WHICKHAM SCHOOL

ICT Data Security Policy

Contents

Policy Review

Last reviewed	By who	Next review
October 2021	N Sheen	October 2024
August 2022	N Sheen	August 2025

1. Aim

ICT Data Security Policies are important in setting agreed standards to ensure data security and safety. Policies and sanctions should be understood and embedded within normal practice.
This policy applies to all Whickham School staff and governors whenever and wherever they are using school data.

Any user using Whickham School data is required to comply with this ICT Data Security Policy. Failure or non-compliance may result in disciplinary action and / or legal action being taken upon individuals or groups of individuals.

The objectives of this policy are to:

1. Ensure the protection of confidentiality, integrity and availability of school information and assets.
2. Ensure all users are aware of *and* fully comply with all relevant legislation.
3. Ensure that all staff understand the need for information and ICT security and their own responsibilities in this respect.

2. Definitions

Information - covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

Personal Data - Any data which can be used to identify a living person. This includes names, birthday and anniversary dates, addresses, telephone numbers, fax numbers, email addresses and so on. It applies only to that data which is held, or intended to be held, on computers ('equipment operating automatically in response to instructions given for that purpose'), or held in a 'relevant filing system'. This includes paper filing systems.

Strong Password – Password which is 8 characters minimum length, contains upper and lower case alphabetical characters and numbers or punctuation characters. It should not contain dictionary words, the owner's date of birth or car registration number.

Encryption – Process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

3. Responsibilities

- The School shall be registered with the Information Commissioner's Office (ICO) under the 2018 Data Protection Act.
- Users of the school's data & ICT Systems must comply with the requirements of the ICT Data Security Policy.
- The School's Leadership Team shall review this document at least annually.
- Users shall be responsible for notifying the Headteacher and/or Deputy Head (in charge of data) of any suspected or actual breach of data security.
- The Headteacher shall inform both the ICO and the Chair of Governors if there are any serious losses of personal data

- 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.
- No personal data shall be taken from the school unless it is on encrypted media. This includes, but is not exclusive to, laptop computers, netbooks, external hard disks, memory sticks and Personal Digital Assistants (PDAs) & other removable media. Encrypted USB keys are issued to all members of staff. If you have not received an Encrypted USB key please request one from the ICT Support Team if you intend on taking any school data off site.
- Users shall not publish spreadsheets, databases or other documents containing personal data on externally accessible web unless these documents are encrypted.

4. Physical Security

- As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.
- Server rooms must be kept locked when unattended.
- All school owned ICT equipment and software should be recorded and an inventory maintained.
- Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.
- **Do not** leave any form of sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.
- **Do not** give out sensitive information or personal data unless the recipient is authorised to receive it.
- **Do not** send sensitive/personal information via e-mail or post without suitable security measures being applied.
- Ensure sensitive information and personal data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks, and following the school's policy for agreed retention periods and recording destruction of records at the end of their life.

5. System Security

- Users **shall not** make, distribute or use unlicensed software or data.
- Users must ensure they have authorisation for private use of the school's computer facilities.
- Password storage and security must be as set out in the acceptable use policy.
- Users who regularly access personal data shall have a unique user ID and a strong password that is renewed at least termly.

- Passwords **shall not** be revealed to unauthorised persons.
- Passwords **shall not** be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data.
- Passwords shall be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.

6. Disposal of Equipment

- The School shall ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data.
- It is important to ensure that any software remaining on a PC being relinquished for reuse 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 shall ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.

7. Data security do's and don'ts

This guide is for anyone working in Whickham School who collects, manages, transfers or uses data about learners, staff or other individuals during the course of their work. Its aim is to raise your awareness of where potential breaches of security could occur. Following these 'dos and don'ts' will help you to prevent data from being lost or used in a way which may cause individuals harm or distress and/or prevent any fines your organisation may suffer if you lose personal data about individuals.

There are plenty of things that you should do (or not do) that will greatly reduce the risks of sensitive information going missing or being obtained illegally. Many of these 'dos and don'ts' will apply to how you handle your own personal information. Using these practices will help you to protect your own privacy. We have separated these points into different areas to make it easier for you to refer back to.

7.1.Working online

Do

- make sure that you follow Whickham School's policies (see AUP).
- make sure that you keep any computers that you own up to date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). Get advice from the ICT Support Team if you need help.
- only visit websites that are allowed by Whickham School. Remember, the websites you visit may be monitored and recorded.
- make sure that you only install software that the ICT Support Team has checked and approved.
- be wary of links to websites in emails, especially if the email is unsolicited.
- only download files or programs from sources you trust. If in doubt, talk to the ICT Support Team.
- Ensure you follow the schools AUP (Acceptable Use Policy) and Data Protection Policy.

7.2. Email and messaging

Do

- read the AUP and in particular the section relating to email usage
- report any spam or phishing emails to the ICT Support Team that are not blocked or filtered

Don't

- click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on.
- turn off any email security measures that the ICT Support Team has put in place or recommended
- email sensitive information or personal data unless you know it is encrypted. Talk to the ICT Support Team for advice.
- try to bypass Whickham School's security measures to access your email off-site (for example, forwarding email to a personal account)
- reply to chain emails.

7.3. Passwords

Do

- follow your organisation's AUP and ICT Data Security Policies
- use a strong password following the School's protocol of 4 random words
- make your password easy to remember, but hard to guess
- choose a password that is quick to type
- use a mnemonic (such as a rhyme, acronym or phrase) to help you remember your password.
- Change your password(s) if you think someone may have found out what they are.

Don't

- share your passwords with anyone else
- write your passwords down
- use your work passwords for your own personal online accounts
- save passwords in web browsers if offered to do so
- use your username as a password
- use names as passwords
- email your password or share it in an instant message.

7.4. Laptops

Do

- shut down your laptop using the 'Shut Down' or 'Turn Off' option
- try to prevent people from watching you enter passwords or view sensitive information or personal data.
- turn off and store your laptop securely (if travelling, use your hotel's safe)
- use a physical laptop lock if available to prevent theft
- lock your desktop when leaving your laptop unattended
- make sure your laptop is protected with encryption software.

Don't

- leave your laptop unattended unless you trust the physical security in place
- use public wireless hotspots – they are not secure

- leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot.
- let unauthorised people use your laptop
- use hibernate or standby.

7.5. Sending and sharing

Do

- be aware of who you are allowed to share information with. Check with the ICT Support Team or Deputy Headteacher if you are unsure.
- ask third parties how they will protect sensitive or personal information once it has been passed to them
- encrypt all removable media (USB pen drives, CDs, portable drives) taken outside your organisation or sent by post or courier.

Don't

- send sensitive information or personal data (even if encrypted) on removable media (USB pen drives, CDs, portable drives) if secure remote access is available
- send sensitive information or personal data by email unless it is encrypted
- place protective labels on outside envelopes. Use an inner envelope if necessary. This means that people can't see from the outside that the envelope contains sensitive information.
- assume that third-party organisations know how your information should be protected.

7.6. Working onsite

Do

- lock sensitive information away when left unattended
- use a lock for your laptop to help prevent opportunistic theft.

Don't

- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room.

7.7. Working offsite

Do

- only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above.
- wherever possible access data remotely instead of taking it off-site
- be aware of your location and take appropriate action to reduce the risk of theft
- make sure you sign out completely from any services you have used
- try to reduce the risk of people looking at what you are working with