WOODBRIDGE HIGH SCHOOL

ICT Data Security Policy

Updated: Autumn 2026

Summary:

The objectives of this Policy, which is intended for all personnel, including governors, who use or support the school's ICT systems or data, are to:

- Ensure the protection of confidentiality, integrity and availability of school information/assets.
- Ensure all users are aware of and fully comply with key legislation.
- Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.

Definitions:

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

Personal Data - Any data which can be used to identify a natural 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'.

Strong Password – A password should be a minimum of 8 characters in length, contain upper- and lower-case alphabetical characters and numbers or punctuation characters. It should not contain personal details relating to the owner, such as name, date of birth, address or car registration number or the name of a close relative or friend.

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

Responsibilities:

- The School is registered with the Information Commissioner's Office (ICO) under the UK Data Protection legislation.
- The Headteacher or Data Protection Officer (DPO) shall inform both the ICO and the Director of Children's Services, London Borough of Redbridge, if a data breach poses a risk to individuals' rights and freedoms. This task can be delegated to a member of the Leadership Group.
- Users shall be responsible for notifying the IT Support Team, Deputy Headteacher i/c ICT and DPO of any suspected or actual breach of ICT data security.
- Users of the school's ICT systems and data must comply with the requirements of the ICT Data Security Policy.
- The School's Leadership Group shall review this document annually.
- Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.

- No personal data shall be taken from the school unless it is on encrypted media. This includes, but is not limited to: laptop computers, tablet devices, external hard disks, memory sticks, smart phones and other removable media.
- Remote access to information and personal data shall only be provided through an encrypted link and users shall require a strong password that is renewed at least termly.
- Users shall not publish spreadsheets, databases or other documents containing personal data on externally accessible web sites unless these documents are encrypted.

Physical Security:

- As far as practicable, only authorised persons should be admitted to rooms that contain servers
- Server rooms must be kept locked when unattended.
- Appropriate arrangements must be 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.
- All school-owned ICT equipment and software is recorded and an inventory maintained.
- Uninterruptible Power Supply (UPS) units are used for servers and network cabinets.
- Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.
- **Do not** leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer, including outside school environments (e.g. home)
- **Do not** give out sensitive information 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 personal data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.

System Security:

- Users **shall not** make, distribute or use unlicensed software or data.
- Users **shall not** make or send threatening, offensive or harassing messages.
- Users **shall not** create, possess or distribute obscene or offensive material.
- Users must ensure they have authorisation for private use of the school's computer facilities.
- Passwords should be memorised. If passwords must be written down, they should be kept in a secure location.
- 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 they are affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.
- Regular backups of data, in accordance with the recommended backup strategy, must be maintained.
- Permission is required for the deletion of folders and files where such an action may compromise the school's data systems and structures
- Security copies should be regularly tested to ensure they enable data restoration in the event of system failure.
- Security copies should be clearly marked and stored in a fireproof location and/or off site.

Virus Protection:

- The school ensures that current and up-to-date anti-virus software is applied to all school ICT systems.
- Laptop users shall ensure they update their virus protection at least weekly.
- Any suspected or actual virus infection must be reported immediately to IT Support and Deputy Headteacher in charge of ICT, and that computer shall not be reconnected to the school network until the infection is removed.

Disposal of Equipment:

- The School shall ensure any personal data or software is erased from a computer or device 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 is 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.

Approval: Approved via Full GB Chair's Action on 1st October 2026 in advance of the F&GP Committee Meeting on 6th October 2026

Date of Next Review: Autumn 2027

Reviewer: Mr J. Clifton (Deputy Headteacher)