Greenside Primary School

A great school in a great community
achieving great outcomes for children

ICT Security Policy

Reviewed by Governors September 2018

1. Introduction

1.1 We are managing a significant investment in the use of ICT. In many areas of work the use of ICT is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the ICT systems and data are maintained at a level that is appropriate for our needs.

1.2 Sufficient resources should be allocated each year to ensure the security of the school's ICT systems and to enable users to comply fully with the legal requirements and policies covered in this Policy. If insufficient resources are available to fully implement this policy, then the potential risks must be documented and reported to Governors.

2. Policy Objectives

2.1 Against this background there are three main objectives of the ICT Security Policy:-

a) to ensure that equipment, data and staff are adequately protected on a cost-effective basis against any action that could adversely affect the school;

b) to ensure that users are aware of and fully comply with all relevant legislation;

c) to create and maintain within the school a level of awareness of the need for ICT security to be an integral part of the day to day operation so that all staff understand the need for ICT security and their own responsibilities in this respect.

2.2 If difficulties arise in the interpretation and/or appreciation of any aspects of the Policy, the ICT co-ordinator will contact the local authority for further support.

3. Application

3.1 The ICT Security Policy is intended for all school staff who have control over or who use or support the school's administration and curriculum ICT systems or data. Pupils using the school's ICT systems or data are covered by the relevant 'Rules for ICT Users' and 'E-mail and Internet Use Good Practice' documents, which are incorporated within this policy.

3.2 For the purposes of this document the terms `ICT' (or `ICT system'), `ICT data' and 'ICT user' are defined as follows:-

- `ICT' (or `ICT system') means any device for automatic storing and processing of data and includes mainframe computer, minicomputer, microcomputer, personal computer (whether hand-held laptop, portable, stand-alone, network or attached to a mainframe computer), workstation, word-processing system, desk top publishing system, office automation system, messaging system or any other similar device;

- `ICT data' means any information stored and processed by ICT and includes programs, text, pictures and sound;

- 'ICT user' applies to any Council employee, pupil or other authorised person who uses the school's ICT systems and/or data.

4. Scheme of Delegation under the ICT Security Policy

4.1 The ICT Security Policy relies on management and user actions to ensure that its aims are achieved. Consequently, owner, corporate and individual levels of responsibility for ICT security are clearly defined below.

4.2 Owner

4.2.1 The owner has the legal title to the property. In this respect, all software, data and associated documentation produced in connection with the work of the school are the legal property of the Local Authority, which will normally hold it for the benefit of the school.
Exceptions to this will be allowed for software and documentation produced by individual Teachers for lesson purposes – this includes schemes of work, lesson plans, worksheets or as otherwise agreed in writing by the Headteacher.

4.2.2 We also use software and data that are the legal property of external organisations and which are acquired and used under contract or licence.

4.3 Governing Body

4.3.1 The governing body has ultimate corporate responsibility for ensuring that the school complies with the legislative requirements relating to the use of ICT systems and for disseminating policy on ICT security and other ICT related matters.
In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Headteacher.

4.4 Headteacher

4.4.1 The Headteacher is responsible for ensuring that the legislative requirements relating to the use of ICT systems are met and that the school's ICT Security Policy, as may be amended from time to time, is adopted and maintained by the school. He/she is also responsible for ensuring that any special ICT security measures relating to the school's ICT facilities are applied and documented as an integral part of the Policy.

In practice, the day to day functions should be delegated to the 'System Manager', who must be nominated in writing by the Headteacher.

4.4.2 The Headteacher is also responsible for ensuring that the requirements of the Data Protection Act 1998 are complied with fully by the school. This is represented by an on-going responsibility for ensuring that the :-

- registrations under the Data Protection Act are up-to-date and cover all uses being made of personal data and
- registrations are observed with the school.

4.4.3 In addition, the Headteacher is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy and to ensure that the appropriate controls are in place for staff to comply with the Policy. This is particularly important with the increased use of computers and laptops at home. Staff should exercise extreme care in the use of personal data at home to ensure legislation is not contravened, in particular the Data Protection Act 1998.

4.5 System Manager

4.5.1 The 'System Manager' is responsible for the school's ICT equipment, systems and data and will have direct control over these assets and their use, including responsibility for controlling access to these assets and for

defining and documenting the requisite level of protection. The System Manager will be an employee of the school.

In many schools the Headteacher will take on the role of the System Manager. It is acceptable for technical functions to be 'out-sourced'. Where the System Manager is not the Headteacher, the governors should be advised of the sensitivity of the post during the appointment process.

