HARROGATE LADIES' COLLEGE & HIGHFIELD

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

HARROGATE LADIES' COLLEGE PUPIL ACCEPTABLE USE OF ICT AND ONLINE SAFETY POLICY

Highfield Pre School, Highfield and College

SLT Responsibility: Siobhan Scully

Governor Committee Review: Pupil Welfare

Review Date: March 2021

Next Review Date: March 2022

PRINCIPAL: Sylvia F. Brett BA (Dunelm), MA (London). **COLLEGE VISITOR:** Baroness Harris of Richmond.
Clarence Drive • Harrogate • North Yorkshire • HG1 2QG **T:** +44 (0)1423 504543 **E:** enquire@hlc.org.uk **www.hlc.org.uk**

REGISTERED OFFICE: Harrogate Ladies' College, Clarence Drive, Harrogate, North Yorkshire HG1 2QG.
Harrogate Ladies' College is registered as a Company in England. Registered number 197987. Educational Charity Registered No. 529579.

Since 1893

1. Introduction

This policy applies to the Harrogate Ladies' College Family of Schools – Highfield Pre-School, Highfield and College - hereafter referred to as "the School".

This Policy on the Acceptable Use of ICT and Online Safety is published on the School Intranet and an electronic copy is provided to each pupil when they join the School as part of the induction process and when significant updates occur.

All pupils and their parents are required to accept the terms of this policy on a termly basis. Acceptance of the policy allows them to be given a pupil account with access to the School network. The School actively promotes the participation of parents to help the School safeguard the welfare of pupils and promote online safety. Some guidance for parents is set out in section 12 below.

When this policy is updated, a new version is provided to all pupils electronically, is published on the website and stored in the School's Policy folder. Paper copies are always available on request from the Senior Deputy Head.

This policy applies to the use of all fixed/mobile electronic technologies and associated software that pupils have access to for personal and school use that might pose e-safety risks during a school day together with any use at any time, whether on or off School premises, which affects the welfare of other pupils or where the culture or reputation of the School are put at risk.

Pupils are responsible for good behaviour on the School network and the Internet, just as they are in the classroom or in a school corridor. General school standards and procedures apply to all who make use of the School's facilities and equipment.

Alongside this Pupil Acceptable Use of ICT and Online Safety Policy, during times of remote learning, the Remote Learning Policy must be adhered to as well. The Remote Learning Policy can be accessed on the School website and via the School Intranet. All pupils are given an electronic copy of this policy when they join the School and when significant updates occur.

Staff are subject to separate policies which forms part of their contract of employment.

2. Online Safety - the School's responsibilities

The School is committed to safeguarding the welfare of all pupils and recognises that an effective online-safety strategy is paramount to this.

The School's responsibilities include:

- Focusing on online safety in all areas of the curriculum and reinforcing key online safety messages as part of assemblies and tutorial / pastoral activities, teaching pupils:
  a) about the risks associated with using the internet and how to protect themselves from potential risks;
  b) to be critically aware of content they access online and guided to validate accuracy of information;

c) how to recognise suspicious, extremist or bullying behaviour;

d) the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

e) the consequences of negative online behaviour; and

f) how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly;

- Ensuring that the School's staff act as good role models in their use of technologies, the internet and mobile electronic devices;
- Providing sufficient online safety training to staff to protect pupils and themselves from online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development training includes training on online safety;
- Logging and monitoring online safety incidents and regularly reviewing this policy to ensure that the School's online safety practices and procedures are adequate.

Pupils must comply with the rules in this policy to keep themselves, and others, safe online.

3. Use of the School Network and Internet

Computer storage areas, personal laptops and other portable storage devices will be treated as areas of personal storage. On entry to the School, pupils are assigned a folder on the School network in which work may be stored. Users have responsibility to ensure that the folder is managed and that they are always able to save new documents.

Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on laptops or servers or disks would always be private, nor that they might hide materials they have downloaded. The School reserves the right to access their user-area and personal devices 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.

