# Codsall High Federation of Schools
# ICT Security & Acceptable Use Policy

This policy applies to all schools, all staff, students, and governors as well as guest users at Codsall High Federation of Schools incorporating Codsall Community High School, Bilbrook CE Middle School and Perton Middle School.

The objectives of the Policy are to:

- Ensure the protection of confidentiality, integrity and availability of school information and assets.
- Ensure all users are aware of and fully comply with all relevant legislation.
- Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.
- To specify minimum standards that constitute acceptable use of ICT systems.

'Information' covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created. The federation's Network Manager is responsible for the federation's ICT equipment, systems and data with direct control over these assets and their use, including responsibility for access control and protection. The Network Manager will be the official point of contact for ICT or information security issues.

**Responsibilities:**

- Users of the school's ICT systems and data must comply with the requirements of this ICT Security Policy
- Users are responsible for notifying the Network Manager of any suspected or actual breach of ICT security; a log of security or privacy breaches will be made in the relevant register, to comply with GDPR.
- Users must comply with the requirements of the Data Protection Act 2018, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.

- Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.
- Adequate procedures must be established in respect of the ICT security implications of personnel changes.

## Procedural Aspects of the Policy

- The **Governing Body** must ensure that the school implements an ICT Security Policy. This must be reviewed annually.
- The **Executive Headteacher** must nominate a Network Manager or members of non-teaching staff with designated systems management responsibilities. This must be documented and included in the Scheme of Delegation approved by the Governing Body. The Executive Headteacher must ensure that the nominated member(s) of non-teaching staff understands the functions of the role and is familiar with the relevant Acts.
- The **Executive Headteacher** must compile a census of data giving details and usage of all personal data held on computer and manually (as required under GDPR) 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.
- The **Network Manager** should ensure that a copy of the relevant Acceptable Use Policy is made available to all users and that users are periodically reminded of their obligations under this policy. 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.
- The **Network Manager** 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 groups and individual users.
- An inventory of all ICT equipment must be maintained and regularly updated by the **Network Manager** (or ICT support staff where the processing of equipment in/equipment out has been delegated by the Network Manager) as equipment is purchased/disposed of. The inventory must be checked and verified annually in accordance with the requirements of financial regulations. The Network Manager must ensure there are clear procedures regarding the disposal of equipment containing confidential or sensitive data; such procedures must be compliant with the Waste from Electronic and Electrical Equipment (WEEE) directive and that that third parties involved in the disposal of equipment are registered under the Data Protection Act as personnel authorised to see data; as such they will be bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

- An inventory of all software and licence details must be maintained and regularly updated by the **Network Manager** as software is purchased/disposed of. The inventory must be checked annually to ensure that the licences accord with installations.
- The **Network Manager** should ensure there are clear procedures regarding the installing/copying of software. The Network Manager should be familiar with the requirements of FAST (the Federation Against Software Theft) and industry best practice.
- The **Network Manager** should periodically undertake a 'password strength checking exercise' to identify any weak passwords being used by staff to protect sensitive data and rectify security weaknesses as soon as possible; the frequency of such exercises will be determined through threat analysis decided at departmental review with the Executive Headteacher.
- The **Network Manager** must ensure that "shared passwords" – such as those used by ICT support staff to administer school servers, are
    - sufficiently complex to satisfy industry best practice on security
    - stored in password management software that utilises strong encryption
- The **Network Manager** should devise and implement a policy on anti-virus software for local networks, stand-alone systems, laptops and privately-owned devices used to access school networks. This must ensure that antivirus software is regularly updated, suitable for the task of identifying malware and protecting school systems and data from malware attacks.

## Backup Strategy

Backups are taken for the purposes of disaster recovery; they are not intended as a method to recover work lost by individual students through user error. All data is backed up every night using an incremental strategy. Once a week, all data is backed up in full; this is kept until backup storage capacity necessitates an overwrite which is usually 9-12 months and never less than 6 months.
All backups are kept in a remote location:

- Codsall: in the music centre
- Bilbrook: at Perton (transferred by VPN)
- Perton: at Bilbrook (transferred by VPN)

All backups are checked to ensure that they have been successful. The backup mechanism is tested once a year in a virtualised environment to check its reliability.

## 'Bring Your Own Device' Policy

Codsall High Federation of Schools grants its students and employees the privilege of purchasing and using smartphones and tablets of their choosing at school for their convenience, subject to relevant Mobile Phone Policies in place at federation schools. Codsall High Federation of Schools

reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined herein. This policy is intended to protect the security and integrity of Codsall High Federation of Schools' data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. Codsall High Federation of Schools' employees and students must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the school network.

## Acceptable Use

- The schools define acceptable use as activities that directly or indirectly support the students' education.
- The schools define acceptable personal use during work time as reasonable and limited personal communication or recreation.
- Employees and students are blocked from accessing certain websites during work hours/while connected to the school network at the discretion of the Network Manager and Executive Headteacher.

