# HOLMEWOOD HOUSE SCHOOL

*'Kindness, aspiration & self-belief'*

# ACCEPTABLE USE OF TECHNOLOGY POLICY (AUP)

| | |
|---|---|
| **Policy Holder** | The Bursar |
| **Date Approved** | January 2024 |
| **Governor Approval** | Full Board |
| **Date for next review** | September 2024 |

**This policy should be read in conjunction with:**

- Online Safety Policy
- BYOD – pupils use of devices in school
- Cyber-bullying
- The use of smart technology including mobile phones
- Safeguarding Policy

## 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 (whether using School computers, laptops, mobile phones, tablets, digital cameras or any other device that can connect to the School network by whatever means) 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.

All staff should ensure that technology use is consistent with the school ethos, school staff code of conduct and safeguarding policies, national and local education and child protection guidance, 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 communication & social networking sites

All staff are expected to ensure that their online reputation and use of technology and is compatible with their role within Holmewood House. This includes the use of email, text, social media, social networking sites such as Whatsapp, Imessage, Snapchat, Facetime, Instagram and 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 will 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 will 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 and limit as far as possible any personal use of these accounts.
- Any electronic communications with pupils, parents and other professionals will only take place within clear and explicit professional boundaries and will be transparent, respectful and open to scrutiny.
- Where members of staff are also parents of pupils at Holmewood House and are friends with other Holmewood House parents, those staff are reminded of the Staff Code of Conduct and the need to act professionally and not say or do anything through social media which might conflict the School's reputation or goals.
- 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. Holmewood House exercises its right to block internet access to harmful sites and inappropriate content; monitor the use of school information systems, including use of internet and the interception of emails; to monitor policy compliance and to ensure the safety of learners, staff and visitors or volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation. Our procedures for filtering and monitoring are informed by the Government guidance on meeting digital and technological standards in schools 2023.

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 s their own. The internet must not be used to download illegal software or pirated music, images or software.

Staff are asked to respect the limits of storage on school networks. Excessive use of streaming and the downloading of large files should be avoided as this can restrict others' use of computer systems.

### Devices and use of property

Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. Staff must report any faults or breakages without delay to the IT department.

The rules that apply to School computers also apply to personal devices used to access the School systems remotely and are subject to the same rules and safeguards in line with the school policies.

### Images and videos

Any images or videos of learners will only be taken 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.

### 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 e.g. not in bedrooms, where nothing personal or inappropriate can be seen or heard in the background. 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. If it is appropriate to communicate with a child on an individual basis, for example, to give feedback on a piece of work – use the child's personal channel in Teams or email the parents directly. Should further direct 1-1 support be necessary, this must be discussed with Head of Learning Strategies and/or HoD before a face to face session can be undertaken. Additional parental agreement must also be sought.
- 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.**

## System security

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 are responsible for remembering to sign out or lock computers when leaving them unattended even if for only a few minutes.
- 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.
- Please be aware that the school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

**Data protection**

The School has appointed the Head of Compliance as Data Protection Officer (DPO) compliance@holmewoodhouse.co.uk who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the GDPR. See also the Data Protection Policy

All staff play an important role in data protection. Staff must ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.

Staff must ensure that devices which may contain information about pupils are password protected. Usernames 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. This could include: 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 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 on the relevant personnel file.
- Important records should **not be kept in personal email folders**, OneDrives, archives or inboxes, nor in local files.

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 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.

Any 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 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 Head.

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.

September 2023