HARROGATE LADIES' COLLEGE & HIGHFIELD

Independent School for Girls Aged 2 to 18 and Boys Aged 2 to 11

IT ACCEPTABLE USE POLICY

Harrogate Ladies' College family of Schools:

Highfield Pre School, Highfield and College

SLT Responsibility:

Governor Committee Review:

Next Review Date: September 2022

Introduction

1.1. Computers are increasingly becoming an integral part of our lives, both working and personal. Please make sure that you are familiar with and adhere to the following Policy.

1.2. This Policy applies to the use of:

1.2.1. all internet and e-mail facilities, workstations and any networks provided by the School; and
1.2.2. all hardware owned, leased, rented or borrowed, accessing school networks or other facilities.

1.3. The Staff IT Acceptable Use Policy (IT AUP) is published on iCommunity and each member of staff is directed to the Policy when they join the School as part of the induction process and when significant updates occur.

1.4. All members of staff are required to accept the terms of the Staff IT AUP every 90 days or when the Policy is updated. Acceptance of the Policy allows staff to be given an account with access to the School network.

1.5. When the Staff IT AUP is updated, staff are informed and asked to read the updated Policy on iCommunity. Paper copies are always available on request from the IT Department.

1.6. This Policy refers to all fixed/mobile electronic technologies and associated software that staff members have access to for personal and school use. This Policy deals mainly with the use (and misuse) of computer equipment, e-mail, the internet, telephones and voice-mail, but it applies equally to the use of copiers, printers, and security access cards. It outlines the standards we require users of these systems to observe, the circumstances in which we will monitor use of these systems and the action we will take in respect of breaches of these standards.

1.7. All staff members are expected to protect our electronic communications systems and equipment from unauthorised access and harm at all times. Failure to do so may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

2. Use of the School Facilities and Internet

2.1. Limited use of telephones, printers and internet facilities for personal purposes is permitted. The School acknowledges that personal use may occur from time to time. Any such use must be in accordance with this Policy and must not disrupt staff duties. Abuse or excessive use of these facilities will be dealt with through the disciplinary procedure.

2.2. On entry to the School, members of staff are assigned a home folder on the School network in which work may be stored. Users have responsibility for the content held within the folder, to ensure that the folder is managed and that they are always able to save new documents.

2.3. Users should not expect that files stored on laptops or servers would always be private. Senior staff may review files and communications to ensure that users are using the system responsibly. The School reserves the right to access their user-area and laptops, tablets or phones and any other forms of storage medium (e.g. CD, DVD, USB device) in their possession if it has grounds to suspect there may be inappropriate material on them.

2.4. Some content is restricted for security purposes. Should staff wish to block or unblock websites or YouTube clips they should do so by completing the form on iCommunity.

2.5. Staff should not access any web page or any files (whether documents, images or other) downloaded from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK, it may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of our AUP. Any indecent images found on any websites should be reported to the IT Department. The following are not permitted:

2.5.1. damaging, degrading or disrupting computers, computer systems or computer networks or performance;

2.5.2. violating copyright laws;

2.5.3. trespassing in others' folders, work or files;

2.5.4. intentionally wasting resources;

2.5.5. entering into any contact with current pupils via social networking or other similar sites;

2.5.6. presenting documents compiled from internet or school network resources as being their own work, or in any other way infringe a Copyright of any other person;

2.5.7. changing any of the computers' default settings, such as screensavers, backgrounds, folders, icons;

2.5.8. malicious damage to or tampering with any system on the School network or changing of data;

2.5.9. creating, transmitting or cause to be transmitted material which is designed or likely to cause annoyance, inconvenience, needless anxiety or offence;

2.5.10. creating, transmitting or cause to be transmitted offensive obscene or indecent material;

2.5.11. gaining unauthorised access to resources or websites by the use of internal/external wireless modems and VPNs. Use of such devices to gain unfiltered access to the internet is strictly forbidden; or

2.5.12. allowing pupils to use the staff member's account and network password.

2.6. Staff members who have been issued with a laptop, tablet or phone must ensure that it is kept secure at all times, especially when travelling. The Information Security Policy provides guidance on how to keep information secure. Staff are required to read this Policy alongside the Staff IT AUP.

3. Staff portable device use

3.1. Portable devices include mobile phones, tablets, laptops and cameras.

3.2. Staff may take the School's portable devices home as long as they are taken with the agreement of the IT Department.

3.3. The downloading of programs to School devices is prohibited.

3.4. The downloading of programs to personal devices is the responsibility of the user and the School cannot monitor or accept any responsibility for any programs that are installed or problems that an

installation might cause. It is the responsibility of the owner to ensure that she/he has a licence for all software installed on her/his device.

3.5. Under no circumstances should computers, printers or other devices be detached from the network to make way for a staff member's own computer or laptop.

3.6. The IT Department is empowered to scrutinise, and if necessary retain for further investigation, any device which is or has been attached to the network. All rules of usage for internet access and computer usage continue to apply.

