Moor End Community Primary School

Information Access and Security Policy

Purpose

This information access and security policy provides clear direction and support for information security that is applicable to all staff at all levels. The policy describes the means by which the school aims to preserve confidentiality, integrity and availability of data.

- Confidentiality: - information is accessible only to those authorised to have access.
- Integrity:- safeguarding the accuracy and completeness of information.
- Availability:- ensuring that authorised users have access to information when required.

It is acknowledged that the school has legal, statutory and contractual requirements with which it must comply. The school; complies with the rules of good information handling, known as the data protection principles and the other requirements of the Data Protection Act.

The Senior Manager in the school invested with overall responsibility for information security is the Head Teacher.

Specialist security advice will be sought where necessary.

This policy will be reviewed and updated every 2 years.

January 2019

Organisational Security

Allocation of responsibilities – An accurate inventory is maintained of all assets associated with information systems.
This is the responsibility of the ICT Coordinator and the Technician.

Each 'information asset' (eg computer) has an owner who is responsible for its day to day security. Information is classified according to its degree of sensitivity and confidentiality, indicating the need and priority for its protection and is labelled appropriately (lowest is all staff access; highest is Headteacher or Technician only, depending on nature). Each classification has defined procedures for copying, storage, transmission (eg post) and destruction.

Information Databases, documentation, manuals, plans, archived information
Software Application and system software
Physical Computer and communications equipment
Services Power, air conditioning

Printouts of details can be obtained from the main server by System Manager.

Personnel Security

This is the overall responsibility of the Headteacher.

Security in job responsibilities

Security responsibilities are clearly documented and where appropriate, addressed at the recruitment phase and included in contracts of employment. Personnel screening processes for permanent and temporary staff includes appropriate controls (e.g. availability of satisfactory references, confirmation of claimed academic and professional qualifications, independent identity checks) Staff sign a confidentiality agreement under their conditions of employment, which states they are bound by the policies the Governors have set in place.

Information security education and training

All staff receives appropriate training and regular updates in security policies and procedures. This includes training in security requirements, controls and legal requirements, as well as in the correct use of information systems. (e.g. log on procedures)

Responding to security incidents and malfunctions

A formal procedure exists for reporting and responding to security incidents, malfunctions and weaknesses. All staff are aware of their responsibilities to note and report such incidents to the ICT Coordinator as quickly as possible.
Recovery is carried out only by appropriately trained and experienced staff.
Users are made aware that, under no circumstances, should they try to prove a suspected security weakness in the system. This will be treated as misuse.
(Details of this can be found in Email and Internet use policy)

Physical and environmental security

This is the overall responsibility of the Headteacher

Secure areas

Areas in which critical or sensitive information is processed are physically secured to prevent unauthorised access, damage or interference. Control is achieved by conventional security procedures. Access to secure areas (if applicable) is controlled and restricted to authorised personnel only, with a pin number process in use.

Equipment security

Equipment is sited or protected to minimise the risk of theft, damage and power failure, this includes security marking and power surge protectors. Cabling is protected from interception or damage. Equipment is correctly maintained and serviced by the School Technician.

Off-site security

Equipment is not taken off site without permission. Where necessary and appropriate (ie teacher laptops) the details are kept in the schools stock book and the users are aware of the precautions to be taken.

Secure disposal or re-use of equipment

Appropriate arrangements are made for the secure disposal of media containing sensitive information. Confidential paper documents are securely disposed of (shredded). Storage devices containing sensitive information are destroyed or securely overwritten before disposal. All equipment containing storage media (e.g. hard disks) is checked to ensure that sensitive data and licensed software have been removed prior to disposal or re-use.

Protection against malicious software (viruses, etc)

Software licensing requirements are complied with and the use of unauthorised software is prohibited. Anti virus detection and repair software is installed and regularly updated. E-mail attachments, downloads and any files of uncertain origin on electronic media or downloaded are checked for malicious software before use. Appropriate back up and recovery procedures are in place. SOPHOS provides virus detection and is updated daily, all machines are checked when they log into the network.

Housekeeping and network management

Back up copies of essential information and software are taken regularly according to an appropriate schedule. These processes are regularly checked to ensure that they are effective. Controls are in place to ensure the security of data in networks and the protection of connected services from unauthorised access.
Curriculum network and Administration machines are backed up by Westfield daily.
Electronic mail

Guidelines exist for the appropriate and acceptable use of e-mail. All users are aware of these and sign an agreement to confirm this. (See separate policy and agreement)

Access control

This is the responsibility of the ICT Technician (System Manager)

Formal procedures are in place to control the allocation of access rights to information systems and services. Users have authorisation from the system manager and the level of access is appropriate for the purpose. User access rights are regularly reviewed, as people leave their access rights and their ID's are removed immediately. Privileges associated with each system and user are identified, allocated on a need to use basis and kept to a minimum.

Systems development and maintenance

This is the responsibility of the ICT Technician and Coordinator

Security issues are identified and considered at an early stage when buying new equipment. Input data is validated to ensure that it is correct and appropriate. Outputs and downloaded or uploaded data are checked for validity and integrity.

Compliance

Appropriate procedures are in place to ensure compliance with legal restrictions in the use of material in respect of which there may be Intellectual property rights, such as copyright, licenses etc. Software is usually supplied under a licence agreement that limits the number of machines it can be installed on. A rigorous system is in place to ensure these licences are adequate and up to date. Only the ICT Technician has rights to install new or additional copies of software.

Pupil use of systems

This is the overall responsibility of the ICT Coordinator

The school subscribes to the NAACE acceptable use policy. Parental consent is obtained annually for use of the Internet. All users' annually sign up to the Acceptable use Policy. Examples of all are in the relevant section.

Sanctions
Anybody found to be disregarding the rules agreed to in these policies will be sanctioned as below:-
1. Child talked to and problem pointed out.
2. Not allowed to access Internet/Intranet unsupervised.
3. Unable to use Internet/Intranet in school.

At each level Parents will be called in to discuss the breach with the Headteacher.