Heath House Prep School

STAFF ACCEPTABLE USE OF TECHNOLOGY POLICY AGREEMENT

Introduction

This Acceptable Use of Technology Policy (herein, 'Acceptable Use Policy' or 'AUP') applies to all staff at Heath House Preparatory School and covers use of all digital technologies in school i.e. email, SIMS, internet, network resources, learning platform, software, communication tools, social networking tools, school website, equipment and systems.

This Acceptable Use Policy has regard to the Education (Independent School Standards) Regulations 2014; the Statutory Framework for the Early Years Foundation Stage for group and school-based providers (September 2026); Keeping Children Safe in Education (KCSIE) 2026; the Prevent Duty Guidance for England and Wales (2023); and statutory DfE guidance on Mobile Phones in Schools (2026). The school also has regard to relevant DfE digital and technology standards, including the filtering and monitoring and cyber security standards.

This AUP is based on best-practice informed by NEN – The Education Network's online safety site[1], The London Grid for Learning (LGfL)[2], the SWGfl (South West Grid for Learning Trust)[3], the UK Safer Internet Centre[4] and information from the ISBA (Independent School's Bursar Association).

This AUP links to the school's Safeguarding Policy, Privacy Policy and Staff Code of Conduct as well as the Tablet Agreement. The school's policy on mobile devices and bringing your own devices to work is set out within this policy. The school's policy on the use of mobile phones and social networking is also set out within this policy.

If you have any concerns about the welfare or safety of a child, including concerns arising from online activity or use of technology, you must report them without delay to the Designated Safeguarding Lead (DSL) or a Deputy DSL, in accordance with the school's Safeguarding Policy.

Please see the Safeguarding Policy for further information about safeguarding and promoting the welfare of children. The school welcomes any questions that staff or parents, carers, or guardians may have about safeguarding and online safety. If you would like to speak to the Designated Safeguarding Lead or the Headteacher about online safety then please contact the School Office on 020 8297 1900.

Policy Statement

[1] http://www.nen.gov.uk/online-safety
[2] https://www.lgfl.net/default.aspx
[3] http://swgfl.org.uk/
[4] https://www.saferinternet.org.uk/

This is a controlled document. The version you are viewing may be out of date. The current master version is held by the School Office Manager and Bursar.

Safeguarding and promoting the welfare of children is everyone's responsibility and all school staff have a responsibility to provide a safe environment in which children can learn (KCSIE, 2026). A safe environment includes the online environment, and online-safety and safeguarding is a responsibility for all members of staff. Safe access to the internet and digital technologies is an essential part of online-safety and safeguarding:

> *"New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.* ***All users should have an entitlement to safe access to the internet and digital technologies at all times****."*
>
> South West Grid for Learning

In accordance with KCSIE 2026, staff must understand that safeguarding extends to the online environment and should remain alert to the range of online risks that may affect pupils, including harmful or inappropriate content, contact, conduct and commerce, as well as misinformation, disinformation and conspiracy theories.

This Acceptable Use of Technology Policy is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- Staff are protected from potential risk in their use of technology in their everyday work.

The school will ensure that staff have good access to digital technology to enhance their work, to enhance learning opportunities for pupils, and will, in return, expect staff to agree to be responsible users.

Acceptable Use of Technology Policy Agreement

Staff must use school systems in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the systems and other users. Staff must recognise the value of the use of digital technology for enhancing learning and ensure that pupils receive opportunities to gain from the use of digital technology. Where possible, staff should educate the young people in their care in the safe use of digital technology and embed online safety in appropriate lessons.

For professional and personal safety, staff must:

- Understand that the school will monitor their use of the school digital technology and communications systems including the use of the internet and any school devices they use;
- Understand that the rules set out in this agreement also apply to use of these technologies (e.g. email, SIMS, network resources, school website, laptops, tablets, school mobile phones, digital cameras etc.) out of school, and to the transfer of personal data (digital or paper based) out of school;

This is a controlled document. The version you are viewing may be out of date. The current master version is held by the School Office Manager and Bursar.