3.7. The School does not accept any responsibility for the theft, loss of, or damage to, mobile phones brought onto school premises.

4. Mobile Phone device protocol

4.1. Use of personal mobile phones during work hours should be limited to urgent situations only. All devices should be silent during these times.

4.2. In cases of misuse of mobile phones, the user's network logon and internet access in school will also be suspended pending further investigation.

4.3. The School reserves the right to inform the police over any extreme material found on staff phones and ensure images are taken off social networking websites.

4.4. Any actions taken will be in accordance with the School's Disciplinary Policy and Safeguarding Policy.

5. Camera, photograph and video protocol

5.1. Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline and will result in disciplinary action being taken up to and including summary dismissal.

5.2. Posting of photographic or other material which, in the reasonable opinion of the Principal is considered to be offensive, on websites such as YouTube, Facebook, Twitter etc. is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material. This is the position whether the computer used is a school computer or a computer operated elsewhere including the staff member's home.

6. E-mail etiquette and content

6.1. All staff members are provided with an '@hlc.org.uk' e-mail account. This is the core mode of electronic communication in the School and staff members are required to use this account and to check it on a daily basis.

6.2. Staff should observe this Policy at all times and note the disciplinary consequences of non-compliance which in the case of a gross breach or repeated breach of the Policy, may lead to dismissal.

6.3. E-mail is a vital business tool, but an informal means of communication, and should be used with great care and discipline. Staff should always consider if e-mail is the appropriate means for a particular communication and appreciate that electronic mail is relatively insecure and consider security needs and confidentiality before transmission.

6.4. Staff should produce and write e-mail with the care normally given to any form of written communication.

6.5. Staff should ensure they use the School standard e-mail sign off for all external e-mails (a disclaimer is automatically included on all external e-mails).

6.6. Where appropriate, hard copies of e-mails should be kept on the appropriate pupil file or a copy sent to pupilfile@hlc.org.uk.

6.7. Staff should ensure that they access their e-mails at least once every working day, stay in touch by remote access when travelling and use an out of office response when away from the office. They should endeavour to respond to e-mails marked 'high priority' within 24 hours.

6.8. Staff should not send abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory e-mails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via e-mail should inform their line manager.

6.9. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff should assume that e-mail messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

6.10. E-mail messages may be disclosed in both legal proceedings and subject access requests in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail cannot be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable, either from the server or using specialist software.

6.11. In general, staff should not:

6.11.1. send or forward private or confidential e-mails at work which they would not want a third party to read;

6.11.2. send or forward chain mail, junk mail, cartoons, jokes or gossip;

6.11.3. contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;

6.11.4. agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained (a name typed at the end of an e-mail is a signature in the same way as a name written at the end of a letter);

6.11.5. download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;

6.11.6. send messages from another worker's computer or under an assumed name unless specifically authorised; or

6.11.7. join any mailing groups or lists without the consent of the School.

7. Printing

7.1. Staff members are encouraged to print responsibly and to try to avoid wastage where possible.

7.2. When printing a document of two or more pages to a desktop printer, you will be prompted about whether you would like the document to be duplexed or left as simplex.

7.3. When printing a colour document of more than five pages to a desktop printer, you will be prompted to convert the document to grayscale or continue printing in colour. Colour documents over thirty pages will be denied. Large colour documents should be sent to a photocopier.

7.4. Desktop printers are set to deny documents of more than thirty pages. These should be printed on photocopiers.

7.5. You will only be able to print two copies of a document to the desktop printers. Duplication should take place on photocopiers.

8. Social Media

8.1. A social networking site is any website which enables its users to create profiles, form relationships and share information with other users. It also includes sites which have online discussion forums, chat-rooms, media posting sites, blogs and any other social space online. It includes but is not limited to, sites such as Facebook, Snapchat, Instagram and Twitter.

8.2. This section of the Staff IT AUP Policy applies to the use of social media for both business and personal purposes, whether during school hours or otherwise. The Policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff or any other IT equipment.

8.3. Staff may be required to remove internet postings which are deemed to constitute a breach of this Policy. Failure to comply with such a request may in itself result in disciplinary action.

8.4. Staff are prohibited from using social media to:

8.4.1. breach our obligations with respect to the rules of relevant regulatory bodies;

8.4.2. breach any obligations they may have relating to confidentiality;

8.4.3. breach our Disciplinary Rules;

8.4.4. defame or disparage the School or our affiliates, parents, staff, pupils, business partners, suppliers, vendors or other stakeholders;

8.4.5. harass or bully other staff in any way or breach our Dignity at Work Policy;

8.4.6. unlawfully discriminate against other staff or third parties or breach our Equal Opportunities Policy;

8.4.7. breach our Data Protection Policy (for example, never disclose personal information about a colleague, pupil or parent online); or

8.4.8. breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

9. Responsible use of social media

9.1. Staff must be aware that their role comes with particular responsibilities and they must adhere to the School's strict approach to social media.