The following are not permitted:

- Damaging, degrading or disrupting computers, computer systems or computer networks or performance;
- Violating copyright laws;
- Using others’ passwords;
- Trespassing in others’ folders, work or files;
- Intentionally wasting resources;
- Any act which results in upheld complaints to, or legal action against, the School;
- Using the School network for illegal activity;

- Viewing, retrieving, downloading or sharing any material which in the reasonable opinion of the Principal is unsuitable.
- Presenting documents compiled from Internet or School network resources as being the pupil's own work;
- Changing any of the computers' default settings, such as screensavers, backgrounds, folders, icons;
- Installing any software whatsoever;
- Circumvention of security or accounting provisions. **The use of routers or dongles is banned in School, the access to wifi rendering these devices unnecessary and a security risk to the School network;**
- Malicious damage to or tampering with any system on the School network or changing of data;
- Transmission, creation or possession of threatening, extremist, defamatory or obscene material;
- Gaining unauthorised access to resources or websites by the use of internal/external wireless modems. Use of such devices to gain unfiltered access to the Internet is strictly forbidden.

4. Bring Your Own Device (BYOD)

A "device" includes, but is not limited to, laptops, tablet computers, iPods and mobile phones.

Pupils in Highfield Pre-School and Highfield are not permitted to bring any mobile electronic device onto the School premises without the express permission of a member of staff. All other pupils must comply with the guidelines below specifically relating to BYOD.

The School is fully committed to enabling all pupils to access technology to enhance Teaching and Learning, within a safe and secure environment at Harrogate Ladies' College. Technology is an important element of HLC's teaching and forms an integral part of a modern curriculum. The School seeks to raise the standard of each pupil's digital competence through regular opportunities to use technology within their studies.

There are three IT suites and numerous resource and study areas equipped with computers which pupils can use, many now choose to use their own devices. Therefore, parents have been informed about BYOD, whereby their daughters can use their own laptop or tablet device at School.

These devices need to be insured and the School requests all pupils store their devices within their lockable space when they are not in use in lessons.

Teaching resources are held largely via the Learning Platform, Firefly, which is available both in school and also from home, to ensure day pupils have the same access to resources at the end of the school day: https://fireflycloud.net.

Users of BYOD:

1. The School recommends that Middle School and Sixth Form pupils bring their own device into School every day.
2. In Lower School, due to COVID- 19 restrictions, and the need to access assemblies and House events remotely, Lower School pupils are currently users of BYOD.
3. Pupils requiring laptop use for SEND requirements can either bring in their own laptop or tablet or will be provided with access to a laptop and should follow guidelines as per the SEND policy.

Recommended software for BYOD

- HLC's aim is to ensure that resources are available to any of the standard web browsers. HLC's Learning Platform https://fireflycloud.net and email systems https://hlc.rmunify.com are accessible remotely via a web browser.
- The pupil's device must have a modern web browser such as Edge, Google Chrome, Firefox or Safari.
- The device should have software compatible with the latest Microsoft Office suite of programs.
- All devices must have a suitable Internet Security system installed to guard against Virus infection and any hacking attempts. The mobile nature of devices mean they are also likely to be used at home and at wireless hotspots where risks for hacking and virus infection is much greater.
- The school network is secure and has several levels of Virus protection. HLC uses SOPOS to prevent the resources which are accessed whilst at School being infected. Smoothwall is used as an Internet filtering and firewall system.
- Pupils will only be able to access the internet via the school wifi and no dongles/4G mobile networks are acceptable for use in school.

Recommended device for BYOD

- The cost and size of laptops and tablets can vary dramatically. HLC recommends that devices weigh less than 2kg, and have a screen smaller than 15" but bigger than 9". The School recommends devices which have a suitable keyboard for longer term use. Pupils are expected to have a protective case for their device, and details of the device including serial number, make and model should be kept in case of any problems.
- The device should have battery capable of lasting the school day, and should be brought into school fully charged.

General Principles for mobile devices:

- The downloading of programs to these 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. The downloading of programs to a personal laptop is the responsibility of the user and the School cannot monitor or accept any responsibility for any programs that are installed.
- Pupils must not use their own devices in lessons unless authorised by a subject teacher and only then for the purpose of school-related work.
- Pupils may only connect their own devices to the School's network. Access to the internet via a mobile service is not permitted on School premises.
- Under no circumstances should School computers, printers or other devices be detached from the network to make way for a pupil's own device.
- Pupils are responsible for the material that exists on, or is accessed via, their own devices. The Network Services 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 as set out in this policy continue to apply.
- It is the responsibility of the owner to ensure that a licence is in place for all software installed on the device.
- The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto school premises, including those that have been confiscated or which have been handed in to the School Office or Examinations Officer.
- Pupils must not use mobile electronic devices in any manner which in the reasonable opinion of the Principal is inappropriate.

