Hedingham School & Sixth Form

Bring Your Own Device (BYOD) Policy 2025

New Policy

Approved by the Curriculum and Personnel Committee on:	-
Ratified by the Full Governing Body on:	**3 December 2025**
Next review due by:	-

Table of Contents

Introduction

Hedingham School recognises that technology offers significant benefits for teaching, learning, and operational efficiency, and we embrace its responsible use. This Bring Your Own Device (BYOD) policy enables staff, governors, students, and authorised visitors to use personal devices to access school systems while safeguarding our data and networks. It is informed by guidance from the UK Department for Education (DfE) and the National Cyber Security Centre (NCSC) to balance usability with security. BYOD usage introduces risks – such as malware, data loss or unauthorised access – so all users must adhere to the following requirements to protect themselves and the school.

This policy emphasises user compliance: the school will not apply intrusive technical controls (e.g. mobile device management software, laptop monitoring software) on personal devices but instead requires users to follow the rules and security precautions outlined below. Failure to do so may compromise school data and systems and will be treated seriously under our disciplinary procedures.

Scope and Purpose

This policy applies to all staff, governors, students, and guests or visitors who use a personally owned device to connect to the school's internet services or access school information (such as email, learning platforms like Seneca or Sparx, or any other Hedingham School systems). It covers use of personal smartphones, tablets, laptops, desktops, wearable devices, or any similar technology ("mobile devices") on school premises and use of personal devices off-site when accessing school accounts or data.

Its purpose is to ensure that any personal device used for school-related activities is operated in a secure, responsible manner that protects school data, maintains network security, and complies with all relevant policies and legal requirements. By using a personal device with school systems, users agree to abide by this policy and understand that non-compliance may result in loss of access or further action.

Related Policies and Legal Compliance

This BYOD policy is designed to complement existing school policies and legal obligations. It should be read in conjunction with our Acceptable Use Policy (AUP) and the Essex County Council Data Protection Policy, as well as the Staff Code of Conduct and E-Safety policies. All conditions of the AUP apply equally to personal devices – for example, prohibitions on inappropriate material, hacking, or bypassing security controls also extend to any BYOD usage. Compliance with this policy is also an important part of the school's overall compliance with data protection law (UK GDPR/Data Protection Act 2018). The school remains the data controller for information accessed or processed on personal devices and is responsible for protecting that data. Therefore, users must follow this policy to enable the school to meet its statutory duties for data security and safeguarding. The policy aligns with DfE standards (including *Keeping Children Safe in Education* requirements for information security, filtering and monitoring) and NCSC best practices to ensure BYOD use does not introduce unacceptable risk.

Roles and Responsibilities Associated with this Policy

The following personnel have a responsibility with regards to this policy. Their specific roles and responsibilities are outlined below.

Role	Staff	Responsibility
Governing Board	Governors	Responsible for approving this policy and ensuring the school meets its attendance and safeguarding duties.
Cyber Security Governor Lead	To be agreed at Full Governors on the	This member of the governing body has overall responsibility for overseeing Cyber Security at the school on behalf of the governing board.
Headteacher	Mr P Finch	Oversees the overall strategy with relation to Cyber Security at the school.
Cyber Security Lead	Mr R Daniels	Works alongside the Network Manager to ensure the school is compliant with its cyber security requirements and develops policy to support this.
Network Manager	Mr S Jarvis	Ensures that all technical aspects of the school are compliant with current cyber security requirements and recommendations. Helps to develop policy alongside Cyber Security Lead.
Network Technician	Mr B Smith	Provides support and guidance to the Network Manage to ensure that the school remains secure against current cyber security requirements and recommendations.
Staff	All Staff	Have a day-to-day responsibility to consider their actions before utilising school networks and/or systems as part of their roles. Is what they are doing safe and not going to put the school into a situation where a cyber security incident could occur.

