ICT Security Policy

February 2018

Date of Review:	**February 2018**
Lead reviewer:	**I Neal, ICT Director**
Approval:	**Finance, Resources, Audit and Risk Committee**
Approved on:	**7 March 2018**
Date of Review:	**February 2019 or earlier in response to statutory changes**

Contents

1. Scope

1.1 Terminology

In this policy:

The term ‘staff’ encompasses employees, officers, consultants, contractors, casual workers and agency workers.

The term ‘volunteers’ includes all those freely giving of their time to contribute to the work of the Trust and its Schools including Members, Trustees and Governors.

The term ‘ICT facilities and systems’ includes computer equipment, telephones, voicemail, fax, CCTV, copiers, scanners, electronic key fobs and cards, cameras, webcams, USB devices, the internet, intranet, School VLE’s, email, all forms of social media and networking sites. This list is not exhaustive.

1.2 Application

This policy applies to all staff and volunteers who are given access to the Trust’s ICT facilities and systems.

The requirements set out in this policy also apply to the use of School’s ICT facilities and systems out of school, and the transfer of personal data (digital or paper based) out of school.

All staff and volunteers must immediately report any break of this policy via the appropriate channels.

The policy itself does not form part of any employee’s contract of employment and may be amended at any time, however it is a condition of use of the Trust’s ICT facilities and systems that users are bound by the Acceptable Use Agreement.

Breach of this policy may result in disciplinary action up to and including dismissal. This policy will apply and disciplinary action may be taken regardless of whether the breach is committed during working hours, and whether the facilities and systems are owned by the Trust or the user, where use affects the welfare of children or young people or constitutes a risk to the Trust or School.

It is acknowledged that this policy cannot cover every eventuality or the breadth of issues arising out of the use of ICT. As such the Trust will always have regard to the intent of this policy in its application to matters which may not be explicitly covered.

1.3 Links with other policies and statutory guidance

This policy has been developed with due regard to the statutory guidance Keeping Children Safe in Education September 2016 (as amended), Guidance for safer working practice for those working with children and young people in education settings October 2015, the Freedom of Information Act 2000 (as amended), the Data Protection Act 1998, the Protection of Freedoms Act 2012 and the Computer misuse Act 1990.

The Trust will also comply with information and guidance displayed on the Information Commissioner’s website (https://ico.org.uk/)

The policy is linked to the Trust’s Code of Conduct, Safeguarding and Child Protection, E-Safety, Disciplinary, Acceptable Use, Anti-Bullying and Dignity at Work, Data Protection, Data Handling and FOI, Reference and Whistleblowing Policies, copies of which are available from the School or can be downloaded from the Policies section of the School’s website.

2. Technical Security

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The Trust will be responsible for ensuring that the Trust's ICT facilities and systems are as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the Trust's policies)
- access to personal data is securely controlled in line with the Trust's Data Protection, Data Handling and FOI policy
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of Trust's ICT facilities and systems
- senior leaders have an overview and have an impact on policy and practice.

2.1 Policy statements

The Trust will be responsible for ensuring that the Trust's ICT facilities and systems are as safe and secure as is reasonably possible and that statements approved within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:

- The Trust's ICT facilities and systems will be managed in ways that ensure that the Trust meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of Trust's ICT facilities and systems.
- Servers, wireless systems and network equipment must be securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the Trust's systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff.
- All users will have clearly defined access rights to Trust's ICT facilities and systems. Details of the access rights available to groups of users will be recorded by the relevant ICT Service Team and will be reviewed, at least annually, by the Online Safety Group.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security (see Acceptable Use Policy).
- ICT Service Team Leader or Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Mobile device security and management procedures are in place (where mobile devices are allowed access to the Trust's / School's systems).
- The Trust's / School's technical staff regularly monitor and record the activity of users on the Trust's / School's systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users' activity
- An appropriate system is in place for users to report any actual / potential technical incident to the relevant ICT Service Team.
- An agreed process is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the Trust's / School's systems.

- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on the Trust's / School's devices by users (see Acceptable Use Policy).
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on the Trust's / School's devices that may be used out of the Trust / School (see Acceptable Use Policy).
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on the Trust's / School's devices (see Acceptable Use Policy and Data Protection, Data Handling and FOI Policy for further detail).
- The Trust's / School's infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- Personal data cannot be sent over the internet or taken off the Trust's / School's sites unless safely encrypted or otherwise secured (see Data Protection, Data Handling and FOI Policy for further detail).

3. Filtering and Monitoring

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the Trust has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situations in the schools.

3.1 Responsibilities

The responsibility for the management of the Trust's / School's filtering policy will be held by a senior member of the relevant ICT Service Team. They will manage the Trust's / School's filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering and monitoring systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to which categories are being filtered by the Trust's / School's filtering service must:

- be logged in change control logs.
- be reported to the Trust ICT Director.
- be reported to the relevant Safeguarding Board every 2 months in the form of an extract from the change control logs.

All users have a responsibility to report immediately to the relevant ICT Services Team any infringements of the Trust's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes, software or hardware that might allow them to bypass the filtering / monitoring / security systems in place to prevent access to such materials.

3.2 Policy Statements

- Internet access is filtered for all users.
- The Trust manages its own filtering service.
- The Trust has provided enhanced / differentiated user-level filtering through the use of the filtering service.
- Illegal content is filtered by actively employing the filter provider's illegal content lists.

- Filter content lists are regularly updated and internet use is logged and frequently monitored.
- The monitoring process alerts the Trust / School to breaches of the filtering policy, which are then acted upon.
- There is a clear route for reporting and managing changes to the filtering system.
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head teacher / Principal (or other nominated member of the senior leadership).
- Mobile devices that access the Trust's / School's internet connection (whether the Trust's / School's or personal devices) will be subject to the same filtering standards as other devices on the Trust's / School's infrastructure.
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by a senior member of the ICT Services Team, the ICT Director or another member of the senior leadership team. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Safeguarding Board.
- The Trust / School supplements their filtering systems with additional monitoring systems.
- The Trust / School will monitor the activities of users on the Trust's ICT facilities and systems as indicated in the Trust e-Safety Policy and the Acceptable Use Agreement.

3.3 Education / Training / Awareness

Pupils / students will be made aware of the importance of filtering and monitoring systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering and monitoring system.

Staff users will be made aware of the filtering and monitoring systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset days.

Parents will be informed of the Trust's / School's filtering and monitoring policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

3.4 Changes to the Filtering System

Staff may request changes to the filtering by submitting a ticket to the relevant ICT Service Team including:

- the web site(s) that they want to have allowed or denied.
- the nature of the site(s).
- which groups of users need to be allowed or denied.
- the reason(s) for why the site(s) should be allowed or denied (there should be strong educational reasons for changes to be agreed).

The relevant ICT Service Team should:

- where appropriate, confirm, usually via a web search, that the web site(s) are as expected.
- log, within the exception on the filtering service, the date, requester's name and subject area.
- where appropriate, test that the allow or deny is now in place.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the relevant ICT Service Team who will decide whether to make school level changes (as above).

3.5 Audit / Reporting

Logs of filtering system changes and of filtering incidents will be made available to:

- Trust ICT Director
- Safeguarding Board
- Governance committee responsible for safeguarding
- Local Authority / Police on request

The categories which are filtered will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

4. Change Management

Change Management is a process whereby any changes being made to ICT facilities and systems are logged, recorded, properly tested and approved by representatives from all interested parties. The purpose of Change Management is to reduce the impact that changes to the ICT environment will or may have on the ability of the Trust / School to carry out its work.

The Trust will carry out changes to our IT operating environment in a way that:

- Is properly planned
- Is properly controlled
- Is recoverable or can be undone where possible
- Has measurable success criteria
- Has proven test results where possible
- Causes minimum disruption to the operations of the Trust

All changes will be properly documented and will follow an approvals process.

