ICT Acceptable Use Policy – Staff
Academic Year 2023-2024

This document sets out the security, administration and internal rules which staff should observe when communicating electronically or using the IT facilities provided by Harrow School (the '**School**'). Staff should familiarise themselves with the terms of this Policy in order to minimise potential difficulties for themselves, colleagues, pupils and the School, which may arise as a result of misuse of email or internet facilities.

This Policy applies to all employees and contractors of the School, as well as resident family members of resident employees who use School ICT facilities.

1. School Systems

1.1 The School acknowledges and welcomes the creativity of staff in the production and storage of material to support teaching, learning and administration. It is important to note that, according to the letter of the law, computer files and electronic messages created and stored on school systems by employees, contractors and residents in the performance of their normal duties technically remain the property of the School. In any question regarding copyright and intellectual property, staff are encouraged to seek advice from the IT Services Department.

2. Monitoring

2.1 The School's computer network is a business and educational tool to be used primarily for School business or educational purposes. Staff therefore have a responsibility to use these resources in an appropriate, professional and lawful manner.

2.2 All messages and files on the School's system will be treated as education or business related which may be monitored. Accordingly, staff should not expect any information or document transmitted or stored on the School's computer network to be entirely private.

2.3 You should also be aware that the School maintains systems that automatically monitor and filter use of the internet, both during school or working hours and outside of those hours. This includes the sites and content visited and the length of time spent using the internet.

2.4 Staff should structure electronic messages in recognition of the fact that the School may, if concerned about possible misuse, have the need to examine its contents.

2.5 Data that the School holds will be archived by the School as it considers appropriate and to comply with statutory requirements.

2.6 The School will routinely send out phishing test emails to staff as part of our cyber security process. Staff that routinely click on phishing emails, both genuine or test, may be subject to disciplinary action depending upon the circumstances.

3. Personal Use

3.1 Any use of the School network, internet or electronic communication for personal purposes is subject to the same terms & conditions as otherwise described in this Policy.

3.2 In the case of shared IT facilities, staff are expected to respect the needs of colleagues and use the computer resources in a timely and efficient manner.

3.3 Inappropriate use of electronic messages or internet facilities for personal reasons during working hours may lead to disciplinary action.

3.4 Staff are discouraged from using work email for personal use and likewise should not use personal email for work communications. Use of the internet during working hours for personal reasons should be kept to a minimum so that it does not interfere with the performance of work duties.

3.5 The internet is a shared resource. Staff should not download or stream excessive volumes of files or images for personal use, nor should staff download or install software or applications without the consent of the Director of IT. The School reserves the right to limit use of the internet for staff who misuse it.

3.6 At all times, Harrow School staff should conduct electronic communications with the utmost propriety and avoid any internet behaviour that may bring themselves or the school into disrepute. Depending upon the severity of the incident this may lead to disciplinary action.

3.7 Staff should familiarise themselves with the Staff Code of Conduct with specific regard to Safeguarding, noting particularly that neither social networking nor gaming sites should be used for communication with current pupils.

4. Content

4.1 Electronic correspondence should be treated in the same way as any other correspondence such as a letter, in that it is a permanent written record which may be read by persons other than the addressee and which could result in personal or the School's liability.

4.2 Staff and/or the School may be liable for what is communicated in an electronic message. Electronic messages are neither private nor secret. It may be easily copied, forwarded, saved, intercepted, archived or requested under a Data Subject Access Request (DSAR) and may be presented in litigation.

4.3 The School network, internet or electronic messaging should never be used for the following purposes:

- to abuse, vilify, defame, harass or discriminate on any grounds. Staff should familiarise themselves with School's Equality and Diversity Statement and the Equal Opportunities and Dignity at Work Policy;
- to send or receive obscene or pornographic material;
- to injure the reputation of the School or any of its employees or to cause embarrassment to the School;
- to spam or mass mail or to send or receive chain mail;
- to infringe the copyright or other intellectual property rights of another person;
- to perform any other unlawful or inappropriate act;
- to upload or publish images of School pupils or staff outside of the School without permission; or
- to infringe the privacy of another person

4.4 Electronic message content that may seem harmless to the sender may in fact be highly offensive to someone else. Staff should be aware that in determining whether an electronic message falls

within any of the categories listed above, or is generally inappropriate, the School will consider the reaction and sensitivities of the recipient of an email.