User Responsibilities and Acceptable Use

All users are expected to use their personal devices in a safe, ethical, and lawful manner when accessing school systems. The following rules apply to ensure acceptable use and protect our community:

- **Authorisation to Connect:** You must obtain specific permission from the school (IT department or other designated authority) before connecting any personal device to the school's network or IT systems. This includes joining the school Wi-Fi or accessing school email and apps from a new device. The school reserves the right to refuse or revoke access for any personal device that is deemed insecure or non-compliant with this policy.

- **Usage Locations and Times:** Personal devices (e.g. laptops/tablets) may only be used on school premises in accordance with school rules. Students are not permitted to use personal devices during lessons or in restricted areas/times unless explicitly allowed for learning purposes (this does not include Mobile Phone devices as these are prohibited within the school building). Staff and visitors may use devices in staff offices or common areas, provided it does not disrupt school activities. Personal use of devices during working hours should be minimal and confined to break times so as not to interfere with professional duties. The school's separate BYOD Wi-Fi network (or guest network) must be used for internet access on personal devices; connecting a private device to any secure internal network segment is prohibited unless approved by IT.

- **Prohibited Activities:** Users must not use personal devices in any way that violates school policies or the law. Examples of strictly prohibited actions include accessing or sharing illegal or inappropriate material; attempting to bypass school security filters or firewalls (e.g. via proxy sites or VPNs); using personal devices to bully or harass; or recording or photographing students, staff, or school activities without permission. In particular, no photos or videos of students or staff may be taken on personal devices during school activities, and no sensitive personal information (such as student data) should be stored in personal apps or unapproved cloud services. Staff must also never use personal devices to contact or communicate with pupils (e.g. no personal phone calls, texts or messaging with students) – all communication must remain on official school platforms.

- **Safeguarding and Appropriate Use:** Any use of personal devices by students is subject to the same monitoring and filtering as school devices. Students must only access the internet through the school's filtered Wi-Fi when on site, to ensure compliance with safeguarding filters. Under no circumstances should students use personal mobile data (3G/4G/5G) or personal hotspots on school devices to bypass school filtering while on school grounds. Staff should also avoid connecting school-owned devices to personal hotspots, as this circumvents security measures. The school may impose additional restrictions on device use in certain areas. All users are reminded that their behaviour online via personal devices must reflect the same standards of respect and professionalism expected in person.

By following the above rules, users help maintain a safe and productive environment for everyone. The school may update acceptable use requirements as needed, and will inform users of any changes – however, it is ultimately each user's responsibility to stay up-to-date and compliant with the latest policy version.

Security Requirements for Personal Devices

Because personal devices are not managed by the school's IT department, each user is responsible for the security of their own device. To protect school data and services, all personal devices used under this policy must meet the following security standards:

- **Supported Operating Systems:** Devices must run an operating system (OS) that is vendor-supported and up to date with security patches. Any device with an obsolete, unpatched or end-of-life OS (for example, an outdated version of Windows, macOS, iOS or Android that no longer receives security updates) is not permitted to connect to school systems. The OS and all apps should be kept updated to their latest versions to reduce vulnerabilities. The school maintains a list of approved or minimum OS versions – for instance, only modern Windows and Mac versions that are still supported by the manufacturer, and mobile devices running recent iOS or Android releases.

- **Device Configuration and Protection:** Users must secure their devices against unauthorised access. At a minimum, a personal device must be locked with a PIN, passcode, password or equivalent authentication, and configured to auto-lock after a short period of inactivity. It is the user's responsibility to prevent others from using their device to access school information – for example, family members or friends should not be allowed to use a device in a way that could reveal school data. All devices should have encryption enabled where possible (e.g. full-disk encryption on laptops or the default encryption on modern smartphones) to protect data at rest.

- **Anti-Malware Measures:** Any laptop or device capable of running anti-virus/anti-malware software must have a reputable security software installed and kept up-to-date. Users should ensure their device has active virus protection with the latest virus definitions and should run regular scans. On platforms like Android, an anti-malware app is recommended. Built-in security features (such as Windows Defender or macOS XProtect) should be kept enabled. The device's firewall should remain active to block unauthorised access.