- Understand that the schools digital technology systems are primarily intended for educational use and that they must only use the systems within the policies and rules set down by the school;
- Keep usernames, passwords and other authentication credentials secure and never disclose them to another person. Staff must not use another person's account or permit another person to use theirs. Passwords must be created and managed in accordance with the school's cyber-security requirements, and staff must use multi-factor authentication (MFA) wherever this is required by the school;
- Immediately report any illegal, inappropriate or harmful material or incident they become aware of to the Head Teacher or DSL;
- Understand their role in the school's filtering and monitoring arrangements and report concerns promptly in accordance with the Safeguarding Policy. This includes reporting where harmful or inappropriate content is accessible, where legitimate educational content appears to be unreasonably blocked, or where filtering or monitoring systems appear not to be operating as expected;
- Never attempt to disable, bypass or circumvent the school's filtering, monitoring, security or access-control systems unless specifically authorised to do so for legitimate technical purposes.
- Be mindful of their professional reputation and the school's reputation, specifically when using social media, in accordance with the school's policies (see the Mobile Phone and Social Networking Policy, below).

Staff must ensure they are professional in their communications and actions when using school IT systems. Staff should:

- Not access, copy, remove or otherwise alter any other user's files, without their expressed permission;
- Communicate with others in a professional manner, not use aggressive or inappropriate language and appreciate that others may have different opinions;
- Ensure that when they take images of others they will do so with their permission and in accordance with the school's policy on the use of digital/video images (see the Staff Code of Conduct). Staff will not use personal equipment to record these images and will only ever use a school device (such as the class mobile phone, tablet or school camera).
- Recognise that publication of any images taken of pupils is to be done by the school's Marketing Assistant or Senior Leadership Team unless authorisation has been sought specifically from the Head Teacher. Any images of pupils must only be posted on the school's approved accounts. Where images are published (e.g. on the school website, school social media pages or in the school newsletter) all content will be checked against the Data Consent Spreadsheet to ensure that what is posted is in line with the permissions that the school holds;
- Not use social networking/ media sites in school for personal reasons. Where it is appropriate for social media to be used for school purposes, (for example if the staff member is the Marketing Assistant), staff must do so with their professional reputation and the school's reputation in mind, in accordance with the school's policies (see the Mobile Phone and Social Networking Policy, below);
- Only communicate with pupils and parents/carers using official school systems and procedures. Any such communication will be professional in tone and manner. Staff must not engage in any online activity that may compromise their professional responsibilities.

This is a controlled document. The version you are viewing may be out of date. The current master version is held by the School Office Manager and Bursar.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school. To support this, staff:

- Will not use personal devices at school (this includes but is not limited to personal mobile phones, laptops and tablets) during time that they are scheduled to be with children;
- Will not use personal accounts, such as email addresses, on the school IT systems (this includes desktop computers, laptops, tablets and school mobile phones). This includes during hours of work, during any breaks, and outside of working hours;
- Will only open hyperlinks in emails or attachments to emails if the source is known and trusted. Staff will not open any hyperlinks in emails or any attachments to emails if they have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes);
- Will report any suspected cyber-security incident without delay in accordance with the school's procedures. This includes suspected phishing, malware, compromised or disclosed passwords, unusual or unauthorised account activity, loss of a device containing school information, or any suspected unauthorised access to, disclosure of or loss of school data;
- Will ensure that their data is regularly backed up to the school's Google Drive;
- Will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminal racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. Staff will not try to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials;
- Will not make large downloads or uploads that might significantly affect network capacity without appropriate authorisation;
- Will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor try to alter computer settings, without the express permission of a member of the Senior Leadership Team;
- Will not disable or cause any damage to school equipment, or the equipment belonging to others;
- Will only transport, hold, disclose or share personal information about themselves or others, as outlined in the Access and Storage of Information Policy and Privacy Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted and staff must have the permission of the Head Teacher to make such transfer. Paper based Protected and Restricted data must be held in lockable storage;
- Will not use any portable storage devices such as USBs, external hard drives or SD cards;
- Must understand that the Privacy Policy requires that any staff or student/pupil data to which they have access, will be kept private and confidential, except when it is deemed necessary that they are required by law or by school policy to disclose such information to an appropriate authority;
- Will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in their professional capacity or for school sanctioned personal use, staff:

- Will show due care and attention to their choice of website, ensuring that the sources they use are credible;

This is a controlled document. The version you are viewing may be out of date. The current master version is held by the School Office Manager and Bursar.