Failure of pupils to follow the guidelines as laid out above will lead to the immediate confiscation of the device and could lead to further disciplinary action being taken, including suspension of the pupil's network logon and Internet access. Devices may be searched in appropriate circumstances, for further information, consult the School's Behaviour Policy.

5. Mobile phone protocol

Some pupils walk to and from school each day and may therefore wish to carry a mobile phone with them. All pupils doing this must hand their mobile phone into the School Office at the start of the school day. They can then be collect it before the pupil leaves.

- Pupils from Upper 3 to Upper 4 must hand any mobile phones into their Form Teacher during morning registration and must collect them from the School Office at the end of the school day, unless they are given express permission by a staff member to use them in a lesson;
- Pupils in Lower 5 and Upper 5 may keep mobile phones about their person but they must be turned off during lesson times. The exception is Upper 5 who may use the phones at break and

lunch times in the Upper 5 Common Room or their form room and Lower 5 who may use their phones in their form rooms at break and lunchtime;

- Pupils in the Sixth Form may keep their mobile device about their person but should only use them outside lesson time unless with the permission of the staff member for that lesson. Use must be restricted to the Sixth Form Centre only;
- Parents wishing to contact their children in an emergency should always telephone the School Office and a message will be relayed promptly;
- Pupils may not bring mobile phones, Smart Watches or any other wearables into examination rooms under any circumstances. If brought to the exam room by the pupil, they must be handed in before and then collected after the examination at the door.
- Pupils permitted to bring mobile phones onto School premises may only use it during School hours with express permission from their subject teacher, Head of School or Housemistress and they may be supervised. In emergencies, pupils may request to use the school telephone.
- Pupils must not use mobile phones in any manner which in the reasonable opinion of the Principal is inappropriate. The taking and storing of indecent images and sexting are serious breaches of discipline and safeguarding issues.
- The School reserves the right to confiscate a pupil's mobile phone for a specified period of time if the pupil is found to be in breach of this policy. The mobile may be searched in appropriate circumstances (see the School's Behaviour Policy). The pupil may also be prevented from bringing a mobile phone into the School temporarily or permanently and at the sole discretion of the Principal.
- Pupils should not use mobile phones to communicate with staff via staffs personal electronic devices. If there are reasonable grounds to believe that inappropriate communications have taken place, the Principal will require the relevant devices to be produced for examination and the usual disciplinary procedures will apply. Staff on school trips and House staff are provided with School phones in order to communicate with pupils.

6. Camera, photograph and video protocol

- Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.
- Lower School Pupils are not allowed to operate mobile phones during school hours. They may only use cameras or other devices with the capability for recording and/or storing still or moving images with the express permission of the member of staff in charge and with the permission of those appearing in the image.
- Lower 6 and Upper 6 pupils may take images with cameras or mobile electronic devices with a camera facility only with the express permission of all those appearing in the image.

- All pupils must allow members of the School’s Senior Leadership Team to access images stored on mobile phones and/or cameras and must delete images if requested to do so. This would only be done if the School had reason to believe that the image constitutes a breach of School discipline.
- Posting of photographic material which in the reasonable opinion of the Principal is considered to be offensive on websites such as YouTube, Instagram, Tik Tok, 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 device used is a School computer, or a device operated elsewhere including the pupil's home.
- Cameras and mobile electronic devices with a camera facility may be confiscated and searched in appropriate circumstances (see the School's Behaviour Policy). If the Principal has reasonable grounds to believe that a pupil's camera or mobile electronic device contains images, text messages or other material that may constitute evidence of criminal activity, she may hand the device to the Police for examination.
- Use of cameras, mobile electronic devices with camera facilities or laptop computers in breach of this policy may result in confiscation of the equipment until the end of term and the pupil may be permanently banned from bringing a camera, mobile electronic device or laptop onto School premises in future.

7. Email

On joining HLC, all pupils are provided with a ‘@hlc.org.uk’ email account, subject to parent/guardian approval. This is the core mode of electronic communication between staff and pupils. Pupils are encouraged to use this account and to check it on a daily basis.

Pupils should not communicate with staff using private email accounts. Private email addresses should only be used by the school as part of HLC communication and after the release of examination results once the pupil has officially left HLC. Until a pupil has left HLC, staff may only communicate with a pupil via school email accounts.