- **No Jailbreaking or Rooting:** Devices that have been jailbroken, rooted, or run unofficial "custom ROM" operating systems are strictly forbidden from accessing school networks or data. Such modifications bypass built-in security controls and pose an unacceptable risk. The school may employ technical solutions to detect and block rooted/jailbroken devices if they attempt to connect. Users must not attempt to circumvent the security settings of their devices or of the school's systems.

- **Network Connection:** Personal devices should connect only through the school's designated BYOD/guest Wi-Fi network (which is isolated and filtered) when on-site. Direct wired connection of personal laptops to the school network is not allowed without explicit permission. The network is segmented to protect school systems,

and personal devices may be placed on a separate VLAN with internet-only access for security. Users must not install any unmanaged network hardware or create personal wireless hotspots on school premises that could bridge into the school network, as this undermines security controls.

- **Physical Security and Electrical Safety:** Users should treat their personal device with the same care as any valuable item on campus. Devices must never be left unattended in unsecured locations. Especially in classroom settings, staff must ensure personal devices are kept out of students' reach and secured (e.g. locked in a drawer or cabinet when not in use). If a personal laptop or device needs to be plugged into the school's mains power, it must be Portable Appliance Tested (PAT) for electrical safety before use on site. (Please contact Site Management or IT Support to arrange a PAT test if needed.) The school accepts no responsibility for personal devices' functionality or maintenance – ensuring the device remains safe to use is the owner's duty.

- **Additional Controls:** Where available and appropriate, the school may require enabling certain security features. For example, if staff are accessing school email or files on a personal mobile, the school's cloud system may enforce a basic security policy (such as requiring a device password or blocking access from devices with outdated OS). All users should also enable Multi-Factor Authentication (MFA) on their school accounts and applications wherever possible, as this is highly recommended by the NCSC to prevent unauthorised access. The Network Manager may periodically remind or assist users to configure such measures.

By meeting the above security requirements, users help protect both their own personal information and the school's data. Users who cannot meet these requirements must not use their device for school purposes. The school reserves the right to audit compliance (through automated checks or scans) and to deny network access to any device that is found to be non-compliant or poses a security threat.

Use of School Data and Systems on Personal Devices

When a personal device is used to access school resources, special care must be taken to protect school data and ensure privacy. The following rules govern how school information is accessed, stored, or transmitted on BYOD devices:

- **No Local Storage of Sensitive Data:** Users must not store sensitive or confidential school data on personal devices or unapproved storage media. "Sensitive data" includes, for example, any information about students or staff, personal identifiers, academic records, special category personal data, or any other information defined by the school's Data Protection policy as confidential. Such data should only be accessed through secure school systems and not downloaded unless absolutely necessary. In particular, it is prohibited to save school files to personal cloud services or unencrypted USB drives outside the school's control. The school's Microsoft 365 (OneDrive, SharePoint, Teams) or other approved platforms **must** be used for storing and managing school documents. If a user does inadvertently create or download any school-related file on a personal device, they should delete it as soon as it is no longer

needed (or move it to an approved secure location) and ensure it is not accessible to others in the meantime.

- **Use of Official Apps/Systems:** Wherever possible, users should utilise the school's official apps or web portals rather than personal software for accessing school data. For example, use the Outlook Web App or official email client for school email, rather than transferring emails to a personal email account. Do not sync school contacts or calendars with personal accounts. Using only sanctioned applications helps maintain security barriers between school data and personal data. The principle of data minimisation applies – only access the information you need, and do not copy or extract it unnecessarily.