- Will perform their due diligence on any website or program before permitting or directing children to use it;
- Will not attempt to access any social networking/ media sites for personal or professional reasons (unless their position within the school explicitly dictates that they may do so i.e. Marketing Assistant or SLT for school purposes only), websites that they have been directed not to access, their personal account for any website (including emails) and any other websites that are deemed inappropriate or unsuitable;
- Will ensure that they have permission to use the original work of others if using in their work;
- Will immediately alert the SLT to any content which they feel should be blocked or seems inappropriate;
- Where work is protected by copyright, staff will not download or distribute copies (including music and videos).

When using the Interactive Display Boards staff:

- **Will ensure that they have thoroughly checked <u>all</u> content prior to displaying it on the interactive board;**
- Will prepare all resources to display and only activate the screen when they are displayed to ensure that only the correct content is shown;
- Will close any web pages down as soon as they are finished using them;
- When showing videos/clips, will ensure that the board is off whilst they prepare the content for display and turn the board off immediately after showing it and close the web page down;
- Any videos/clips shown to pupils will be shown in full screen mode so that no comments or other suggested videos can be seen;
- Will highlight any issues with the Interactive Display Board to a member of the Senior Leadership Team as soon as it occurs;
- Will ensure that they turn off the Interactive Display Board when it is not in use.

AI (Artificial Intelligence)

When using AI, the HH team will:

- comply with the age restrictions and terms of use of AI tools. Pupils must not use open-access commercial generative AI tools unless the school has specifically approved their use. Any pupil use of AI must take place through school-approved platforms, following appropriate data-protection and safeguarding checks and under staff supervision appropriate to the pupil's age and the activity;
- use AI in a way that is consistent with the school's safeguarding, online-safety, data-protection, cyber-security and filtering and monitoring arrangements;
- ensure that any generative AI product or platform proposed for use with pupils is appropriately assessed before use, having regard to relevant Department for Education generative AI product safety standards and the school's safeguarding, filtering and monitoring, cyber-security and data-protection requirements;

This is a controlled document. The version you are viewing may be out of date. The current master version is held by the School Office Manager and Bursar.

- critically review AI-generated content for accuracy, bias, appropriateness and suitability before using it for school purposes or sharing it with pupils;
- remain professionally responsible for any work produced with the assistance of AI. AI-generated material must not be treated as automatically accurate, appropriate or authoritative;
- Ensure they are mindful of any potential misuse of AI in children's homework
- only use AI tools and platforms that have been approved by the school and only through authorised school accounts. Staff must not enter confidential, special-category or safeguarding information about pupils, families or staff into generative AI tools unless the school has expressly approved that specific use and appropriate data-protection safeguards are in place. Simply removing a person's name or replacing it with a label such as "Child 1" does not necessarily anonymise information where the individual could still be identified from the remaining details. Staff must therefore minimise and, wherever possible, fully anonymise any personal information before using an approved AI tool.

iPads

Heath House has a growing suite of iPads for use by children within their lessons. The iPads will only be used under the strict supervision of Heath House Staff for appropriate and sanctioned activities. Children, regardless of their age or the activity they are engaged in, should not be left alone using the iPad. The time iPads are used for will be mandated by teachers and the reasons for use will be within teachers planning. iPads are, under no circumstances, to be taken home by any pupil or teacher.

Use of the iPads is with the focus on broadening the computing curriculum at Heath House and allowing use of integrated technology throughout the wider curriculum areas. The Senior Leadership Team, in collaboration with Class Teachers, determines which applications are available for children to use so that robust checks can be conducted prior to use to determine suitability.

