



HOLMEWOOD HOUSE SCHOOL

'Kindness, aspiration & self-belief'

ACCEPTABLE USE OF TECHNOLOGY POLICY (AUP)

Policy Holder	The Bursar
Date Approved	March 2026
Governor Approval	Full Board
Date for next review	March 2027

This policy should be read in conjunction with:

- Online Safety Policy
- Cyber-security
- Use of smart technology including mobile phones
- Safeguarding Policy
- Data Protection
- Retention of Records

SCOPE OF THIS POLICY

This policy applies to all members of the school community (staff) who use any form of technology systems and services provided or accessed as part of their role within Holmewood House both professionally and personally. All staff users of the network are expected to adhere to the guidelines set out in this policy. The policy refers to the use of email as well as IT networks, data and data storage, remote learning and online and offline communication technologies.

The use of technology should be consistent with the school ethos, school policies and the law. Access to school systems is not intended to confer any status of employment on any contractors.

Staff are reminded that the school has robust filtering and monitoring procedures for all Holmewood House IT systems, and that the school can view content accessed or sent via its systems.

ONLINE BEHAVIOUR

All staff should follow these principles in respect of all online activities:

- All online communications, and any shared content should be respectful and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

ONLINE COMMUNICATION & SOCIAL NETWORKING SITES

All staff are expected to ensure that their online reputation and use of technology and is compatible with working for Holmewood House. This includes the use of email, text, social media, social networking sites, X formally Twitter or similar services, gaming and any other personal devices or websites.

In order to do this:

- Staff must take appropriate steps to protect themselves online.
- Staff must not discuss or share data or information relating to learners, staff, Holmewood House business or parents on social media.
- Staff must ensure that their use of technology and the internet will not undermine their role or interfere with their duties and will be in accordance with the School code of conduct and the law.
- Staff must not use such services to impersonate others, send indecent, obscene, offensive, threatening or inappropriate language or images, nor to participate in any form of “cyber-bullying”. Nothing must be posted on such services which identifies the School with unacceptable opinions or activities, or which would bring the School into disrepute.
- All communication must take place via Holmewood House approved communication channels such as via a school provided email address, account or telephone number.
- All remote learning and any other online communication must take place in line with current Holmewood House confidentiality expectations as outlined in Staff Code of Conduct.
- Staff and pupils should keep their personal, family and social lives separate from their school IT use. Personal use of school accounts for school business is not permitted.
- Electronic communications with pupils, parents and other professionals must take place within clear and explicit professional boundaries, be transparent, respectful and may be open to scrutiny.

- Staff, including those who are also parents of pupils at Holmewood House, must act professionally and not say or do anything through social media which might damage the School's reputation.
- Staff are reminded that low-level concerns may relate to behaviour both on and offsite and on and offline.

INTERNET ACCESS, FILTERING AND MONITORING

The School network is actively filtered and monitored as an important part of providing a safe environment for pupils to learn. Our procedures for filtering and monitoring are informed by the Government guidance on meeting digital and technological standards. All monitoring will be proportionate, in accordance with data protection, privacy, and human rights legislation

Staff must not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act. Neither should they attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

Copyright must be respected. Staff should not plagiarise work found on the internet and claim as their own. The internet must not be used to download illegal software or pirated music, images or software.

USING THE SCHOOL'S IT SYSTEMS

All IT property belonging to the School should be treated with respect and care and used only in accordance with any training and policies provided.

Use of the school's IT systems (including by connecting your own device to the network) is contingent on complying with the following:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.
- Staff are asked to respect the limits of storage on school networks particularly when streaming or downloading of large files.
- Staff must report any faults or breakages without delay to the IT department.

USE OF PERSONAL DEVICES OR ACCOUNTS

All official school business of staff must be conducted on school systems; it is not permissible to use personal email accounts for school business.

The use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the Deputy Head.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies, including the BYOD policy and use of two-factor authentication and encryption.

TRACKING DEVICES AND TECHNOLOGY

The school is not responsible for individual settings on personal devices, nor for the use of tracking apps / devices for purely personal and domestic purposes.

Use of this technology in the context of school activities is not specifically encouraged but if parents do plan to use it then they should be aware of potential third party privacy considerations and only use it for domestic / personal purposes in respect of their own child and/or their or their child's belongings.

IMAGES AND VIDEOS

Images or videos of learners must be taken on school devices in line with the Holmewood House image use policy.

It is not permitted to use personal mobile devices to take, store or upload images or videos of children.

All staff must follow the guidance in the Use Of Personal Smart Technology Policy.

SYSTEM SECURITY & PASSWORDS

Each member of staff is responsible for their own account. Staff use of the School's IT systems (including by connecting your own device to the School network) must follow these principles:

- Holmewood House network systems should be accessed via an individual username and password (minimum of 8 characters), which must not be shared with anyone else.
- Staff should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.
- Staff must sign out or lock computers when leaving them unattended.
- Passwords will be updated regularly, prompted by the security system.
- Two step authentication is required for remote access.
- Staff must not attempt to circumvent the content filters or other security measures installed on the school's IT systems or attempt to access parts of the system that they do not have permission to access.
- Unless authorised to do so, staff should not attempt to install software on, or otherwise alter, school IT systems.
- Staff must not attempt to gain unauthorised access to anyone else's computer or to confidential information to which they do not have access rights.