Devices may not be used at any time to:

- Store or transmit illicit materials
- Store or transmit proprietary information belonging to another company
- Harass others
- Engage in external business activities

Employees and students may use their mobile device to access the following school-owned resources: email, calendars, contacts, documents and software packages (where licensing restrictions permit) subject to restrictions on time and location of mobile phone use that may be in place in individual schools' Mobile Phone policies.

## Devices and Support

- Smartphones including iPhone, Android and Windows phones are allowed, subject to restrictions in the relevant school's Mobile Phone Policy that may apply to students' use of mobile phones on school site. Tablets including iPad, Android and Windows Surface are allowed.
- Connectivity issues are supported by ICT; employees and students should contact the device manufacturer or their carrier for operating system or hardware-related issues. ICT support staff will assist staff and students in configuring devices to connect to school wifi access points.

## Security

- In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the school's network. Password complexity is referenced in *Password policy*
- The device must lock itself with a password or PIN if it's idle for five minutes.
- Employees' and students' access to school data will be limited, based on user profiles defined by ICT and automatically enforced.

## Risks/Liabilities/Disclaimers

- The schools reserve the right to disconnect devices or disable services without notification.
- Lost or stolen devices owned by the school must be reported to the ICT helpdesk soon as possible. Privately-owned devices that contain data owned by the school that have subsequently been lost, must also be reported to ICT.
- The employee or student is expected to use his or her devices in an ethical manner at all times and adhere to the Acceptable Use Policy.
- The employee or student is personally liable for all costs associated with his or her device.
- The employee or student assumes full liability for risks including, but not limited to, the partial or complete loss of school and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- Codsall High Federation of Schools reserves the right to take appropriate disciplinary action.

# Security & safety requirements for ICT systems

## Password policy

CHFS will enforce a policy of strong passwords for all staff users and users with elevated privileges, on the grounds that they regularly have access to sensitive personal information. Staff passwords should be:

- Alphanumeric, including a mix of upper and lower case letters
- contain at least one "special character" (such as $, %, #, ?, ! etc)
- at least 10 characters in length

*Passwords should never be:*

- written down
- easy to guess

ICT staff will periodically undertake password security exercises where staff and student passwords will be subjected to security testing procedures for the purposes of identifying users with weak

passwords and protecting school systems from unauthorised access by third parties who might seek to exploit users' weak passwords. Staff users will be required to change their password(s) in situations where periodic security testing identifies that weak passwords have been used, or where it is known or suspected that a user's password may have been compromised by unauthorised third parties.

## Unattended workstations

Staff screensavers will lock with a password after 60 minutes of inactivity . Staff must be mindful of what is being displayed on their screen and who can see it; leaving unlocked workstations with sensitive data such as email or SIMS applications active must be avoided

## Portable media

- Portable media such as USB devices may be used to transport files between home and school. ICT staff will use Group Policy to ensure that devices will be mounted "read only" when connecting to school computers unless the device is protected using suitable disk encryption (such as BitLocker).
- Any files containing personal information or other sensitive data may only be transported outside the CHFS on encrypted devices.
- When disposing of legacy portable hardware that may not have been encrypted in the past, staff should seek advice from the ICT support staff to ensure that any sensitive data is securely erased.
- As an alternative to portable media, staff are encouraged to make use of remote desktop connections which prevent the need to transport sensitive data on physical devices.

## File-type & software restrictions

The Network Manager will ensure appropriate security policies are in place to prevent unauthorised users from using file types that could bypass security measures or otherwise cause security problems. This includes but is not limited to: preventing the execution of non-whitelisted executable files or shell scripts; preventing the download of executable or software package files or harmful office macros.

## Physical security

As far as practicable, only authorised persons will be admitted to rooms that contain servers or provide access to data. Server rooms must be kept locked when unattended. Uninterruptible Power Supply (UPS) units will be used for servers and network cabinets.

## Internet use & filtering

The Network Manager will ensure that appropriate firewalls are in use at the extremities of the school networks to guard against nefarious actors gaining unauthorised access to school systems. Filtering proxy servers will also be used to ensure that all internet traffic is age-appropriate, safe to use and logged. Where staff or students become aware of inappropriate material being accessed on school systems, this should be reported to the ICT helpdesk: helpdesk@cc-hs.com. Social media including but not limited to Facebook & Twitter will be blocked for all students. Non-approved email systems such as Hotmail will be blocked to prevent cyberbullying and access to unauthorised materials. The school Acceptable Use Policy (AUP) is available as part of this document for staff and students; all persons using the network will be required to accept the *AUP* before they logon.
Parental permission will be required before any student is allowed to use school ICT facilities; this is managed through the home-school agreements and pre-admission procedures for each school.