- **Data Protection Compliance:** All BYOD users are expected to understand and follow the school's Data Protection Policy and the UK GDPR principles when handling personal data. Appropriate technical and organisational measures must be in place to prevent unauthorised or unlawful processing or disclosure of personal data accessed via your device. This includes ensuring that any personal device used has adequate security (as detailed in the section above) and that you do not expose data to anyone not authorised to see it. Remember that using a personal device for school purposes does not exempt you from data protection obligations – any personal data relating to individuals (students, parents, staff, etc.) must be treated with confidentiality and care, regardless of the device used. The Information Commissioner's Office (ICO) has explicit guidance on BYOD, and non-compliance can lead to regulatory action. In practice, this means never emailing personal data from a school account to a personal account; never using social media or consumer messaging apps to discuss identifiable individuals; and reporting any loss or potential breach of data immediately (see Incident Reporting below).

- **Separation of Personal and School Content:** Users should, where possible, keep school information separate from personal information on their device. For example, use different user profiles, or at least segregate school files in a dedicated folder. Do not back up school data alongside personal data to unapproved services. The goal is to ensure that if a device is lost, sold, or repaired, no school data is accidentally exposed, and that when a staff member or student leaves the school, all school data can be securely removed without affecting personal content.

- **No Unauthorised Recording or Transfer:** As noted in Acceptable Use, using personal devices to record audio, video, or images in school or during school activities is forbidden unless expressly authorised for a specific purpose. Similarly, you must not use your personal device to transfer school data to any third party or system not approved by the school. For example, do not download pupil information onto your personal laptop and then upload it to a non-school service. Any intentional unauthorised copying or exporting of school data is a serious breach of trust and policy. If you are unsure whether a certain use of data on your device is permitted, seek guidance from the Data Protection Officer (DPO) or Network Manager before proceeding.

- **Cloud Services and Email:** When accessing school cloud services (such as Office 365, Google Classroom, etc.) from a personal device, ensure you log out after use, especially on shared or family devices. Avoid selecting options that save your login credentials on a device that others might use. Do not integrate school email accounts into personal email apps that co-mingle personal and work emails unless the app can guarantee security (for instance, using Outlook app with a managed policy if provided). School email should never be auto forwarded to a personal email address. All use of school email and cloud on personal devices is still subject to the school's monitoring and data retention policies.

These guidelines ensure that personal devices do not become a weak link in our data protection chain. In summary: treat all school-related information on your own device with the same care and security as you would on a school-owned device. If in doubt about any practice, contact the Network Manager or DPO for advice. Users found to be mishandling personal data on their devices may be subject to investigation and action under our data protection and disciplinary policies.

Network Access, Monitoring and Privacy

Monitoring and Logging:

By connecting a personal device to the school's Wi-Fi or systems, you consent to monitoring and security checks as described here. The school will log details of devices and network usage for security, auditing, and filtering purposes. This means that the websites you visit, the duration of access, and any data transmitted through school networks can be recorded and may be reviewed by authorised IT or safeguarding staff.

Content of network traffic (including emails or form data submitted) may be captured by our monitoring systems or filters. The school employs these measures to detect improper activity, protect students, and ensure compliance with policies. Users should have no expectation of absolute privacy when using personal devices on the school network or when accessing school accounts. In line with our AUP, if there is reason to believe that a user is engaging in unlawful or policy-breaching activity via their device, the school reserves the right to inspect relevant communications or files to investigate. Monitoring will always be conducted in a reasonable manner and in accordance with applicable laws and regulations (such as the Investigatory Powers Act and data protection law). The school will normally inform individuals if their usage will be or has been monitored, and the scope of information collected, unless there are exceptional circumstances that make notification impossible or counter-productive (for example, as part of an investigation into suspected misconduct). All monitoring logs will be retained and protected in line with our data retention policies.

Security Testing:

In addition to general monitoring, the school may conduct periodic security sweeps or penetration tests on the BYOD network and any connected devices to identify vulnerabilities. For instance, IT may run network scans to detect devices with outdated software or known security issues. These scans do not access personal content on devices; they are intended to check device configurations (such as OS version, presence of required updates, etc.). By using BYOD, you agree to allow such security checks. Any device found to pose a serious threat (e.g. infected with malware or performing

suspicious network activity) may be temporarily blocked from the network, and the user will be notified to remedy the issue.

