# ICT Security Policy

## 1. Introduction

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

1.2. It is the policy of Turncroft to ensure that:

• information will be protected against unauthorised access

• confidentiality of information will be assured

• integrity of information will be maintained

• regulatory and legislative requirements will be met

• business continuity plans will be produced, maintained and tested

• ICT security cpd will be available to all staff

## 2. Policy Objectives

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

• to ensure that equipment, data and staff are adequately protected against any action that could adversely affect the school;

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

• 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.

## 3. Application

3.1. The ICT Security Policy is intended for all school staff who are either controllers of the system or who are users and supporters of the school's administration and curriculum ICT systems or data. Pupils using the school's ICT systems or data are covered by the school's 'Acceptable Use Policy' documents.

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 or combination of devices used for the storage or processing of data and includes: workstation (netbook, notebook, desktop/tower PC), PDA, cash till, server or any other similar device;

• 'ICT data' means any information stored and processed within the ICT system and includes programs, text, pictures and sound;

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

**4. Roles and Responsibilities**

4.1. The ICT Security Policy relies on management and user actions to ensure that its aims are achieved. Consequently, roles and responsibilities are defined below.

**4.2. Governing Body**

4.2.1. The governing body has the 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.

**4.3. Headteacher**

4.3.1. 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. 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 this policy.

4.3.2. The day to day functions are delegated to the Office Manager,

4.3.3. The Headteacher is responsible for ensuring that the requirements of the General Data Protection Regulation are complied with fully by the school. This is represented by an ongoing responsibility for ensuring that the:

• registrations under the General Data Protection Regulation are up-to-date and cover all uses being made of personal data and

• registrations are observed with the school.

4.3.4. 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 General Data Protection Regulation.

**4.4. System (ICT) Manager**

4.4.1. The 'ICT 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 ICT Manager is Mrs McIver, Office Manager

4.4.2. The ICT 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.

4.4.3. In line with these responsibilities, the ICT 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.

4.4.4. It is vital, therefore, that the ICT 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.

**4.5. School ICT Manager**

4.5.1. The School's ICT Manager is responsible for maintaining, repairing and proactively supporting the ICT System so that it can meet the requirements of the ICT Security Policy.

4.5.2. The School's ICT Manager will also monitor the ICT System for breaches of security and inform the Headteacher.

**4.6. Users**

4.6.1. Users are those employees, pupils or authorised guests of the school who make use of the ICT system to support them in their work. All users of the school's ICT systems and data must comply with the requirements of this ICT Security Policy. The school has an Acceptable Use Policy which summarises the responsibilities of users of the school's ICT systems.

4.6.2. Users are responsible for notifying the ICT 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 BwD Internal Audit department.

4.6.3. Users are responsible for the equipment they use including:

• Physical security

• Security of data

• Their own passwords.

• Backing of their files/work

**5. Management of the Policy**

5.1. 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 by the Headteacher.

5.2. 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 through staff meetings.

5.3. 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.

5.4. 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.

5.5. 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.

**6. Physical Security**

***6.1. Location Access***

6.1.1. Adequate consideration should be given to the physical security of rooms containing ICT equipment (including associated cabling). The server room should be locked when not in use.

6.1.2. The ICT 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.

**6.2. Equipment siting**

6.2.1. 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.

6.2.2.The same rules apply when accessing the School's ICT System or ICT data away from school, e.g. at a User's home or visiting another school.

**6.3. Inventory**

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

**7. Legitimate Use**

7.1. The school's ICT facilities must not be used in any way that breaks the law or breaches Council standards.

7.2. 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 personal use of the school's computer facilities.

**7.3. Private Hardware & Software**

7.3.1. 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 and recorded by the ICT Manager.

**7.4. ICT Security Facilities**

7.4.1. The school's ICT systems and data will be protected using appropriate security arrangements outlined in the rest of Section 7. 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.

7.4.2.For new systems, it is recommended that such facilities be confirmed at the time of installing the system..

**7.5. Authorisation**

7.5.1. Only persons authorised by the ICT Manager and in full compliance with the schools ICT policies, are allowed to use the school's ICT systems. The ICT manager will ensure the user is fully aware of the extent to which an ICT User may make use of the ICT System.

7.5.2. 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.

7.5.3. 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.

7.5.4. Failure to change access eligibility and passwords will leave the ICT systems vulnerable to misuse.

**7.6. Passwords**

7.6.1. The level of password control will be defined by the ICT 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.

**7.6.2. Passwords for staff users**

7.6.2.1 Encryption passwords MUST be a minimum of 8 characters, including a mix of letters (upper and lower case) and numbers.

7.6.3. Passwords should be memorised and if written down MUST not be kept with the device in any form.

7.6.4. Passwords should protect access to all ICT systems. ICT devices will be protected with a password to restrict unauthorised access.

7.6.5.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.

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

7.6.7. Users must not reveal their password to anyone. The ICT manager will keep a log of all encryption passwords in a secure area to which only he has access.

**7.7. Security of the network**

7.7.1. Only devices approved by the ICT Manager should be permitted to be connected to the network, either through wired or wireless connectivity.

7.7.2. Where devices are connected to the network using wireless, the wireless network should be secure; as a minimum this should be done using WPA. Open Access Wireless Access Points must not be connected to our school's network.