- The School reserves the right to conduct searches of staff accounts and devices if they were used for school business in contravention of this policy.

DATA PROTECTION

The School has appointed www.dpofoeducation.co.uk to work with the Compliance Officer as Data Protection Lead (DPO) compliance@holmewoodhouse.co.uk to ensure that all personal data is processed in compliance with this Policy and the principles of the GDPR.

Staff must ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR. See the Data Protection Policy.

Devices which may contain information about pupils are password protected.

Username or passwords should not be 'saved' or 'remembered' on public computers. This includes not sharing School passwords with family members or others.

Staff must not take sensitive information off site without prior permission from the Head, Bursar or DSL, including exam results, medical, child protection, or criminal record information.

Any such information taken off site e.g. for school trips, must be printed, stored securely during the period of time it is needed, and then securely destroyed. Trip leaders have permission to take copies of medical information on School trips. Staff must not make or distribute lists of pupils or parents including personal details without legitimate reasons to do so.

Staff are required to use the Holmewood House Office 365 Cloud provision/SharePoint and **not their personal Cloud storage** as this will be regarded as taking information off site.

When e-mailing a group of parents, staff **must use BCC** to avoid sharing email addresses to all of the recipients.

RETENTION OF DIGITAL DATA

The following principles apply to ensure effective data storage and that no important information should ever be lost as a result of the school's email deletion protocol:

- All emails sent or received on school systems will be archived whether or not deleted and email accounts will be suspended and contents archived once that person has left the school.
- Any information from email folders that is necessary for the school to keep for longer, including personal information (e.g. for a reason set out in the school privacy notice), should be held in the relevant personnel or pupil file.
- Important records should **not be kept in personal email folders**, OneDrives, archives or inboxes, nor in local files.
- it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague.

If you consider that reasons exist for the protocol not to apply or need assistance in how to retain and appropriately archive data, please contact The Compliance Officer or Bursar.

BREACH REPORTING

The law requires schools to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands.

This could include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

If staff or pupils become aware of a suspected data breach, you must notify the Data Protection Officer compliance@holmewoodhouse.co.uk as soon as you become aware of the issue and certainly within 24hrs. Where the breach meets the reporting criteria issued by the IOC, the school must report this to the IOC without undue delay (i.e. generally within 72 hours), and certainly if it presents a risk to individuals. The school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

BREACHES OF THIS POLICY

A deliberate breach of this policy or attempt to access or use personal information without a legitimate reason, to 'hack' into the School's ICT infrastructure, or to deliberately evade or circumvent the School's firewall, for example by the use of a Virtual Private Network (VPN), is likely to be dealt with as a disciplinary matter using the school's usual applicable procedures and may, in addition, may result in the school restricting that person's access to school IT systems.

If you become aware of a breach of this policy or the Online Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the Bursar and the Designated Safeguarding Lead.

POLICY COMPLIANCE

All staff are expected to comply with this policy. Should staff have any queries or questions regarding safe and professional practice online either in Holmewood House or off site, they are expected to raise them with the Designated Safeguarding Lead or the Bursar.

If the School believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures. Additionally, should the School suspect criminal offences have occurred, the police will be informed.

ANNEX A

ONLINE AND REMOTE TEACHING AND LEARNING

When engaging in online teaching, staff must adhere to the following principles to ensure safe and effective pupil engagement:

- Online teaching must take place using school approved platforms, e.g. Zoom or Teams. Appropriate privacy and safety settings must be in place to manage access and interactions.
- Staff must use Holmewood House accounts when engaging in online teaching, contacting pupils via Teams or email. **Use of personal accounts to communicate with parents or pupils is not permitted.**
- Access links should not be made public or shared by participants.
- All online lessons should be formally timetabled, attendance should be registered at the start of each session; Heads of Department or member of SLT may drop in at any time.
- Personal data used by staff and captured by Teams or Zoom must be processed and stored in accordance with our Data Protection policy.
- Behaviour and conduct during online teaching and learning must remain in line with existing Holmewood House policies and expectations. Staff must ensure pupils follow the code of conduct for pupils engaged in online learning.
- Staff should remain professional at all times during online teaching. When recording videos or livestreaming lessons remotely (i.e. when not at school), staff should still dress appropriately and film in a neutral area. Pupils should be encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent or another appropriate adult.
- A live class taught remotely should be recorded and backed up on individual staff's Office 365 'One Drive' folders, so that if any issues were to arise the video can be reviewed.
- Safeguarding guidance must be followed when working 1-1 with pupils.
- Staff should discuss the benefits and risks of the online world regularly with their classes. Pupils must be given advice about what to do if they are worried about anything online or need to talk to someone while they are remote learning. Childline can be contacted for free on 0800 1111, <https://www.childline.org.uk/get-support/>
- Concerns regarding online or remote learning should be raised, in the first instance, with the relevant Head of Section and the Assistant Head of Learning & Teaching.
- **Safeguarding concerns must be referred to the DSL without delay and staff should follow the guidance in the school Safeguarding Policy.**

Acceptance of this policy:

Acceptable Use of Technology (AUP staff)

Please confirm that you understand and accept this policy by signing below and returning the signed copy to the HR Manager.

I understand and accept this acceptable use policy:

Name:

Signature:

Date: