ICT Information Security Policy

Aspiring Foundations Federated Nursery Schools

Date : Sept 18

1. Introduction

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

1.2 It is the policy of the school 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 training 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 information asset owners 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 (laptop, netbook, notebook, desktop/tower PC), 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, 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.

Governing Body

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.

Headteacher

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.

The day to day functions are delegated to the ICT Manager, who must be nominated in writing by the Headteacher. This would take the form of an item in a job description.

The Headteacher is responsible for ensuring that the requirements of data protection legislation are complied with fully by the school. This is represented by an on-going responsibility for ensuring that the data protection registrations with the Information Commissioner are up-to-date and cover all uses being made of personal data

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.

System (ICT) Manager

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 will be an employee of the school.

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.

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 the school's Data Protection Officer. The Headteacher or Chair of Governors must advise the DPO of any suspected or actual breach of ICT security pertaining to financial irregularity.

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.

School ICT Support Contractor

The school's ICT support contractor is responsible for maintaining, repairing and proactively supporting the ICT System so that it can meet the requirements of the ICT Security Policy. The School ICT Support Contractor will respond to actions delegated by the school's nominated 'ICT Manager' in order to ensure that the ICT System can comply with the ICT Security Policy.

The contractor will also monitor the ICT System for breaches of security and inform the Headteacher.

Users

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.

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 the school's DPO.

Users are responsible for the equipment they use including:

- Physical security
- Security of data
- Their own passwords.
- Ensuring their work is saved and that all saved work is backed up under contract with the school's ICT support contractor

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. A record of the training provided through the school to each individual user will be maintained. Maintenance of this record should be the responsibility of the nominated 'ICT Manager'.

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 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 of 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). 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 when left unattended. Ideally, such rooms should have a minimum of key pad access.

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 school's 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

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

Laptop/computer passwords will be changed on a 90 day cycle.

7.6.3 Passwords should be memorised - never written down and left with the device.

7.6.4 Passwords or screen saver protection should protect access to all ICT systems. The BIOS area of ICT devices should 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.

7.6.8 In the event of forgotten passwords/locked out accounts, the school's ICT support contractor will be asked to reset.

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 the 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 manger and must not be shared without written permission. These are changed at least termly.

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.

7.8 Filtering of the Internet

7.8.1 Access to the internet for children should be filtered using an approved system as provided by the school's ICT Support Contractor.

7.8.2 It is the responsibility of the ICT Manager to monitor the effectiveness of filtering at the school and report issues to the Headteacher.

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

7.9 Backups for the curriculum network

7.9.1 The school's ICT support contractor manages the school's onsite/offsite secure backup processes. 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 by the ICT support contractor as set out in the school's service level agreement

7.9.2 The data that is saved on the school's admin network is securely saved and backed up offsite by Halton Borough Council in accordance with the school's service level agreement.

7.9.3 Curriculum 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 offsite in a restricted access fireproof location.

7.9.4 The work involved in re-installing data or files from the curriculum backup is carried out by the school's ICT support contractor and 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.

7.10 Lost work saved on curriculum network

7.10.1 The school's ICT support contractor manages the school's onsite/offsite secure backup processes. When work has been lost within a period of 3 months the school's ICT support contractor will restore and recover lost work.

7.11 Operating System Patching

7.11.1 The responsibility for providing system patching sits with the ICT support contractor in accordance with the school's service level agreement.

7.12 Virus Protection

7.12.1 The responsibility for providing virus protection sits with the ICT support contractor in accordance with the school's service level agreement.

7.13 Disposal of ICT Equipment

7.14 Disposal of Equipment

7.14.1 Refer to the school's 'Disposal of Redundant ICT Equipment' Policy.

8. Security Incidents

8.1 Refer to the school's Data Protection Policy.

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.