ICT Security Policy

Acorns School ICT Security Policy

This policy should be read in conjunction with the generic LEA policy for ICT security

Introduction

This information access and security policy provides clear direction and support for information security that is applicable to all staff at all levels of the organisation. 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 who is invested with overall responsibility for information security is the Headteacher.

Organisational Security

An accurate inventory is maintained of all the assets associated with information systems.
This is the responsibility of the school secretary.
Each 'information asset' (e.g. information system, database, etc) has an owner who is responsible for its day to day security.

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).

Equipment security

Equipment is sited or protected to minimise the risk of theft (including security marking), damage (e.g. fire, water, and impact).

Off-site security

Equipment is not taken off-site without authorisation. Where necessary and appropriate, equipment is logged out and back by (Deputy Headteacher). Equipment and media taken off the premises is not left unattended in public places.

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 (e.g. by shredding, incineration). Storage devices containing sensitive information are destroyed or securely overwritten (rather than using the standard delete function) prior to disposal.

Clear desk and screen policy

Business critical information is held in a fire resistant safe or cabinet, with copies stored securely offsite.
PCs and printers are not left logged on when unattended and are protected as appropriate by key locks, passwords or other controls when not in use. Users terminate active sessions and log off when out facility is afforded by password protected screen savers.

Protection against malicious software (viruses, etc.)

Software licensing requirements are compiled with and the use of unauthorised software is prohibited. Anti-virus detection and repair software is installed and regularly updated. Electronic mail attachments, downloads and any files of uncertain origin on electronic media or downloaded are checked for malicious software before use. Appropriate business continuity plans for recovery from attack are in place (e.g. data and software back-up and recovery arrangements).

Housekeeping and network management

Back-up copies of essential information and software are taken regularly according to an appropriate schedule. At least three generations of back-up information are retained for important applications and are stored with an appropriate level of physical protection at a sufficient distance to escape a disaster at the main site. Back-up media and restoration processes are regularly checked to ensure that they are effective.

Electronic mail

Staff understand their responsibility not to use e-mail in such a way as to compromise the good name of the school (e.g. defamatory e-mail, harassment, unauthorised purchasing). *Staff guidance appended*.

User password management

Users understand the need to keep passwords confidential and to avoid sharing them, keeping a paper record or recording them in a way that makes them accessible to unauthorised persons.

Systems development and maintenance

This is the responsibility of the ICT subject leader / Technician / Headteacher .
Security issues are identified and considered at an early stage when procuring or developing new information systems. Input data is validated to ensure that it is correct and appropriate. Outputs and downloaded or uploaded data are checked for validity and integrity.

Intellectual property rights (IPR)

Appropriate procedures are in place to ensure compliance with legal restrictions in the use of material in respect of which there may be IPR, such as copyright, design rights or trademarks. Software is usually supplied under a license agreement that limits the number of copies that can be made of the software. Controls are in place including: maintaining an appropriate inventory or asset register of software, maintaining proof of license ownership (e.g. licences, master disks, manuals, etc), controlling the number of users, carrying out checks that only authorised software is in use and applying sanctions against unauthorised copying of software.

Pupil use of systems

This is the responsibility of Class staff.
The school subscribes to the NAACE acceptable use policy as recommended by Lancashire County Council's Education and Cultural Services Advisory Team. Parental consent is obtained for use of the Internet. Pupils sign up to an acceptable use policy (sample appended).

	Notes	
1.	The Governing Body must ensure that the school implements an ICT Security Policy - this can either be the 'model' policy or the school can create an amended policy based upon the 'model'. This must be reviewed bi-annually and must include Email and Internet Use Policies for Staff and Pupils	Yes
2.	The Headteacher must nominate a System Manager This must be documented and included in the Scheme of Delegation approved by the Governing Body. It would not be unusual for the Headteacher to nominate themselves to act in this capacity, especially in small schools.	Yes
3.	The Headteacher must compile a census of data giving details and usage of all personal data held on computer and manually (as required under the Data Protection Act 1998) in the school, and file a registration with the Data Protection Registrar. Users should be periodically reminded of the requirements of the Data Protection Act, particularly the limitations on the storage and disclosure of information.	Yes