Teachers are not to use the iPads for their work (each teacher has access to a desktop PC or 'communal' laptops for printing) nor are they to be used for personal means.

iPads are currently stored in the Old Library building. All devices are locatable via the 'Find My' app from the School Manager's school phone. Staff are unable to download new apps without seeking permission from the School Manager and/or Head Teacher and passwords/ controls ensure this as a further method of safeguarding.

All iPads are connected to the school Wi-Fi which has stringent filters as outlined in the Safeguarding Policy.

iPads all have screen protectors and robust cases to protect them and prevent as much damage as possible. Any damage, however it is caused, must be reported to the Head Teacher or School Manager at

This is a controlled document. The version you are viewing may be out of date. The current master version is held by the School Office Manager and Bursar.

the earliest opportunity. In the same way, any misuse of the iPad must also be reported to the Head Teacher as soon as possible.

Mobile Devices

A 'mobile device' is any transportable device capable of storing data. This covers a wide range of equipment, including (but not limited to) mobile phones/ smartphones, USB sticks, external hard drives, memory cards, memo devices, laptops, tablets, digital cameras, camcorders, audio recorders, CD/DVDs, music players, and other external hard drives and devices.

Heath House is a mobile phone-free environment for pupils. The use of mobile phones by pupils is prohibited during the school day, including during lessons, the time between lessons, breaktimes, and lunchtimes. Any smart technology with similar functionality (e.g. smartwatches that can send/receive notifications) is also prohibited.

Individual exceptions may be made where necessary to meet a pupil's medical needs, disability or other exceptional circumstances. Any such arrangement must be agreed by the Head Teacher or Senior Leadership Team and appropriately recorded.

Staff must not use personal mobile phones while supervising pupils or in the presence or sight of pupils. Personal use is permitted only during designated breaks, away from pupils, in accordance with the Mobile Phones and Social Networking section of this policy.

All class teachers are equipped with a school mobile phone which is to be used to:

- Capture images of the children for publication (such as in the school's newsletter or for the schools social media pages). Publication of such images is controlled by the Head Teacher, Senior Leadership Team and Marketing Assistant;
- Send captured images to the Head Teacher, Senior Leadership Team or Marketing Assistant's email addresses or via Google Chat for their use. This should be done using the staff member's school email address or @globalschools.com Google account (which is pre-loaded onto the school phone);
- Make emergency calls back to the school office or to the Senior Leadership Team whilst out of the school building (for example if an incident occurs whilst on the Heath or at the Waterfront Leisure Centre);
- Authenticate their access to CPOMS (this must not be done whilst with children);
- Check their emails where an appropriate time is identified for this (for example whilst off site, staff may wish to rotate and decide that each member of the team may spend 10 minutes looking at emails etc. whilst the children are on the coach).
- Monitor the staff Google calendar to help ensure that they are informed and organised for all school events;
- Monitor the 'Heath House Staff' Google Classroom to help ensure that they are aware of any information being shared between members of the team that is relevant to them or their class;

Please note: it is not appropriate for staff to use their mobile phones for checking emails/ Google Apps, whilst the children are actively taking part in a session (such as swimming, climbing or cycling lessons).

This is a controlled document. The version you are viewing may be out of date. The current master version is held by the School Office Manager and Bursar.

School mobile phones are all set up by the School Manager. Before the device is issued to staff members:

- The serial number is taken and registered on the asset record. At this time the device will be assigned to an individual;
- The device is configured with appropriate security controls, including a secure passcode or other authentication method;
- The user's accounts are loaded (such as their school email and Google accounts);
- Relevant prohibitive permissions are set (such as preventing some application downloads).