4.1 Policy Statements

- Changes will categorised as:
    - Planned Major Change
    - Maintenance and minor updates
    - Emergencies and Unplanned Outages
- Every change to a Trust / School resource such as operating systems, infrastructure, networks and applications is subject to the Change Management Policy and must follow the Change Management Procedures.
- A formal request either in writing or logged on the Helpdesk system (as determined by the Change Management Procedure) must be submitted for all changes, both scheduled and unscheduled.
- A Change Management Log must be maintained for all changes. This would typically form a part of the Change Request Form information. The log must contain, but is not limited to:
    - Date of submission and date of change
    - Owner and custodian contact information
    - Nature of the change
    - Address the risks associated with the change if it is or is not implemented.
    - Authorisation appropriate to the type of Change.
    - Indicate the backout plan if the change implementation fails.
    - Indicate the availability of resources to implement the change.
    - Indication of success or failure.
- Customer notification must be completed for each scheduled or unscheduled change following the required procedures.
- The Change Advisory Board (CAB) will convene as required to review change requests and to ensure that change reviews are being satisfactorily performed.
- The CAB may deny a scheduled or unscheduled change for reasons including, but not limited to:

    - inadequate planning,
    - risks too high,
    - the timing of the change will negatively impact a key business process,
    - or if adequate resources cannot be readily available etc. Adequate resources may be a problem on weekends, holidays or special events.
- Emergency change types will require the approval of the Change Manager and hence will not require CAB approval, thus allowing immediate implementation.
- A change request cannot be implemented prior to being approved by the CAB / Change Manager.

5. Patch Management

The purpose of this policy is to ensure networked devices attached to the Trust / School network are updated accurately and timely with security protection mechanisms (patches) for known vulnerabilities and exploits to reduce or eliminate them in order to limit the impact on the Trust / Schools.

5.1 Policy Statement

All networked devices belonging to or managed by the Trust / School will be patched with vendor provided operating system / application security patches.

These patches will be applied as soon as possible following appropriate testing of the security patches by the appropriate ICT Service Team.

New devices must be patched to the current agreed patch level **prior** to the device being connected to the production network.

Current patch status for all networked devices must be monitored by the ICT Service Teams. Devices that cannot be patched must be reported, with the exact mitigation effort, to the Trust ICT Director or designate.

6. System Access

Access control rules and procedures are required to regulate who can access School / Trust information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing School / Trust information in any format, and on any device.

6.1 User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. Each user must be allocated access rights and permissions to computer systems and data that:

- Are in line with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

6.2 User Registration

A request for access to the School's / Trust's computer systems must first be submitted by the HR department to the ICT Service Desk. The ICT Service Team is then responsible for creating the usernames with the relevant access rights.

When a member of staff or volunteer leaves the Trust, their access to computer systems and data must be suspended at the close of business on their last working day. It is the responsibility of the HR department to request the suspension of the access rights via the ICT Service Desk.

6.3 User Responsibilities

It is a user's responsibility to prevent their username and password being used to gain unauthorised access to School / Trust systems by:

- Following the Password Policy Statements as set out in the Acceptable Use Policy.
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing the ICT Service Desk of any changes to their role and access requirements.

6.4 Network Access Control

The use of mobile data on non-School owned PCs / Laptops connected to the School's / Trust's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from ICT Service Desk before connecting any equipment to the wired network.

6.5 User Authentication for External Connections

Where remote access to the network is required, an application must be made via the ICT Service Desk. Remote access to the network must be secured by two factor authentication consisting of a username and one other component, for example a smart app (also see Acceptable Use Policy).

6.6 Supplier's Remote Access

Partner agencies or 3rd party suppliers must not be given details of how to access the School's / Trust's network without permission from the ICT Service Desk. Any changes to supplier's connections must be immediately sent to the ICT Service Desk so that access can be updated or removed. All permissions and access methods must be controlled by the ICT Service Desk.

Partners or 3rd party suppliers must contact the ICT Service Desk before connecting to the network and a log of activity must be maintained. Remote access software must be disabled or password protected when not in use.

6.7 Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section (section 6.1) and the Password Policy (see Acceptable Use Policy) must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g. username.
- Displaying a general warning notice that only authorised users are allowed.

All access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

6.8 Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The administrator of the system (usually the relevant ICT Service Team) is responsible for granting access to the information within the system. The access must:

- Be compliant with the User Access Management section (section 6.1) and the Password Policy (see Acceptable Use Policy).
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Be logged and auditable.