Privacy Considerations:

The school respects that your personal device may contain private information unrelated to school. Our monitoring is focused on school-related use and network traffic through school systems – we do not remotely access your device's personal files, nor activate cameras/microphones, etc., and we do not track your location. We also encourage users to mark any truly personal communications (e.g. a private email sent during break via school Wi-Fi) as such, to the extent possible. However, personal use of the school network is itself limited and any data transmitted through it can be monitored. If you wish to keep certain activities completely private, it is advisable to use your own network connection (outside school premises) and personal accounts rather than the school's. Note that even then, if those activities involve school data or are carried out in a way that impacts the school (for example, posting something online that brings the school into disrepute), they may still fall within the scope of school policies.

In summary, all device access is logged and subject to monitoring for legitimate purposes of safeguarding, security, and policy enforcement. The school will strike a fair balance between individual privacy and our duty to protect the school community. If you have any concerns about privacy or monitoring, please discuss them with IT or senior leadership. Ultimately, when using any device for school purposes, assume that your actions are visible to the school – and behave accordingly.

Incident Reporting and Response

Despite precautions, security incidents or data breaches can occur with personal devices (for example, a lost phone that was still logged into email, or a malware infection). It is crucial that users report any such incidents immediately so that the school can take appropriate action to mitigate risks. All staff, students, and visitors using BYOD must notify the school without delay in the event of:

- **Device Loss or Theft:** If your personal device used for school activities is lost, stolen, or otherwise goes missing – whether on or off school grounds – you must inform the Network Manager and Data Protection Officer immediately. Prompt reporting allows us to assess if any school data might be at risk and to initiate measures such as changing passwords, remotely disabling access tokens, or alerting authorities if needed. The school will log these incidents and treat them as a potential data security breach. Even if the device is recovered later, early notice is critical.

- **Compromise or Malware Infection:** If you suspect that your personal device has been compromised – for example, you discover malware/virus alerts, signs of unauthorised access, or you accidentally clicked a suspicious link that might have infected your device – stop using the device for any school-related work and report the issue to the Network Manager right away. Do not try to hide or ignore a security problem on your device, as this could worsen the impact. The Network Manager can assist in containing the threat (such as by revoking the device's access to school email until it is cleaned) and advise on next steps.

- **Unauthorised Access or Data Breach:** If you become aware that school data has been exposed or accessed by an unauthorised person through your device, this must be reported as a data breach to the Data Protection Officer (DPO) and the Network Manager immediately. Examples include: you find that a file containing personal data was uploaded to the wrong place, or someone else in your household saw confidential information on your screen, or your device was left unattended and might have been accessed. Quick reporting enables the school to fulfil its own legal obligations (such as breach notification to ICO within 72 hours, if required) and to take steps to protect affected individuals.

- **Policy Violations or Suspected Misuse:** If you realise you have accidentally violated this BYOD policy (for instance, you notice that automatic backups from your device uploaded a school document to your personal cloud), or if you witness someone else misusing a personal device in a way that risks security, you should report it. The aim is not to punish accidental mistakes but to remedy them. Self-reporting of a mistake will be handled with an emphasis on fixing the issue; however, deliberate or negligent breaches will invoke disciplinary processes.

When an incident is reported, the school will respond in line with our Cyber-Incident Response Plan and Data Breach Procedure. This may include technical measures (like disabling certain accounts or wiping data if possible), investigation by IT and the DPO, and notifications to leadership or external authorities as appropriate. Users are expected to cooperate fully in any investigation – for example, you may be asked to provide your device for inspection or to assist in identifying what data might have been compromised.