All emails from and to the pupil’s @hlc email account are subject to the same standards applied elsewhere in this policy. Pupils should follow the guidelines of Use of the School’s Network and Internet, Section 3 above. Pupils should be aware of issues related to ‘cyber-bullying’ and sanctions as outlined in this policy, Section 9 and 16 below.

8. Personal Safety

Pupils must not:

- Pupils must not use any type of social media to interact with people that they do not know in person;

- Reveal their home address, image, or phone numbers, or those of other pupils or of staff when on-line. They must use school addresses and phone numbers only;
- Arrange to meet someone that they have only met on the Internet or by email or in a chat room.
- Share their network password or allow others to use it;

Pupils must:

- Use only their account and keep their password private;
- Create a strong password and change their password regularly;
- Report to a system administrator, teacher or administrator any unsolicited email, security problems, any unpleasant or inappropriate material, messages, or anything that makes them feel uncomfortable when on-line;
- Use social and blogging websites with great care being aware of the dangers that can be associated with posting pictures, text, opinions, videos and communications on-line. All social networking sites such as Facebook, Twitter and qq.com are restricted as explained in section 10 'Use of Social Networks';
- Make themselves aware of the security settings available when using social and blogging websites to protect personal information which is published on-line.

9. Cyber-bullying

Cyberbullying is the use of ICT, particularly mobile electronic devices and the Internet, deliberately to upset someone else. Any behaviour which seeks to intimidate or humiliate and which is repeated, intentional, malicious, such as to cause distress, unhappiness or insecurity, is strictly forbidden.

Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

On the School's Firefly dashboard there is an icon to https://www.thinkuknow.co.uk/the education programme from NCA-CEOP, a UK organisation which protects children both online and offline.

Pupils should remember the following:

- Always respect others - be careful what you say online and what images you send.
- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- Do not retaliate or reply online.
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to evidence what is happening and can be used by the School to investigate the matter.

- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving inappropriately.
- It is important to act. In the event that a pupil witnesses cyberbullying, it is important to support the victim and report the bully.

If any pupil thinks that they, or another person, is being bullied, they should talk to a teacher or any trusted adult about the incident as soon as possible. For further guidance, see the School's Anti-bullying Policy.

The website http://www.digizen.org/kids/ also provides useful support and resources to pupils who may feel uncomfortable with their use of the Internet. Other useful resources include:

- https://www.internetmatters.org/
- https://www.ceop.police.uk/safety-centre/
- https://www.issuesonline.co.uk/subscription/login
- http://www.saferinternet.org.uk/
- http://www.kidsmart.org.uk
- http://www.safetynetkids.org.uk/
- http://www.safekids.com/
- http://www.thinkuknow.co.uk

10. Use of Social Networks

- The use of social networking sites such as Facebook, Twitter, qq.com or similar sites is prohibited during the school day. Access is only available between 7.00am and 7.30am and after 7.00pm and is restricted to pupils in Middle School or older;
- Pupils must never make contact or chat to anyone who is not known to them and only invite known friends to chat rooms or alike;
- Pupils should only accept friendship requests from people they know in real life;
- ‘Friend’ requests must not be made to or by members of the School’s staff;
- Pupils must consider how the images they share or comments they make may be used or viewed by others. Abusive or bullying language must never be used, nor should any other inappropriate language or comments be made;
- Pupils must not make comments about the School, staff members, other pupils or any other person that could be considered as defamatory or which could bring the School into disrepute. Behaviour of this kind will result in disciplinary action being taken in accordance with this policy and the School's Behaviour Policy;

- Inappropriate use of social networking sites may be reported to the site hosting it and inappropriate posts removed.

11. Guidelines for boarders

Boarding pupils are subject to all of the provisions in this policy at all times. Pupils may use the sockets or wireless network available in each of the boarding houses to remotely log on to the School system and use the Internet. This access is monitored by the Housemistress or Assistant Housemistress and may be suspended, at their discretion, if it is believed that a girl is spending too much time on the Internet.