4.5.2 Consequently, the System Manager will administer the practical aspects of ICT protection and ensure that various functions are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.

4.5.3 In line with these responsibilities, the System Manager will be the official point of contact for ICT security issues and as such is responsible for notifying the Headteacher or Chair of Governors of any suspected or actual breach of ICT security occurring within the school. The Headteacher or Chair of Governors should ensure that details of the suspected or actual breach are recorded and made available to Internal Audit upon request. The Headteacher or Chair of Governors must advise Internal Audit of any suspected or actual breach of ICT security pertaining to financial irregularity.

4.5.4 It is vital, therefore, that the System Manager is fully conversant with the ICT Security Policy and maintains an up to date knowledge of best practice and follows the associated approved practices.

4.6 Internal Audit

4.6.1 The Local Authority's Internal Audit Section is responsible for checking periodically that the measures prescribed in each school's approved ICT Security Policy are complied with, and for investigating any suspected or actual breaches of ICT security.

4.6.2 Specialist advice and information on ICT security may be obtained from the Local Authority's ICT Unit, who will liaise with Internal Audit on such matters.

4.7 Users

4.7.1 All users of the school's ICT systems and data must comply with the requirements of this ICT Security Policy, the relevant rules of which are summarised in *`The Rules for ICT Users'*

4.7.2 Users are responsible for notifying the System Manager of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly to the Headteacher, Chair of Governors or to Internal Audit.

5. The Legislation

5.1 Background

5.1.1 The responsibilities referred to in the previous sections recognise the requirements of the current legislation relating to the use of ICT systems, which comprise principally of :-

Data Protection Acts 1984 & 1998;
Computer Misuse Act 1990;
Copyright, Designs and Patents Act 1988
The Telecommunications Act 1984

5.1.2 It is important that all staff are aware that any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.

5.1.3 The general requirements arising from these acts are described below.

5.2 Data Protection Acts 1984 & 1998

5.2.1 The Data Protection Act exists to regulate the use of computerised information about living individuals. To be able to meet the requirements of the Act, the Headteacher is required to compile a census of data giving details and usage of all relevant personal data held on computer within the school and file a registration with the Data Protection Registrar. It is important that amendments are submitted where the scope of the system extends to new areas of operation. The 1998 Act is consistent with the principles established in the 1984 Act, but extends the regulation to certain manual records as well as computerised information.

5.2.2 It is important that all users of personal data are aware of, and are reminded periodically of, the requirements of the act and, in particular, the limitations on the storage and disclosure of information.

5.2.3 Failure to comply with the provisions of the prevailing Act and any subsequent legislation and regulations relating to the use of personal data may result in prosecution by the Data Protection Registrar.

5.3 Computer Misuse Act 1990

5.3.1 Under the Computer Misuse Act 1990 the following are criminal offences, if undertaken intentionally:-

Unauthorised access to a computer system or data;
Unauthorised access preparatory to another criminal action;
Unauthorised modification of a computer system or data.

5.3.2 All users must be given written notice that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written 'in-house', will be regarded as a breach of school policy and may be treated as gross misconduct and that in some circumstances such a breach may also be a criminal offence.

5.4 Copyright, Designs and Patents Act 1988

5.4.1 The Copyright, Designs and Patents Act 1988 provides the legal basis for the protection of intellectual property which includes literary, dramatic, musical and artistic works. The definition of "literary work" covers computer programs and data.

5.4.2 Where computer programs and data are obtained from an external source they remain the property of the originator. Our permission to use the programs or data will be governed by a formal agreement such as a contract or licence.

5.4.3 All copying of software is forbidden by the Act unless it is in accordance with the provisions of the Act and in compliance with the terms and conditions of the respective licence or contract.

5.4.4 The System Manager is responsible for compiling and maintaining an inventory of all software held by the School and for checking it at least annually to ensure that software licences accord with installations. To ensure that we comply with the Copyright, Designs and Patents Act 1988 and in order to satisfy the County Council's responsibilities as a corporate member of FAST (Federation Against Software Theft), users must get prior permission **in writing** from the System Manager before copying any software.

5.4.5 The System Manager is responsible for compiling and maintaining an inventory of all software held by the school and for checking it at least annually to ensure that software licences accord with installations.

5.4.6 All users must be given written notice that failure to comply with the provisions of the Act will be regarded as a breach of school policy and may be treated as gross misconduct and may also result in civil or criminal proceedings being taken.