Remember that under the Data Protection Act, the school must keep personal data secure and respond to breaches; your prompt action in reporting incidents is a key part of that compliance. The school will maintain confidentiality to the extent possible and will only involve staff necessary to address the incident.

Enforcement and Disciplinary Consequences

Compliance with this BYOD policy is mandatory. The conditions set out are designed to protect both the individual user and the school. Failure to follow this policy may result in withdrawal of access to school IT systems and/or disciplinary action, depending on the severity of the breach and the user's role:

- **For Staff and Governors:** Any breach of this policy will be taken seriously. Minor or first-time violations may result in a reminder or retraining. Repeated or more serious violations (for example, knowingly using an unpatched, high-risk device, or sharing confidential data via a personal device) will lead to formal disciplinary procedures. Breaches that result in actual compromise of school data or safety – such as a data leak traced to an unsecured personal device, or a deliberate disabling of security features – may be considered as gross misconduct. The staff Code of Conduct and Disciplinary Policy will be referred to in such cases. The governing body will be informed of significant incidents involving governors or staff devices, and appropriate action taken.

- **For Students:** Misuse of personal devices or failure to comply with this policy will invoke the school's behaviour and e-safety disciplinary sanctions. For instance, a student who bypasses the school filter using their phone or who uses their device to harass others will face consequences outlined in the Behaviour Policy (this could include loss of device privileges, confiscation of the device by staff, parental meetings, or other penalties as appropriate). The school reserves the right to confiscate a student's personal device if it is being used in contravention of this policy or school rules, as per our standard procedure. In such cases, the device would be held securely and returned to the student or parent at an appropriate time. Persistent disregard for the BYOD rules may result in other disciplinary measures.

- **For Visitors/Guests:** Visitors (including parents, contractors, or volunteers) who violate the BYOD rules – for example, by connecting insecure devices or attempting to access unauthorised areas of the network – may have their access terminated immediately. Serious breaches by visitors will be escalated to the Headteacher and could result in the individual being denied future access to the premises or even reported to authorities if unlawful activity is detected. Guests are on school property at our discretion, and we expect them to uphold our security standards.

Liability:

It is important to note that users bring personal devices to use at school at their own risk. The school accepts no responsibility for loss, theft, or damage of personal devices on site or while in use for school activities. You should have appropriate insurance or take precautions if you are concerned about your device. The school also does not guarantee that its network access will be compatible with every device or that IT support will be able to troubleshoot personal hardware/software issues. The IT team will not install software on personal devices (aside from perhaps providing configuration instructions for email/Wi-Fi) and is not responsible for maintaining or repairing personal equipment. By participating in BYOD, users acknowledge these limitations.

However, the school does take responsibility for its own data and systems. This means if a personal device is suspected to be the source of a security breach, the school will investigate and take appropriate action, which could include requiring the user to cease using the device for school tasks, or in extreme cases, legal action. All users are reminded that they have a duty of care to protect school information. Non-compliance with this policy exposes both the individual and the school to risk, and will be handled accordingly.

Review and Policy Development

The BYOD policy will be reviewed regularly to ensure it remains effective and up-to-date with emerging cyber security threats, statutory requirements, and educational needs. Technology and cyber threats evolve quickly, as do DfE and NCSC recommendations, so the school will update this document as needed. Users will be notified of significant changes to the policy and may be required to re-acknowledge the policy whenever it is updated. Ultimately, it is each user's responsibility to ensure they read and understand the latest version of this policy. The school's senior leadership and governors will approve any major changes, ensuring the policy continues to align with our overall safeguarding and IT policies.

By following this BYOD policy, Hedingham School's community can enjoy the benefits of personal devices in our educational environment while maintaining strong protection of data and systems. All users are asked to familiarise themselves with these requirements and to uphold them consistently. The cooperation of every staff member, student, and visitor in adhering to these rules is essential for a safe and secure digital environment at our school. Thank you for your understanding and for doing your part to support cybersecurity and data protection at Hedingham School.