## Monitoring system usage

Codsall High Federation of Schools is mindful of its obligations in regard to the monitoring of data on school networks and the potential for monitoring activity to contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act, 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. ICT support staff will be mindful of their obligations under law, including the Data Protection Act (2018) which incorporated the General Data Protection Regulations (GDPR) into UK law; monitoring of ICT system use for school business will be reasonable and proportionate, the purposes of protecting students from harm; complying with the law; and preventing unauthorised access to school ICT systems or private information.

In order to facilitate the monitoring of internet traffic passing through CHFS systems, ICT staff may deploy TLS certificate systems to act as 'man in the middle' providers when users access encrypted web traffic using the HTTPS protocol. Web browsers on school-operated devices will have the appropriate TLS certificate-signing authorities pre-installed and 'trusted' to facilitate such monitoring and this will be disclosed to users in the *AUP*. The school may only monitor authorised private use of a school computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of the protection of well-being or for the protection of the rights and freedoms of others. The Network Manager should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place. Users should be aware that the protocols discussed here in *Monitoring system usage* apply to all internet traffic at all times on CHFS workstations. Users will be informed that all ICT system usage is monitored as part of the AUP.

## Rules for ICT use by third parties

Under some circumstances, it may be desirable to grant third parties (that is, people who are neither staff, governors or students) access to school ICT systems, such as ICT service providers, potential staff attending interview or pre-employment induction, or potential students.

In general,

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- Copyright and intellectual property rights must be respected.
- Users must respect the work of others which might be stored in common areas on the system. Conversely, users should always try and store their files and data in their own secure area or on removable media. Files and data stored in common areas of the system must be transferred at the earliest opportunity to the users own area. Such files will be regularly removed from the system.
- The school ICT systems may not be used for private business purposes, unless the Executive Headteacher has given permission for that use. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in access privileges being revoked and could be used to inform decisions about potential employment or acceptance in the case of candidates for employment or admission.

Guidance for best practice for staff communication is included in the appendix: *E-mail & Internet use good practice for staff* and for *Classroom monitoring of students' ICT usage*, as is the *Acceptable Use Policy*.

# Appendix

## Acceptable Use Policy

This Acceptable Use Policy (AUP) applies to all users of ICT systems at the Codsall High Federation of Schools. In consenting to use ICT systems operated by CHFS, or connecting to systems operated by CHFS using privately-owned devices, all users agree to follow the best practices outlined below. Prior to logging in to CHFS-owned workstations, users are required to confirm their compliance with and acceptance of the AUP.

At all times, users will act in good faith to maintain the security and privacy of school ICT systems and users' private data. Users agree to comply with any obligations outlined in the ICT Security Policy.

Students are required to accept and comply with the student usage particulars, that they will:

- only use their own login and password, and keep their password secret
- only user the computers for school related study
- be responsible for their own files and understand that the school will check files and monitor the websites visited
- only contact people they know or those whom the teacher has approved of
- will not give out any personal information such as mobile phone numbers or addresses, or arrange to meet strangers; report any contact from people outside of school immediately to an adult
- only enter sites on the internet that have been authorised by the teacher; not enter social media websites or play internet games
- only store files for school use on the network
- not plagiarise other pupils' electronic work or by using the internet

Staff agree that:
They will protect private information held in their capacity as an employee of the school, making use of confidential waste bins to dispose of printed media and adhering to the requirements in the ICT Security Policy for electronic media. Their use of ICT systems will be legal, in compliance with all school policies and for the purposes of their job role.

All users accept that their usage of systems may be monitored and in particular that 'man in the middle'-style encryption interception may be used to ensure website access is compliant with the school's filtering of illicit content. Users understand and accept the principles of monitoring covered in the ICT Security Policy.

## Classroom monitoring of students' ICT usage

Staff should ensure they are able to visually monitor pupils' use of computers at school and that there is always a responsible person present. Monitoring software such as HP Tutor may be used to facilitate in-lesson monitoring by teaching staff. ICT will log access to the network using software tools, and in particular, logs of network and internet traffic will be kept for the purposes of generating an audit trail of student and staff ICT usage.

Where staff or students' use of ICT systems could constitute illegal activity, staff are duty bound to bring this to the attention of the Executive Headteacher or other members of the Senior Leadership Team so that appropriate action can be taken; where staff identify activity that constitutes a safeguarding concern, they must immediately raise this with the Designated Safeguarding Lead.

## E-mail & Internet use good practice for staff

The following guidelines (some of which also apply to other forms of correspondence) advise what is and what is not good practice when using e-mail and other similar systems to communicate.

Staff should:

- treat E-mail as they would a letter, remembering that they can be forwarded/ copied to others;
- only contact children for professional reasons and in accordance with school policy;
- use "BCC" fields when addressing emails to multiple recipients whose confidentiality needs to be maintained.

Staff should not:

- use internet or web-based communication channels to send students messages of a 'personal' nature
- use or access social networking sites of children or young people
- use internet or web-based social media channels to bring Staffordshire County Council or the federation or individual school's name into disrepute;