Internet access is available as follows:

Year Group	**Internet Access Times**
• Upper 3	• 6.00am – 8.30pm each week day (Sunday to Thursday) • 6.00am – 10.00pm on weekends (Friday and Saturday)
• Lower 4	• 6.00am – 9.00pm each week day (Sunday to Thursday) • 6.00am – 10.00pm on weekends (Friday and Saturday)
• Upper 4	• 6.00am – 9.30pm each week day (Sunday to Thursday) • 6.00am – 10.00pm on weekends (Friday and Saturday)
• Lower 5	• 6.00am – 10.00pm every day
• Upper 5	• 6.00am – 10.30pm every day
• Sixth Form	• 6.00am – 11.00pm every day

- After 7.00pm, access to approved recreational sites is permitted on the boarding computing facilities. Requests for particular sites to be made available should be directed to the Housemistress or Assistant Housemistress in the first instance;
- Connection to the Internet will be disabled every night in accordance with the timetable above;
- All activity on the School's computing facilities is monitored, which will alert the ICT department to any breaches of this policy;
- Pupils are welcome to use their own electronic devices capable of connecting to a wireless network, including laptops, tablet computers, iPods and mobile phones but these should only be connected to the School's network. Connection to the internet via a mobile service is not permitted. Please contact the Network Services Department by telephone for further information.

- Middle School and Sixth Form pupils should ensure all mobile phones and tablets are turned off at the end of the day. These times are in line with the Internet access times for their year group and are shown in the table above;
- Lower School must hand in all electronic devices to the staff member on duty, each evening, from Sunday to Thursday. The times for the handing in of devices is in line with the Internet access times for their year group, (shown in the table above);
- Please refer to the Boarders' Handbook for further information about communication in the boarding houses.

12. Guidance for parents and guardians

The School expects parents and guardians to:

- Promote online safety and to support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;
- Talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour;
- Encourage their child to speak to someone if they are being bullied or need support;
- Encourage their child to adheres to the Remote Learning Policy https://www.hlc.org.uk/school-policies/

The online resources above provide useful information together with the DfE guidance Advice for Parents and Carers on Cyberbullying.

Useful resources for parents include:

- www.internetmatters.org
- www.commonsensemedia.org
- www.thinkuknow.co.uk
- www.safeinternet.org.uk

If parents or guardians have any concerns or require any information about online safety, they should contact the Senior Deputy Head or a Designated Safeguarding Person.

13. Safeguarding and Prevent

The school recognises that it has a duty under Section 26 of the Counter-Terrorism and Security Act (2015) to have due regard to the need to prevent people from being drawn into terrorism and to promote and safeguard the welfare of children and vulnerable adults (Education Act 2002, KCSIE 2019).

Staff are responsible for the well-being of the pupils and must ensure age appropriate material only is accessible via the school network by the use of filters. Any member of staff who feels someone is showing an interest in extremist, abusive or inappropriate material should report this to the DSL in the first instance.

Any member of staff who believes pupils have access to inappropriate material should report this to the IT manager.

14. Printing

All pupils are allowed a set number of printer credits for the year, these are allocated on a monthly basis. Pupils who use more than their monthly allocation may request more credits by contacting 'support@hlc.org.uk'. Any additional credits will be taken from the following months' allocation. Credits are shown as a cost in pounds and pence with a black and white print costing approximately 1p and a colour print costing approximately 8p per page of A4.

15. Procedures

Pupils are responsible for their actions, conduct and behaviour on the internet in the same way that they are responsible during classes or at break time. Use of technology should be safe, responsible and legal. Violations of the rules in this policy will be dealt with in accordance with the School's Behaviour Policy.

Bullying incidents involving the use of technology will be dealt with under the School's Anti-bullying Policy.

If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's child protection procedures outlined in the School's Safeguarding and Child Protection Policy. If a pupil is worried about something that he/she has seen on the internet, he/ she should talk to a teacher about it as soon as possible.

16. Sanctions

Violations of the rules in this policy will result in a temporary or permanent ban from the School network. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour in accordance with the School's Behaviour Policy including confiscation of devices and, in the most serious cases, expulsion. Any action taken will depend on the seriousness of the offence. When applicable, the Police or local authorities may be involved.

The School reserves the right to charge a pupil or his / her parents for any costs incurred to the School, or to indemnify any significant liability incurred by the School, as a result of a breach of this policy.

17. Monitoring and review

All serious online safety incidents will be logged. The Senior Deputy has responsibility for the implementation and annual review of this policy and will consider the record of online safety incidents and new technologies, with the Safeguarding team where appropriate, to decide whether or not existing security and e-safety practices and procedures are adequate.

The Senior Deputy will report, annually, to the Governors on the effectiveness of the School's online safety and acceptable use of ICT procedures.