4.5 If staff receive any inappropriate material which is not relating to Safeguarding it should be deleted immediately. If staff receive inappropriate material which may be related to Safeguarding they should stop immediately, not touch the device and contact the School's Designated Safeguarding Lead. The material should not be forwarded to anyone else. Staff should then not take any further action until advised to do so by the appropriate member of Senior Staff.

4.6 Comments that are not appropriate in the workplace or School environment will also be inappropriate when sent by any electronic communication. Electronic messages can easily be misconstrued. Accordingly, words and attached documents should be carefully chosen and expressed in a clear, professional manner.

4.7 Use of the School's computer network in a manner inconsistent with this policy or in any other inappropriate manner, including but not limited to use for the purposes referred to in this Policy, may give rise to disciplinary action. This could include termination of an employee's employment or contractor's engagement.

4.8 Managing School Data is the responsibility of both staff and the IT Services department, especially with mobile devices which are being used by staff away from the School. Be vigilant about the physical security of mobile devices containing School data. Staff must take responsibility for ensuring that, where they are in use, their OneDrive and OneNote files are being backed up. If OneDrive or OneNote files on the device are not syncing correctly (identified by either a missing OneDrive icon, or a red X) then staff must inform IT as soon as possible to prevent potential data loss. Staff should contact IT Services if they have any queries about this. Here is a link to more information.

4.9 When leaving the School's employment, it is the staff member's responsibility to ensure they have a new, personal, non-School email account. It is their responsibility to copy or forward any relevant personal data to their new personal account, ensuring that anything transferred does not contain School data and complies with The Data Protection Act 2018 and UK General Data Protection Regulation (UK-GDPR). Upon the ending of a contract of employment, the staff login is closed, and any school-issued mobile devices are erased.

5. Data Protection and Privacy

5.1 In the course of carrying out duties on behalf of the School, staff may have access to, or handle personal information relating to others, including pupils, colleagues, contractors, residents, parents, governors and suppliers. Electronic messages should not be used to communicate personal information about anyone except in accordance with the School's Data Protection Policy and Privacy Policy or with proper authorisation.

5.2 The Data Protection Act 2018 and UK General Data Protection Regulation (UK-GDPR) requires both the staff member and the School to take reasonable steps to protect any personal information, that they hold as a consequence of their employment, from misuse and unauthorised access. Please note that Data Protection breaches may be treated as gross misconduct by the School, which could result in summary dismissal for employees and significant fines for employers. We stress therefore:

- Staff must take responsibility for the security of their School-issued device and any personal computers and removable storage devices (including mobile phones) that they may use as a consequence of their employment;
- Unless absolutely necessary, staff must not use their own home computer, laptop or any portable electronic device to store school confidential data (such as pupil/parent addresses, email addresses, telephone numbers, medical histories, staff information or the like);
- If staff are working with School data outside of the school (either by email or internet storage,

or by using removable storage media such as memory sticks, removable hard drives etc.) they must take all reasonable precautions to encrypt the data during use and to securely delete or destroy the data once it is no longer required;

- If staff need any assistance or advice regarding appropriate security measures they should contact the IT Services department.

5.3 Staff will be assigned a username and a password to use the School's electronic communications facilities. Staff should ensure that their login details are not disclosed to anyone else and that steps are taken to keep these details secure. For example, staff should change their password regularly and if it must be written down it should be stored in a secure password manager which is password protected. For advice on creating secure passwords and keeping details safe staff should contact IT Services.

5.4 Certain IT systems are protected by multi-factor authentication (MFA) for an extra step of security. Staff must ensure that they have set this up where required, in order to keep their account and School data safe.

5.5 Staff are encouraged either to lock their screen or log out when leaving their desk, and to log out and shutdown their computer overnight. This will avoid others gaining unauthorised access to personal or confidential information within the School.