When using school mobile phones, staff must:

- Keep the device passcode secure and must not share it with pupils or unauthorised persons. Staff must not change or remove security settings, passcodes or authentication arrangements without authorisation from the Senior Leadership Team;
- Ensure that they leave the device at school at the end of the working day unless pre-authorisation has been given. SMT members and school's Marketing Assistant may take their school mobile phone home with them as this is appropriate and relevant for their role;
- Not use any unauthorised apps unless specific permission has been given by the Head Teacher or Senior Leadership Team. Depending on a staff member's role, the apps which they are authorised to use may vary.
    - As a general rule, school phones used by class teachers should not be used to access social media apps, WhatsApp or any game applications.
    - School phones used by the Head Teacher, Senior Leadership Team and the school's Marketing Assistant may access the school's social media accounts and WhatsApp but should not access any game applications.
- Never use the device for personal use or attempt to log in to any of their personal accounts using the device;
- Not use their device whilst in the changing area or poolside for swimming lessons;
- Ensure they update the software on the device as needed (seeking help from the School Manager as needed);
- Return the school mobile phone they have been issued to the School Manager at the end of every half term (for maintenance checks etc.);
- Not use their school assigned mobile phone to circumnavigate the strict internet filters in place on the main broadband at Heath House;
- Report any damage (however it may have been caused) to the Head Teacher and Senior Leadership Team immediately so that repairs can be arranged;
- Inform the Head Teacher or Senior Leadership Team of any misuse (or suspected misuse) as soon as possible;
- Ensure that they use the original charger for the device;
- Not allow children to access the device at any time;
- Not attempt to modify the phone in any way. This includes applying any permanent marks or decorations;
- Not swap device with another member of staff;
- Not dispose of or sell the device;
- Clean the screen regularly using appropriate means;
- Make sure their hands are clean before using the device;

This is a controlled document. The version you are viewing may be out of date. The current master version is held by the School Office Manager and Bursar.

- Keep the device away from food and drink.

School mobile phones remain the property of Heath House at all times.

Bringing Your Own Device (BYOD) Policy
It is the school's policy that as a general rule, **staff may not use their own mobile devices**, including laptops, tablets, mobile phones, digital cameras or other recording equipment.

All classrooms are equipped with suitable PCs, Tablets, Mobile Phones (for use as outlined above) and Interactive Boards and it is therefore the view of the Senior Leadership Team that personal devices are not essential for any member of staff to carry out their role whilst at school. If a staff member feels that they would benefit from an additional device or an alteration to the technology provided in their classroom they should discuss this with the Senior Leadership Team.

USB sticks and External Storage Devices
USB sticks and external storage devices such as external hard drives are **not permitted** at Heath House. All data which needs to be transported must be stored on each staff members individual Synology account or within the 'Shared Area' of Synology. This is to ensure that the school complies with the Data Protection Act and the General Data Protection Regulation, and that personal and sensitive information is protected from unauthorised access, dissemination, alteration or deletion, this also prevents any accidental loss of information i.e loss of the USB stick. Please see the Access and Storage of Information Policy for further information. Any USBs or external storage devices found to be in use on a school device (laptop/ PC) will be removed.

Mobile Telephones
Staff may bring personal mobile phones to work; however, to model a phone-free environment, **staff must not use their own mobile phones for personal reasons in the presence or sight of pupils** at any time during the school day. This includes during lessons, breaktimes, and lunchtimes. Staff are not permitted to access the school Wi-Fi or ICT systems using their mobile phones and should not attempt to use the school Wi-Fi to access social media or personal email accounts.

Mobile Phones and Social Networking Policy
We believe our staff should be completely attentive during their hours of work to ensure all children at Heath House receive good quality care and education. This is why personal use of mobile phones is not permitted during teaching/ pupil facing time. We feel that restrictions need to be placed on staff when they access social networking sites. The school has a high reputation to upkeep and comments made on sites such as 'Facebook' could have an impact on how parents of pupils and parents of prospective pupils view the staff and the school. Staff are therefore not to access social media sites during teaching/ pupil facing time.
Staff must:

- **Not** use their mobile phones for personal reasons during teaching/ pupil facing time;
- **Only** use their school mobile phone in front of children for legitimate and necessary reasons (such as making a call back to the school office or sending a quick message/ email with a photo of an activity to the school office/ Marketing Assistant);

This is a controlled document. The version you are viewing may be out of date. The current master version is held by the School Office Manager and Bursar.

