then report this to the class teacher. Adults who want to discuss a child whom they are not related to, should be directed to the Head Teacher.

Voluntary Staff working with pupils should only discuss them with school staff. Confidentiality outside school is very important.

Staff Relationships

Any staff room discussions about pupils, school matters or issues must remain confidential between school staff. This is particularly relevant when voluntary helpers are present. Staff meetings are confidential unless minuted.

Professional relationships are expected to be maintained at all times and clear communication between team members is essential. This includes a positive, focused discussion of any concerns or differences of opinion with other staff as they arise to resolve the problem. In the event of unresolved issues the Head Teacher or Senior Teacher will become involved to help solve the issue.

9. Security of Paper Records

Paper documents should always be filed with care in the correct files and placed in the correct place in the storage facility.

- Records that contain personal data, particularly if the information is sensitive should be locked away when not in use and should not be left open or on desks overnight or when you are not in the office.
- Always keep track of files and who has them
- Do not leave files out where others may find them.
- Where a file contains confidential or sensitive information, do not give it to someone else to look after.

Paper records should be disposed of with care. If papers contain confidential or sensitive information shred them before disposing of them. Particular care must be taken when selecting papers to be placed in a recycling bin.

9. Electronic software

- Prevent access to unauthorised people and to those who don't know how to use an item of software properly. It could result in loss of information.
- Keep suppliers CDs containing software safe and locked away. Always label the CDs so you do not lose them in case they need to be re-loaded.

- When we buy a license for software, it usually only covers a certain number of machines. Make sure that you do not exceed this number as you will be breaking the terms of the contract.

Guidance for your password are:

- Don't write it down
- Don't give anyone your password.
- Your password should be at least 6 characters
- The essential rules your password is something that you can remember but not anything obvious (such as *password*) or anything that people could guess easily such as your name.
- You can be held responsible for any malicious acts by anyone to whom you have given your password.
- Try to include numbers as well as letters in the password
- Take care that no-one can see you type in your password
- Change your password regularly, and certainly when prompted. Also change it if you think that someone may know what it is.

Many database systems, including SIMs, particularly those containing personal data should only allow a level of access appropriate to each staff member. The level may change over time.

- Lock your computer by using CTRL/ ALT/ DEL when you are away from it for any length of time.

10. Use of E Mail and Internet

- To avoid a computer virus arriving over the Internet, do not open any flashing boxes or visit personal websites.
- Do not send highly confidential or sensitive personal information via e mail
- Save important e mails straight away
- unimportant e mails should be deleted straight away.
- Do not send information by e mail which breaches the Data Protection Act. Do not write anything in an e mail which could be considered inaccurate or offensive, and cannot be substantiated

11. Electronic Hardware

- All hardware held within School should be included on the asset register.
- When an item is replaced, the register should be updated with the new equipment removed or replaced.
- Do not let anyone remove equipment unless you are sure that they are authorised to do so
- In non-secure areas, consider using clamps or other security devices to secure laptops and other portable equipment to desk tops.

Disposing of hardware.

Computers to be disposed of must be completely 'cleaned' before disposal. It is not enough just to delete all the files.

12. Home working guidance

In essence, if you work outside the school or at home, the guidance is the same as given above, However, you may need to consider these extra points. Information is more liable to be lost or stolen outside the office:

- Do not access confidential information when you are in a public place, such as a train and may be overlooked.
- Do not have conversations about personal or confidential information on your mobile when in a public place. Ensure that, if urgent, you have your conversation in a separate room or away from other people.
- If you use a laptop
 - Ensure that it is locked and passworded to prevent unauthorised access.
 - Make sure that you don't leave your laptop anywhere it could be stolen. Keep it with you at all times and secure it when you are in the school.
 - When working on confidential documents at home do not leave them lying around where others may see them; dispose of documents using a shredder.
 - *If you are using your own computer, ensure that documents cannot be accessed by others. When you have completed working on them, transfer them back to the school and delete them from your computer.*

Review

This policy will be reviewed biennially in line with our other policies or earlier if additional legislation requires it.

Glossary of legislation

The Data protection Act 1998

The Freedom of Information Act 2000

The Environmental Information Regulations 1992

The Human Rights Act 1998

The Regulation of Investigatory Powers Act

Copyright and Intellectual Property rights

The Computer Misuse Act