5.5 The Telecommunications Act 1984 and 2000

5.5.1 The Telecommunications Act 1984, section 43 makes it an offence to send 'by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character'.

5.5.2 The Telecommunications Regulations 2000 impose restrictions on the interception of communications such as e-mail.

6. Management of the Policy

6.1 The Headteacher should allocate sufficient resources each year to ensure the security of the school's ICT systems and to enable users to comply fully with the legal requirements and policies covered in this Policy. If insufficient resources are available to fully implement this policy, then the potential risks must be documented and reported to Governors.

6.2 Suitable training for all ICT users and documentation to promote the proper use of ICT systems will be provided. Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data. A record of the training provided through the school to each individual user will be maintained by the user.

6.3 In addition, users will be made aware of the value and importance of such ICT systems and data, particularly data of a confidential or sensitive nature, and be made aware of their personal responsibilities for ICT security.

6.4 To help achieve these aims, the relevant parts of the ICT Security Policy and any other information on the use of particular facilities and techniques to protect the systems or data will be disseminated to users.

6.5 The Headteacher must ensure that adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures should be applied that provide for continuity of ICT security when staff vacate or occupy a post. These measures as a minimum must include:-

- a record that new staff have been issued with, have read the appropriate documentation relating to ICT security, and have signed the list of rules;
- a record of the access rights to systems granted to an individual user and their limitations on the use of the data in relation to the data protection registrations in place;
- a record that those rights have been amended or withdrawn due to a change to responsibilities or termination of employment;

7. Physical Security

7.1 Location Access

7.1.1 Adequate consideration should be given to the physical security of rooms containing ICT equipment (including associated cabling). As far as practicable, only authorised persons should be admitted to rooms that contain

servers or provide access to data. The server rooms should be locked every evening and shutters closed to protect the data. Rooms where back up data is stored should also remain locked.

7.1.2 The System Manager must ensure appropriate arrangements are applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

7.2 Equipment siting

7.2.1 Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:-

- devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;
- equipment is sited to avoid environmental damage from causes such as dust & heat;
- users have been instructed to avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users;
- users have been instructed not to leave hard copies of sensitive data unattended on desks;

The same rules apply to official equipment in use at a user's home.

7.3 Inventory

7.3.1 The Headteacher, in accordance with the School's Financial Regulations, shall ensure that an inventory of all ICT equipment (however financed) is maintained and all items accounted for at least annually.

8. System Security

Annex B6 contains details of security guidelines for System Managers.

8.1 Legitimate Use

8.1.1 The school's ICT facilities must not be used in any way that breaks the law or breaches County Council standards. Such breaches include, but are not limited to:-

- making, distributing or using unlicensed software or data;
- making or sending threatening, offensive, or harassing messages;
- creating, possessing or distributing obscene material;
- unauthorised private use of the school's computer facilities.

8.2 Private Hardware & Software

8.2.1 Dangers can occur from the use of unlicensed software and software infected with a computer virus. It is therefore vital that any private software permitted to be used on the school's equipment is acquired from a responsible source and is used strictly in accordance with the terms of the licence. The use of all private hardware for school purposes must be approved by the System Manager.

8.3 ICT Security Facilities

8.3.1 The school's ICT systems and data will be protected using appropriate security arrangements outlined in the rest of Section 8. In addition consideration should also be given to including appropriate processing controls such as audit trails, input validation checks, control totals for output, reports on attempted unauthorised access, etc.
For new systems, it is recommended that such facilities be confirmed at the time of installing the system. Information on the range of such facilities can be sought from the Council's ICT Unit

8.4 Authorisation

8.4.1 Only persons authorised by the System Manager, are allowed to use the school's ICT systems. The authority given to use a system will be sufficient but not excessive and the authority given must not be exceeded.
Failure to establish the limits of any authorisation may result in the school being unable to use the sanctions of the Computer Misuse Act 1990. Not only will it be difficult to demonstrate that a user has exceeded the authority given, it will also be difficult to show definitively who is authorised to use a computer system.
All ICT systems should display a message to users warning against unauthorised use of the system.

8.4.2 Access eligibility will be reviewed continually, including remote access for support. In particular the relevant access capability will be removed when a person leaves the employment of the school. In addition, access codes, user identification codes and authorisation rules will be reviewed whenever a user changes duties.
Failure to change access eligibility and passwords will leave the ICT systems vulnerable to misuse.