- **Only** use their mobile phones for personal reasons during a designated break, and not in sight of children**;**
- **Not** take images of children using their personal mobile phones under any circumstance;
- **Not** post or publish anything onto social networking sites or platforms such as 'Facebook' that could be construed to have an impact on the school's reputation, or the professional or personal reputation of any member of staff (please also see the Social Media Policy);
- **Not** post/publish anything onto social networking sites/platforms that would offend any other member of staff, volunteer, pupil or parent/carer of a pupil/prospective pupil at the school;
- **Maintain** appropriate professional boundaries with parents on personal social-media accounts. Staff must not use personal social-media accounts to communicate about school matters or establish online relationships with parents/carers where this could compromise professional boundaries. Any pre-existing personal relationship should be managed transparently and in accordance with the Staff Code of Conduct;
- **Not** communicate with current pupils through personal social-media accounts, accept or initiate social-media connections with them, or otherwise engage with them through personal online accounts. Staff must also maintain appropriate professional boundaries in relation to former pupils, recognising that safeguarding concerns and power imbalances may continue beyond a pupil leaving the school;
- **Be aware** that if any of the above points are not followed then the member of staff involved will face disciplinary action, which could result in dismissal.

The Staff Code of Conduct contains the following passage on the use of communication technology, including mobile phones and social networking sites:

Communication with Pupils Including the Use of Technology
Heath House staff are expected to conform to this Code and limit their communications with pupils and parents of pupils to professional matters. All communications should be made using school property, for example, written notes in the child's journal, or telephone calls made via the school office or telephones in the Old Library and Tranquil Hall or school mobile phones (when off site).

Staff must comply with the school's policy on use of mobile phones (both school issued phones and personal devices) and technology as set out in the Acceptable Use of Technology Policy Agreement. Staff must not communicate with pupils or parents/carers about school matters through personal telephone numbers, personal email accounts, personal social-media or messaging accounts, online gaming platforms or other personal digital accounts. Video calls or other online communications for school purposes must take place only through school-approved systems and in accordance with school procedures.

Please see the Staff Code of Conduct Policy for further information.

Working from Home
Where staff are required or authorised to work remotely, including where remote education is provided to pupils, all relevant school safeguarding, online-safety, data-protection and professional-conduct requirements continue to apply. Staff must use school-approved systems and accounts for school business and must ensure that any online learning activities, resources and communications are

This is a controlled document. The version you are viewing may be out of date. The current master version is held by the School Office Manager and Bursar.

appropriate and secure. Where pupils access remote education from home, the school will provide appropriate guidance to parents/carers about safe access and supervision, taking account of the pupil's age and circumstances. Please see the Working from Home Guidelines for further information. In line with the Privacy Policy, personal data relating to children must never be downloaded, extracted, or stored locally on personal devices at home. Secure, authenticated cloud-based access to official school systems (such as SIMS, Microsoft Teams, and Google Workspace) is permitted for business continuity, provided it is accessed through a secure internet connection and not left visible to others.

Staff must understand that they are responsible for their actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school;
- I understand that failure to comply with this Acceptable Use Policy Agreement may result in disciplinary action in accordance with the school's procedures. Where appropriate, concerns may also be referred to relevant safeguarding, regulatory or law-enforcement bodies in accordance with statutory requirements and school policy.

User signature

- I have read and understood the above points and agree to use the school digital technology and communication systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines;
- I understand that I have a responsibility for my own and others' e-safeguarding in line with the Safeguarding Policy and I undertake to be a safe and responsible digital technologies user;
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety and safeguarding policies;
- I understand that I am responsible for the security and reasonable care of portable devices assigned to me, such as a laptop or mobile phone. I will report any loss, theft or damage promptly and comply with the school's procedures for the safe use, storage and return of school equipment.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Staff Name: _____

Signed: _____

Date: _____

Authorised signature (SLT)

I approve this user to be set up on/ continue using the school systems relevant to their role and with any relevant portable devices.

Name: _____

Signed: _____

Date: _____

This is a controlled document. The version you are viewing may be out of date. The current master version is held by the School Office Manager and Bursar.

Internal use only

Last reviewed	September 2026
Date for review	September 2027

This is a controlled document. The version you are viewing may be out of date. The current master version is held by the School Office Manager and Bursar.