4.	The Headteacher should ensure that a copy of the relevant 'Rules for ICT Users' (*attached as Annex C1-C3*) is issued to all system users. This should include all relevant aspects of the ICT Security Policy and any other information on the use of facilities and techniques to protect the systems or data. This will include Inappropriate use of Email and the Internet Use of private hardware and software Access rights Equipment siting, room layout, physical security Appropriate use of the school facilities	Not comp lete
5.	The Headteacher should retain a record of; the access rights to systems and data granted to individual users; any amendments or withdrawal of these rights due to a change in responsibilities or termination of employment or starters/leavers; the training provided to each individual user.	Yes
6.	An inventory of all ICT equipment must be maintained and regularly updated as equipment is purchased / disposed of. The inventory must be checked and verified annually in accordance with the requirements of Financial Regulations.	Yes
8.	An inventory of all software and licence details must be maintained and regularly updated by the Systems Manager as software is purchased / disposed of. The inventory must be checked annually to ensure that the licences accord with installations.	Yes
9.	The Systems Manager should ensure there are clear procedures regarding installing, upgrading, repairing and disposal of equipment.	Yes
11.	The Systems Manager must ensure that a Backup strategy is agreed, documented and implemented. Clear instructions must be given to Users to ensure this is followed. *(Recommended strategy attached as Annex B3)*	Yes
12.	The Systems Manager should confirm and implement a policy on anti-virus software for local networks, standalone systems, laptops and home PC's (particularly where data may be transferred to school). This must ensure that anti-virus software is regularly updated.	Yes

Annex 1
Lancashire County Council - ICT Security Policy for Schools

A Recommended Backup Strategy for Schools

All data should be backed up at least 3 times each week - say, Monday, Wednesday & Friday. Hence at least three copies of the data will always be available. (In the case of a large school, processing vast amounts of data daily, a backup every day would be preferable.)

At least one of the backups should be kept away from the school premises (in case of fire or theft).

All backups should be checked to ensure that they have been successful. (E.g. If a backup has been made to a tape, the contents of the tape should be checked to see that a file, or files exist, and that their date of creation is consistent with the date of the backup.)

LRM/FMS users are strongly recommended to backup the financial files before any reconciling (manual or automatic) is undertaken. Label the disk with the month during which the backup was taken, and keep it for at least 12 months.

A 'Long Term Backup' should be taken at the beginning of each term. This should be kept and not overwritten until the beginning of the next term. This will help protect against data corruption that goes unnoticed for several weeks, during which 'older' backups will have been overwritten by 'newer' ones.

Differing media are employed in schools for backing up purposes. E.g. Magnetic tapes, floppy disks, hard disks, Zip drives. If you suspect your principal backup medium is not working correctly (tape drives can be notoriously unreliable), use an alternative.

If possible, use more than one medium for backup anyway. For network users, the option to record onto workstation hard disks is always available. Do this as well as tape and floppy disk backup.

If you are unsure about your backups - please telephone the Westfield Centre and

check whether or not your current processes are adequate and reliable.

Lancashire County Council - ICT Security Policy for Schools

Rules and Agreements for Staff

Rules for ICT Users – Staff

	Notes
1.	Ensure you know who is in charge of the ICT system you use, i.e. the System Manager. You must be aware that any infringement of the current legislation relating to the use of ICT systems :- Data Protection Acts 1984 & 1998 Computer Misuse Act 1990 Copyright, Designs and Patents Act 1988 Provisions of this legislation may result in disciplinary, civil and/or criminal action.
	You must be aware that any infringement of the current legislation relating to the use of ICT systems :- Data Protection Acts 1984 & 1998 Computer Misuse Act 1990 Copyright, Designs and Patents Act 1988 Provisions of this legislation may result in disciplinary, civil and/or criminal action.
3.	ICT resources are valuable and the confidentiality, integrity, availability and accurate processing of data are of considerable importance to the school and as such all users have a personal responsibility for ICT security. Consequently, you must ensure that you receive appropriate training and documentation in the use of your ICT system and in the protection and disclosure of data held.

4.	Follow the local rules determined by the Headteacher in relation to the use of private equipment and software. All software must be used strictly in accordance the terms of its licence and may only be copied if specifically approved by the System Manager.
5.	Ensure that wherever possible your display screen cannot be viewed by persons not authorised to see the information. Ensure that equipment is sited so as to avoid environmental risks, e.g. dust, heat. Do not leave you computer logged on, i.e. where data can be directly accessed without password control, when not in attendance. These same rules apply to official equipment used at home.
6.	You must not exceed any access rights to systems or limitations on the use of data granted to you by the System Manager.
8.	The System Manager will advise you on what "back ups" you need to make of the data and programs you use and the regularity and security of those backups.
9.	Ensure that newly received floppy disks, CD ROMs and emails have been checked for computer viruses. Any suspected or actual computer virus infection must be reported immediately to the System Manager.
10.	Due regard must be given to the sensitivity of the respective information in disposing of ICT printouts, floppy disks, etc.
11.	Users must exercise extreme vigilance towards any suspicious event relating to ICT use and immediately report any suspected or actual breach of ICT security to the System Manager or, in exceptional cases, the Headteacher, Chair of Governors or Internal Audit.
12.	Users of these facilities must complete the declaration attached to the "E-mail & Internet Acceptable Use Policy".