5.6 In order to comply with the School's obligations under the Data Protection Act, staff must use the blind copy (BCC) option when sending emails to multiple recipients where disclosure of those persons' email addresses will impinge upon their privacy. This is especially important when communicating to Parents.

5.7 In addition to the above, staff should familiarise themselves with the Data Protection Act 2018 and UK General Data Protection Regulation (UK-GDPR) and ensure that their use of email does not breach these. If staff require more information on compliance, contact the school's Privacy Officer.

6. Distribution and Copyright

6.1 When distributing information over the School's computer network or to third parties outside the School, staff must ensure that they and the School have the right to do so, and that they are not violating the intellectual property rights of any third party.

6.2 If staff are unsure of whether you have sufficient authorisation to distribute the information they should contact the Director of IT.

6.3 In particular, copyright law may apply to the information staff intend to distribute and must always be observed. The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files and downloaded information) must not be distributed through electronic message without specific authorisation to do so.

7. Social Media Rules

The School recognises that many staff make use of social media in a personal capacity outside the workplace and outside normal working hours. While they are not acting on behalf of the School in these circumstances, staff must be aware that they can still cause damage to the School if they are recognised online as being one of its staff. Therefore, it is important that the School has strict social media rules in place to protect its position.

When logging on to and using social media websites and blogs at any time, including personal use on non-School computers outside the workplace and outside normal working hours, staff must not:

- conduct themselves in a way that is potentially detrimental to the School or brings the School or its pupils, contractors, residents, parents, governors and suppliers into disrepute, for example by posting images or

video clips that are inappropriate or links to inappropriate website content

- allow their interaction on these websites or blogs to damage working relationships with or between staff and pupils, colleagues, contractors, residents, parents, governors and suppliers of the School, for example by criticising or arguing with such persons
- include personal information or data about the School's staff, pupils, colleagues, contractors, residents, parents, governors or suppliers without their express consent (an employee may still be liable even if staff, pupils, colleagues, contractors, residents, parents, governors or suppliers are not expressly named in the websites or blogs as long as the School reasonably believes they are identifiable) - this could constitute a breach of the Data Protection Act 2018 which is a criminal offence
- make any derogatory, offensive, discriminatory, untrue, negative, critical or defamatory comments about the School, its staff, pupils, contractors, residents, parents, governors or suppliers (an employee may still be liable even if the School, its staff, pupils, contractors, residents, parents, governors or suppliers are not expressly named in the websites or blogs as long as the School reasonably believes they are identifiable)
- make any comments about the School's staff that could constitute unlawful discrimination, harassment or cyber-bullying contrary to the Equality Act 2010 or post any images or video clips that are discriminatory or which may constitute unlawful harassment or cyber-bullying - staff can be personally liable for their actions under the legislation
- disclose any trade secrets or confidential, proprietary or sensitive information belonging to the School, its staff, pupils, colleagues, contractors, residents, parents, governors or suppliers or any information which could be used by one or more of the School's competitors, for example information about the School's work, its products and services, technical developments, deals that it is doing or future business plans and staff morale
- breach copyright, trademark law or any other proprietary interest belonging to the School, for example, using someone else's images or written content without permission or failing to give acknowledgement where permission has been given to reproduce particular work or using Harrow School branding. If staff wish to post images, photographs or videos of their work colleagues or pupils, contractors, residents, parents, governors or suppliers on their online profile, they should first obtain the other party's express permission to do so.

Staff must remove any offending content immediately if they are asked to do so by the School.

Staff should remember that social media websites are public, even if they have set their account privacy settings at a restricted access or "friends only" level, and therefore they should not assume that their postings on any website will remain private.

Staff must also be security conscious when using social media websites and should take appropriate steps to protect themselves from identity theft, for example by placing their privacy settings at a high level and restricting the amount of personal information they give out, e.g. date and place of birth. This type of information may form the basis of security questions and/or passwords on other websites, such as online banking.

Should staff notice any inaccurate information about the School online, they should report this to their line manager in the first instance.