8.5 Passwords

8.5.1 The level of password control will be defined by the System Manager based on the value and sensitivity of the data involved, including the possible use of "time out" passwords where a terminal/PC is left unused for a defined period.

8.5.2 Passwords for staff users should be changed at least termly and should not be re-used. They should be a minimum of 6 alphanumeric characters and not obviously guessable.

8.5.3 Passwords should be memorised. If an infrequently used password is written down it should be stored securely.
Passwords or screen saver protection should protect access to all ICT systems, including "boot" passwords on PCs, particularly laptop/notebook PCs as they are highly portable and less physically secure.
It is acknowledged that the use of 'boot' passwords may not be feasible on Curriculum systems.

8.5.4 A password must be changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur, such as:-

- when a password holder leaves the school or is transferred to another post;
- when a password may have become known to a person not entitled to know it.

The need to change one or more passwords will be determined by the risk of the security breach.

8.5.5 Users must not reveal their password to anyone, apart from authorised staff. Users who forget their password must request the System Manager issue a new password.

8.5.6 Where a password to boot a PC or access an internal network is shared, users must take special care to ensure that it is not disclosed to any person who does not require access to the PC or network.

8.6 Backups

8.6.1 In order to ensure that our essential services and facilities are restored as quickly as possible following an ICT system failure, back-up copies of stored data will be taken at regular intervals as determined by the System

Manager, dependent upon the importance and quantity of the data concerned. Currently the school server is backed up 5 times a week.

Where programs and data are held on the Council's systems or other multi-user system, such security is likely to be covered by existing procedures. In the case of other ICT systems (including PCs) the user will normally need to make security copies of their data.

8.6.2 Security copies should be clearly marked as to what they are and when they were taken and stored away from the system to which they relate in a restricted access fireproof location and/or off site.

8.6.3 Instructions for re-installing data or files from backup should be fully documented and security copies should be regularly tested to ensure that they enable the systems/relevant file to be re-loaded in cases of system failure. This will be carried out by the school technician and the

8.7 Virus Protection

8.7.1 The school will use appropriate Anti-virus software for all school ICT systems.
All Users should take precautions to avoid malicious software that may destroy or corrupt data.

8.7.2 The school will ensure that every ICT user is aware that any PC with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the System Manager who must take appropriate action, including removing the source of infection.
The governing body could be open to a legal action for negligence should a person suffer as a consequence of a computer virus on school equipment.

8.7.3 Any third-party laptops not normally connected to the school network must be checked by the System manager for virus's and anti-virus software before being allowed to connect to the network.

8.7.4 Teachers must take the necessary steps to ensure anti-virus protection software on their laptop is updated on a weekly basis as a minimum.

8.8 Disposal of Waste

8.8.1 Disposal of waste ICT media such as print-outs, floppy diskettes, pen drives and magnetic tape will be made with due regard to the sensitivity of the information they contain. For example, paper will be shredded or places in the locked red bins if any confidential information from it could be derived.
The Data Protection Act requires that adequate mechanisms be used when disposing of personal data.

8.9 Disposal of Equipment

Prior to the transfer or disposal of any ICT equipment the System Manager must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations. School currently uses Stone Computers to dispose of any old equipment who ensure that hard drives are wiped at their recycling centre.
The Data Protection Act requires that any personal data held on such a machine be destroyed.
It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.

8.10 Repair of Equipment

8.10.1 If a machine, or its permanent storage (usually a disk drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from hard disks and stored on floppy disk or other media for subsequent reinstallation, if possible.The school will ensure that third parties are currently registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of *it.*

9 Security Incidents

9.1 All suspected or actual breaches of ICT security shall be reported to the System Manager or the Headteacher in their absence, who should ensure a speedy and effective response to be made to an ICT security incident, including securing useable evidence of breaches and evidence of any weakness in existing security arrangements. They must also establish the operational or financial requirements to restore the ICT service quickly.

The Audit Commission's Survey of Computer Fraud and Abuse 1990 revealed that over 50% of incidents of ICT misuse are uncovered accidentally. It is, therefore, important that users are given positive encouragement to be vigilant towards any suspicious event relating to ICT use.

It should be recognised that the school and its officers may be open to a legal action for negligence if a person or organisation should suffer as a consequence of a breach of ICT security within the school where insufficient action had been taken to resolve the breach.

At Greenside Primary School we will continually strive to ensure that everyone is treated with respect and dignity. Each person will be given fair and equal opportunities to develop their full potential regardless of their gender, transgender, ethnicity, culture and religious background, sexuality, disability or special educational needs and ability.