INFORMATION SECURITY POLICY

1. Introduction and General Expectations

1.1. Scope and Purpose

1.1.1. This policy applies to **all users** within the Wrekin College (the College'), which includes Wrekin Senior and Wrekin Prep, as well as temporary users, visitors, and third-party partners.

1.1.2. The policy covers **all forms of information** - digital (text, video, audio, email, files) and physical (spoken, written on paper, stored in cabinets).

1.1.3. The purpose of this policy is to protect the integrity, privacy, and reputation of the College, protect employees, and ensure the College is protected from legal liability.

1.2. Compliance

Compliance with this document is **compulsory**.

1.2.1. **Legal Requirements:** All information must be used legally, complying with UK and European law, including the **UK General Data Protection Regulation** (UK GDPR) and the **Data Protection Act** (DPA 2018) and the **Computer Misuse Act** (CMA).

1.2.2. **Protecting Confidentiality:** Personal, confidential, or sensitive information must always be protected, especially when removed from school premises (physically or electronically) or when transmitted outside the College.

1.2.3. **Reporting Breaches:** Users must report any attempted security breaches. If a password is compromised, the Information Security Officer must be notified and the password changed immediately. Losses, theft, or damage to assets that compromise security must be reported immediately to the Information Security Officer.

1.2.4. **Consequences:** Breaches will be fully investigated. Violations may lead to disciplinary action.

1.2.5. Seeking Help: If you suspect you or someone else is being abused via email, report the individual to the Headmaster or Head of Wrekin Prep.

1.3. Responsibilities

Roles	Staff	Responsibilities
Data Protection Lead	Bursar	● Together with Headmaster and Governors, liable for all aspects of the College's information security. ● Respond to information security incidents.
Information Security Officer	Head of IT	● Implement and maintain Security Policy documents. ● Responsible for the security of the IT infrastructure. ● Plan against security threats, vulnerabilities, and risks. ● Ensure security training programs. ● Ensure IT infrastructure supports Security Policies. ● Help in disaster recovery plans.
Information Asset Owners	Typically senior and middle managers, head of department or functional area	● Know what information the assets hold, and what enters and leaves and why. ● Know who has access and why, and ensure their use of the asset is monitored. ● Understand and address risks to the asset. ● Assist DPL with Subject Access Requests.
IT Team		● Implements and operates IT security. ● Implements the privileges and access rights to the resources. ● Supports Security Policies.
Users	All Staff	● Meet Security Policies. ● Report any attempted security breaches.

2. Policy Enforcement and Sanctions

2.1. Methods of Enforcement Breaches of information security will be fully investigated. Enforcement Mechanisms include:

2.1.1. Systematic Filtering and Monitoring: Inbound and outbound traffic is filtered using **Fortinet's Fortiguard cloud filtering system (https:// www.fortiguard.com/services/wf)**. Internet traffic is monitored using **Sensornet Monitoring Service** and overseen by the **DSL Team**. The College has the right to monitor and disclose staff's online history.

2.1.2. Access Control Monitoring: Yearly reviews of system users and permissions / roles takes place. Checks of key systems such as backups, firewall rules and

server updates take place regularly.

2.1.3. **Email Monitoring:** The College reserves the right, at the behest of the Headmaster, Bursar or Head of Wrekin Prep, to **monitor and access the College email**. Purposes for monitoring include investigating or detecting unauthorised use and preventing or detecting crime.

2.2. **Nature of Sanctions** Violations of the policies defined in this document **may lead to disciplinary actions**. The use of the email system in specific prohibited ways (e.g., transmitting material that is abusive or discriminatory) constitutes **gross misconduct**. The school will take no responsibility for any offence caused by staff members downloading, viewing, or forwarding inappropriate emails.

3. Access Control and Passwords

This section governs secure access to IT services and infrastructure.

3.1. **Access Rules:** Access to IT systems or data must be requested via senior management. Access is granted under the **principle of "less privilege"**—meaning you only receive the minimum access rights required for your job function.

3.2. **Password Security:** Systems handling valuable digital information must be protected with a password.

3.2.1. Passwords ideally should have a **minimum length of twelve characters**. (For mobile phones there must be a minimum of a six figure password).

3.2.2. Passwords should consist of **three random words** and include letters (upper and lower case), numbers, and special characters.

3.2.3. **Two-step (multi-factor) verification** should be enabled where available and must be used for remote access.

3.3. **Usage:** Do not share passwords. If a session is idle for 10 minutes, you will be required to re-authenticate.

3.4. **Data Storage:** Personal Identifiable Information (PII), whether paper or digital, must be securely stored in lockable cabinets/cupboards or encrypted; password-protected online platforms are to be used.

3.5. **Removable Media:** Staff **cannot use USB sticks or SD cards** without permission from the IT department or senior management. Personal data should **never** be stored on such devices without encryption.

4. Equipment, Software, and Physical Security

4.1. Assets and Equipment (Desktops, Laptops, Mobile Devices)

4.1.1. Usage and Care: Users are responsible for preserving and correctly using assigned assets. Do not drink or eat near the equipment.