9.2. Behaviour online can be permanent and so staff must be extra cautious about what they say as it can be harder to retract.

9.3. Staff must:

9.3.1. ensure that wherever possible their privacy settings on social media sites are set so that pupils cannot access information relating to their personal lives;

9.3.2. obtain the prior written approval of the Director of Admissions and Marketing to the wording of any personal profile which you intend to create where the School is named or mentioned on a social networking site;

9.3.3. seek approval from the Director of Admissions and Marketing before they speak about or make any comments on behalf of the School on the internet or through any social networking site;

9.3.4. report to their Line Manager immediately if they see any information on the internet or on social networking sites that disparages or reflects poorly on the School;

9.3.5. immediately remove any internet postings which are deemed by the School to constitute a breach of this or any other school policy;

9.3.6. consider whether a particular posting puts their effectiveness as a member of staff at risk; and

9.3.7. post only what they wish to be in the public domain.

9.4. Staff must not:

9.4.1. provide references for other individuals, on social or professional networking sites, as such references whether positive or negative can be attributed to the School and create legal liability for both the author of the reference and the School;

9.4.2. except for identifying their place of work, post or publish on the internet or on any social networking site, any reference to the School, your colleagues, parents or pupils;

9.4.3. use commentary deemed to be defamatory, obscene, proprietary, or libellous. Staff must exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations;

9.4.4. discuss pupils or colleagues or criticise the School or staff;

9.4.5. post images that include pupils unless it is via an approved school channel;

9.4.6. initiate friendships with current pupils on any personal social network sites; or

9.4.7. accept pupils as friends on any such sites; staff must decline any pupil-initiated friend requests.

10. The use of social media for School purposes

10.1. Social media should not be used for purposes relating to the School's business unless the prior authority of the Director of Marketing and Admissions has been obtained.

10.2. Social media should not be used for purposes relating to the delivery of the curriculum to pupils unless the prior authority of the Deputy Head Academic has been obtained.

10.3. Where the use of social media is authorised for such purposes, any social media accounts (including blogs, forums, twitter etc.), sites or pages used or set up for the purpose of furthering the School's business or facilitating the provision of the curriculum to its pupils shall remain the property of the School.

11. Communicating with the Media

11.1. You must not speak to or communicate with the media on matters concerning the School's affairs or regarding your position in the School without the prior written permission of the Director of Admissions of Marketing. This includes postings on social media, e-petitions etc. where you may be identified as an employee of the School.

12. Personal use of social media

12.1. We recognise that staff may work long hours and occasionally may desire to use social media for personal activities at the office or by means of our computers, networks and other IT resources and communications systems. We authorise such occasional use so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity.

12.2. While using social media at work, circulating chain letters or other spam is never permitted.

12.3. Staff must ensure that their use of social media does not create any breaches of internet security and therefore must be careful to avoid any applications that might interrupt our IT systems.

12.4. Excessive use of social media that interrupts staff productivity will be subject to a disciplinary procedure, consistent with this Policy.

12.5. We prohibit staff from using their work e-mail address for any personal use of social media

13. The monitoring of social media

13.1. The contents of our IT resources and communications systems are our property. Therefore, staff should have no expectation of privacy in any message, files, data, document, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

13.2. We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting,

reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other network monitoring technologies.

13.3. We may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

13.4. Staff must not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the organisation.

14. Social media and the end of employment

14.1. If a member of staff's employment with the School should end, for whatever reason, any personal profiles on social networking sites should be immediately amended to reflect the fact that you are no longer employed or associated with our School.

14.2. All professional contacts that a member of staff has made through their course of employment with us belong to our School, regardless of whether or not the member of staff has made social media connections with them.

14.3. All members of staff agree that on the termination of employment they will provide to the Director of Admissions and Marketing any relevant passwords and other information to allow access to any social media site, page or account which has been used or set up for the purpose of furthering the School's business or facilitating the provision of its curriculum and will relinquish any authority they may have to manage or administer any such site, page or account.

15. Health and Safety

15.1. In line with health and safety policies always ensure you are in the right environment to work and your remote work-station allows for correct posture and safe working practice. It is the individual's responsibility to seek advice on the appropriate working conditions for remote use and follow national guidelines.

16. Monitoring and Breach of this Policy

16.1. The School reserves the right to monitor the use and content of all technology in order to:

16.1.1. ascertain compliance with regulatory or self-regulatory procedures;

16.1.2. monitor standards which are achieved by persons using the system in the course of their duties and for staff training purposes;

16.1.3. to prevent or detect crime;

16.1.4. to investigate or detect unauthorised use of the School's telecommunication system;

16.1.5. ensuring the effective operation of the system such as protecting against viruses, backing up and making routine interceptions such as forwarding e-mails to correct destinations; and

16.1.6. to gain access to routine business communications for instance checking voice mail and e-mail when staff are on holiday or on sick leave.

16.2. Any breach of this Policy may result in disciplinary action being taken up to and including summary dismissal.