8. Confidentiality

8.1 As mentioned above, the internet and electronic communications are insecure means of transmitting information. Therefore, items of a highly confidential or sensitive nature should not be sent via electronic communication unless it is encrypted or password protected. Alternatively a OneDrive link to the item can be used to restrict access to specific email addresses. Staff should be aware that emails sent between organisations can often be held by third party email companies so are not only stored on the School's network.

8.2 All emails that are sent outside of the School from School email addresses contain the School's standard disclaimer message. This message will be set to appear automatically on each outgoing email. Please contact IT Services if this feature is not working. The standard disclaimer is:

8.3 Always maintain a reasonable degree of caution regarding the identity of the sender of incoming email. Staff should verify the identity of the sender by other means if they have concerns. Please notify IT Services of any suspicious activity regarding suspect emails, clicked links or malicious attachments by providing details or a screenshot of the email. Staff should not forward suspicious emails on to anyone else.

9. Viruses

9.1 All external files and attachments will be automatically virus-checked using scanning software. However it is extremely important that staff always remain vigilant when opening attachments or clicking links contained in emails or other electronic communications. Failure to do so could have potentially catastrophic effects on the School network.

9.2 If you are concerned about an email attachment or believe that it has not been automatically scanned for viruses, do not open the attachment or reply to the email but contact IT Services.

10. General

10.1 This policy may be updated or revised from time to time. The School will notify staff annually of any revisions to this Policy. If staff are unsure whether they are reading the most current version, they should contact the Director of HR.

10.2 The terms and recommended conduct described in this Policy are not intended to be exhaustive, nor do they anticipate every possible use of the School's electronic communications and internet facilities. Staff are encouraged to act with caution and take into account the underlying principles intended by this Policy. If staff feel unsure of the appropriate action relating to use of electronic communications or the internet, they should contact IT Services.

11. Mobile Device User Agreement

This includes mobile phones, laptops, tablets and Surface devices and applies to Staff who have been issued with a mobile device to perform their work-related duties.

11.1 Where a device is allocated to a specific person it is intended for their use only. Allocated devices should not be transferred to other Staff or allowed to be used by others, including family members, in cases where these devices will be used away from the School.

11.2 Staff must follow the expectations outlined in this Policy when using the School issued device.

11.3 School devices are School property and should be used for School-related work and are not for personal use. If there are any investigations, Harrow IT Services reserve the right to, at any point, request the return of the issued device to perform any required searches of its contents.

11.4 In the event of failure to return a device or accessories upon departure from the School, you will be responsible for the full replacement cost of the items not returned.

11.5 If any OneDrive or OneNote data is stored on the mobile device, it must be backed up. Staff should report any OneDrive or OneNote sync errors (as shown by a red X, or a missing OneDrive icon) to IT Services as soon as possible to avoid possible data loss. In the event of a system failure or hardware problem, unsynchronised data is at risk. Staff should contact IT Services with any questions regarding this. Here is a link to more information.

11.6 Staff should use only software licensed or approved by Harrow School, as authorised and installed by the School's IT Services staff.

11.7 School mobile devices are covered by a limited manufacturer's warranty. This covers faults with the device but not accidental damage, loss or theft. The School's insurance policy does not cover loss, damage or theft of these devices. After a consideration of the circumstances, any repairs or replacements that are otherwise required (broken screens, water damage, theft etc.) could thus be recharged to the respective Staff member by the School depending upon the circumstances.

11.8 Staff should not modify or adjust the device in any way that voids the manufacturer's warranty. Staff making any such modifications will be liable for the full cost of the device in the event of a required repair or replacement.

11.9 The allocated device and all relevant accessories must be returned when the staff member's employment with Harrow School ceases, or when requested by the School. The use of the device provided by the School is not transferable to anyone and expires in line with the termination of the Staff member's contract of employment with Harrow School.

11.10 Where the School provides a laptop or Surface device BitLocker encryption will be enabled for the local disk on the mobile device. Staff should not under any circumstances attempt to disable or remove this encryption.

Director of IT
September 2023