7.7.3. Encryption is applied to wireless networks, encryption keys should be kept secure and remain the property of the system manager and must not be shared without written permission.

7.7.4. Mobile devices may with permission connect to the network but in full compliance with the ICT policies and this permission may be withdrawn at any time. The ICT Manager will inform the owner/user that if a mobile device connects to the School's internet connection, then the device's online activity will be monitored and logged by the School's Internet Service Provider.

**7.8. Encryption**

7.8.1. All devices that have access to data attached to the ICT System are fully encrypted Devices subject to encryption may include:

• Laptops

• PDAs

• Smartphones

• USB Pendrives/Memory cards

• Desktops

7.8.2. Where technology prevents the use of encryption (e.g. SD Memory Cards used in Digital Cameras) then any data deemed Impact Level 2 or above should not be stored on these devices.

**7.9. Filtering of the Internet**

7.9.1. Access to the internet for children and staff is filtered using an approved system provided by BwD.

7.9.2. It is the responsibility of the ICT Manager to monitor the effectiveness of filtering at the school and report issues to the Headteacher and our school's internet service provider.

7.9.3. Where breaches of internet filtering have occurred, the ICT Manager should inform the Headteacher/DSL and assess the risk of continued access.

**7.10. Backups**

7.10.1. In order to ensure that 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 ICT Manager, dependent upon the importance and quantity of the data concerned.

7.10.2. Data essential for the day to day running and management of the school should be stored on our school's network.

7.10.3. Backups contain data that must be protected and should be clearly marked as to what they are and when they were taken. They should be stored away from the system to which they relate in a restricted access fireproof location, preferably off site.

7.10.4. 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.

**7.11. Operating System Patching**

7.11.1. The ICT manager will ensure that all machines defined as part of the ICT System are patched up to date according to those releases distributed by the manufacturers of the operating systems.

**7.12. Virus Protection**

7.12.1. Our school will use appropriate Anti-virus/Anti-malware software for all school ICT systems.

7.12.2. All Users should take precautions to avoid malicious software that may destroy or corrupt data.

7.12.3. Our school will ensure that every ICT user is aware that any device in the ICT system (PC, laptops, netbook, Ipads) with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the ICT Manager who must take appropriate action, including removing the source of infection.

7.12.4. 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.

7.12.5. Any third-party laptops/mobile devices and mobile storage not normally connected to the school network must be checked by the ICT Manager for viruses and up-to-date antivirus software before being allowed to connect to the network.

7.12.6. The school will ensure that up-to-date anti-virus signatures are applied to all servers and that they are available for users to apply, or are automatically applied, to PCs or laptops.

**7.13. Disposal of Waste**

7.13.1. Disposal of waste ICT media such as print-outs, floppy diskettes and magnetic tape will be made with due regard to the sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it could be derived.

7.13.2. The Data Protection Act (GDPR) requires that adequate mechanisms be used when disposing of personal data.

**7.14. Disposal of Equipment**

7.14.1. The Data Protection Act requires that any personal data held on a part of the ICT system subject to disposal to be destroyed.

7.14.2. Prior to the transfer or disposal of any ICT equipment the ICT 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 (GDPR) 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.

7.14.3. 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. The school should maintain a regularly updated asset register of licenses and should indicate when licenses have been transferred from one part of the ICT system to another.

**7.15. Repair of Equipment**

7.15.1. 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 other media for subsequent reinstallation, if possible. The school will ensure that third parties are currently registered under the Data Protection Act (GDPR) 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.

**8. Security Incidents**

8.1. All suspected or actual breaches of ICT security shall be reported to the ICT 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.

8.2. 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.

8.3. 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.

**9. Acceptable Use Policy**

9.1. The school's Acceptable Use Policy applies to all school staff, students and third parties who use either or both of these facilities. The policy covers the use of Email, the Internet, services accessed through the Internet and local file and network usage. The conditions of use are explained in the policy. All school staff accessing these facilities must be issued with a copy of the 'Acceptable Use Policy and other relevant documents and complete the user declaration attached to the policy. For all students, the school will ensure that the relevant 'Acceptable Use Policy' document is issued and the consent form is completed by pupils and their parents. In addition, copies of the 'Acceptable Use Policy' document and consent form will be issued to all visitors.

**10. Personal Use**

10.1. The School has devoted time and effort into developing the ICT Systems to assist you with your work. It is, however, recognised that there are times when you may want to use the Systems for non-work related purposes, and in recognising this need the School permits you to use the Systems for personal use.

10.2. You must not use the systems for personal use during working hours. You must not allow personal use of systems to interfere with your day to day duties. Any non-job related use of the systems during working hours may be subject to disciplinary action.

10.3. You must not use School software for personal use unless the terms of the licence permit this and you are responsible for checking the licensing position. Microsoft Office and Internet Explorer are licensed for personal use.

10.4. Use of the systems should at all times be strictly in accordance with the provisions of paragraph 9.1 above. You must pay all costs associated with personal use at the School's current rates e.g. cost of paper.

10.5. You are responsible for any non-business related file which is stored on your computer.

**11. Disciplinary Implications**

11.1. Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under the Computer Misuse Act 1990, and may lead to prosecution of the School and the individual(s) concerned and/or civil claims for damages.

Policy written: August 2020

Policy Approved by Governors: September 2020

Policy Review Date: August 2023

Elizabeth Shears

Celia Rushton