4.1.2. Security: You must **lock your laptop or desktop screen** when leaving the room, even if briefly.

4.1.3. Installation and upgrades: Only the IT Team is authorised to maintain, upgrade, or change the configuration of IT assets. Users must not install unauthorised software or modify hardware. All software must be centrally purchased and correctly licensed.

4.1.4. Portable Devices: Special care must be taken to protect school portable assets (laptops & mobiles) from theft, extreme temperatures, magnetic fields, and falls. When flying, school portable equipment must remain in your possession as hand luggage. Encryption and passwords should be implemented on portable assets.

4.1.5. Lost or Stolen: Any school owned devices lost or stolen should be reported to the Information Security Officer as soon as possible.

4.2. Physical Security

4.2.1. Access: Staff must challenge anyone not wearing a badge in secure areas. Visitors must sign in and out, wear an identification badge, and be monitored by staff if required.

4.2.2. Secure Storage: Offices and buildings with classrooms that house IT equipment must be locked when not in use. Paper storing confidential information must be secured (e.g., locked filing cabinets/safes) or placed in the white disposal bags provided by facilities when needing to be destroyed.

4.2.3. Data Location: Data should be stored on network file servers or approved cloud services, not locally on a device, to ensure recovery and integrity.

5. Network and Remote Access

5.1. Antivirus and Vulnerability Management

5.1.1. Antivirus: All computers and devices with access to a school network must have an antivirus client installed. School owned equipment is protected by Avast Business Hub with real-time protection and virus definitions which update daily. Staff are not able to disable central protection on school-owned devices.

5.1.2. **Backups:** Regular backups take place daily and are cloud based via Redstor including immutable backup (offline/inaccessible backup)

5.1.3. **VLANS** (Virtual Local Area Networks) logically segment the network - this improves network performance and security.

5.1.4. **Updates (Patching):** High-risk or critical security updates for operating systems and applications must be installed within **14 days** of them becoming available. Staff must update individual devices when notified that a restart is required. Software or online platforms which are not correctly licensed or owned by the school should not be used.

5.1.5. **Vulnerability Scans**: Scans are run once a year on networks at the College.

5.2. Remote Access

5.2.1. **VPN Requirement:** As all primary systems used by the school are cloud based there is no VPN access offered or provided to staff externally.

5.2.2. **Authentication:** Multi-factor authentication is required. This is to be set up by all staff using an authenticator app.

5.2.3. **Data Handling: No personal data should be downloaded** to a laptop's hard drive; access files by logging into the school VPN. The hard drive of the device used for remote access must be encrypted.

5.3. Internet and Mobile Usage

5.3.1. **Internet Use:** Access to the Internet is permitted. Personal use is allowed in your own time (e.g., lunch break) provided it does not interfere with your work. Internet traffic is filtered and monitored.

5.3.2. **Prohibited Use:** Accessing inappropriate sites is prohibited. This includes pornography, peer-to-peer networks, online gaming/betting, 'money making' sites, or running a private business. Be aware that staff online history may be monitored and disclosed.

5.3.3. **BYOD (Staff/Governors):** Personal devices connecting to College Wi-Fi must use **only** the designated WREKINGUEST College Wi-Fi network. Staff are permitted to access Gmail from their personal mobile devices. Devices used for school services must be password protected. Only Google apps should be used to access school data on personal devices, allowing for data wiping if the device is lost/stolen.

5.3.4. Mobile Connectivity: When not on the school network and using school data, use 3G, 4G, or 5G connectivity; **do not connect to public Wi-Fi hotspots**.

5.3.5. Pupils: Pupils are only allowed to use mobiles in line with the College's mobile use for pupil regulations.

6. Email Policy

This section defines the proper and secure use of electronic mail.

6.1. Professional Conduct (Gross Misconduct): Do not create, transmit, or forward material that is offensive, obscene, indecent, defamatory, abusive, or discriminatory (including on grounds of sex, age, disability, etc.). Do not use emoticons in exchanges with parents.

6.2. Format and Tone: All electronic communication with parents must be **formal**, beginning with a formal salutation, even if parents address staff informally. All emails should have a subject message reflecting the contents.

6.3. School Business: Only conduct school business on your school email account.

6.4. Communication with Pupils: Do not communicate with pupils on their personal emails in any circumstances. All communications should be directed to parents.

6.5. Confidentiality: Do not send or forward trivial messages or jokes that could cause IT system delays. Personal information whose disclosure could cause harm must not be sent by email unless correct encryption procedures have been followed.

6.6. Security: Do not open suspicious attachments or emails from unknown sources. If responding to an email with a long trail, the secure approach is to cut and paste the relevant part of the email into a new mail and respond to only that new email.

6.7. Disclosure Awareness: Be aware that anything put in an email is potentially disclosable as evidence in court or subject to a Subject Access Request under GDPR (including gossip).

6.8. Monitoring: College reserves the right to monitor and access staff email for purposes connected with school operation (e.g., detection of crime, monitoring standards, or accessing routine business when staff are absent).

Policy owner:	Bursar
Approved by:	Headmaster
Date of last review:	September 2026
Next review:	September 2027