IT Acceptable Use & E-safety Policy

Mission Statement

'To educate young people to meet the challenges of life courageously, to use their talents to the full and to live the values of Christ's Gospel'

This policy outlines our purpose in providing IT e-safety facilities and access to the internet and explains how the school is seeking to avoid the potential problems caused by unrestricted internet access.

Internet access in school

Providing access to the internet in school will raise educational standards and support the professional work of staff.

Teachers and students will have access to web sites world-wide (including museums and art galleries) offering educational resources, news and current events. There will be opportunities for discussion with experts in many fields and to communicate and exchange information with students and others world-wide.

In addition, staff will have the opportunity to access educational materials and good curriculum practice, to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the LEA and DfE and receive up-to-date information.

The internet will also be used to enhance the school's management information and business administration systems.

All staff (including teachers, technicians, learning support staff and boarding staff) and any other adults involved in supervising students accessing the internet, will be provided with the School IT Acceptable Use & E-safety Policy, and will have its importance explained to them.

Our school IT Acceptable Use & E-safety Policy will be available for parents and others to read on demand.

Ensuring Internet access is appropriate and safe

The internet is a communications medium and is freely available to any person wishing to send e-mail or publish a web site. In common with other media such as magazines, books and video, some material available on the internet is unsuitable for students. Students in school are unlikely to see inappropriate content in books due to selection by publisher and teacher and the school will take every practical measure to ensure that students do not encounter upsetting, offensive or otherwise inappropriate material on the internet. The following key measures have been adopted to help ensure that our students are not exposed to unsuitable material:

- our internet access is purchased from Exponential-E and is filtered and monitored by our firewalls to prevent access to material inappropriate for students;

- Day students using the internet will normally be working in the classroom, during lesson time and during private study where they will be supervised by an adult (usually the class teacher) (all internet usage is monitored and restricted);
- staff will check that the sites pre-selected for student use are appropriate to the age and maturity of students;
- staff will be particularly vigilant when students are undertaking their own search and will check that the students are following the agreed search plan;
- a report is generated daily to identify searches of concern by students, which is emailed to and reviewed by the Deputy Head (DSL), the IT Manager and the House Mistresses. This includes multi-lingual checks.
- students will be taught to use e-mail and the internet responsibly in order to reduce the risk to themselves and others;
- our 'Rules for Responsible internet Use' *(Shown at Appendix 1)* will be posted near computer systems.
- the IT Manager will monitor the effectiveness of internet access strategies;
- the IT Manager will ensure that occasional checks are made on files to monitor compliance with the school's IT Acceptable Use & E-safety Policy;
- the Headteacher will ensure that the policy is implemented effectively;
- methods to quantify and minimise the risk of students being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice from our Internet Service Provider, our IT network service company and the DfE.
- Students will be trained in the safe use of the internet in their PSHEE lessons, form time, IT lessons and the Sixth Form Horizons programme.

It is the experience of other schools that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. **The school cannot accept liability for the material accessed, or any consequences thereof**.

An important element of our 'Rules of Responsible internet Use' is that students will be taught to tell a teacher **immediately** if they encounter any material that makes them feel uncomfortable.

If there is an incident in which a student is exposed to offensive or upsetting material the school will wish to respond to the situation quickly and on several levels. Responsibility for handling incidents involving students will be taken by the Head of IT and IT Manager, in consultation with the Deputy Headteacher.

If one or more students discover (view) inappropriate material our first priority will be to give them appropriate support. The student's parents/guardians will be informed and will be given an explanation of the course of action the school has taken. The school aims to work with parents/guardians and students to resolve any issue.

If staff or students discover unsuitable sites, the IT Manager will be informed. The IT Manager will review and if necessary, block the website and report the URL (website address) and content to the Internet Service Provider; if it is thought that the material is illegal, after consultation with the ISP, the site will be referred to the internet Watch Foundation and the police. The IT Manager will also liaise with our IT network service company.
Students are expected to play their part in reducing the risk of viewing inappropriate material by obeying the 'Rules of Responsible Internet Use' which have been designed to help protect them from exposure to internet sites carrying offensive material. If students abuse the privileges of access to the

internet, or use of e-mail facilities, by failing to follow the 'Rules of Responsible Internet Use', rules they have been taught, or failing to follow the agreed search plan, when given the privilege of undertaking their own internet search, then sanctions consistent with our School Behaviour Policy will be applied. This may involve informing the parents/guardians. Teachers may also consider whether access to the internet may be denied for a period.

Maintaining the security of the school ICT network
We are aware that connection to the internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons.

The IT Manager will ensure virus protection is kept up to date (this is automated), will stay updated with IT news developments, and work with the IT Network Service Company to ensure system security strategies are relevant to protect the integrity of the network. These are reviewed regularly and improved as and when necessary. This may include restrictions on e-mail attachments and downloads.

Using the Internet to enhance learning
Students will learn how to use a web browser and suitable web search engines. Staff and students will use the internet to find and evaluate information. Access to the internet will become a planned part of the curriculum that will enrich and extend learning activities and will be integrated into the class schemes of work.

As in other areas of their work, we recognise that students learn most effectively when they are given clear objectives for internet use.

Different ways of accessing information from the internet will be used depending upon the nature of the material being accessed and the age of the students:

- access to the internet may be by teacher demonstration;
- students may access teacher-prepared materials, rather than the open internet;
- students may be given a suitable web page or a single web site to access;
- students may be provided with lists of relevant and suitable web sites which they may access; older, more experienced, students may be allowed to undertake their own internet search having agreed a search plan with their teacher; students will be expected to observe the 'Rules of Responsible Internet Use' and will be informed that checks can and will be made on files held on the system and the sites they access.
- Students will be able to use their own electronic device to gain access to the internet using Thornton Wi-Fi, logging on using their own school network credentials. This must be adhered to and will allow their usage to be appropriately restricted and website use monitored.

Younger students accessing the internet will be supervised by an adult, normally their teacher, at all times. They will only be allowed to use the internet once they have been taught the 'Rules of Responsible Internet Use' and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the students' minds as they monitor the students using the internet.
Senior students will receive e-safety training in Year 7 and regular updates during the preceding years. This will take place during IT lessons in Years 7-9 and in PSHEE in subsequent years, and the Sixth Form Horizon programme.
Training on the appropriate use of Social Media sites will be offered to parents and students via evening sessions.
In the Horizon programme, PSHEE and form time, students in the Sixth Form will revisit the above and receive specific teaching regarding the appropriate use of IT (including Social Media)

Using information from the Internet

We believe that, in order to use information from the internet effectively, it is important for students to develop an understanding of the nature of the internet and the information available. In particular, students should know that, unlike the school library for example, most of the information on the internet is intended for an adult audience, much of the information on the internet is not properly audited/edited and most of it has copyright.

Students will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV; teachers will ensure that students are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium); when copying materials from the Web, students will be taught to observe copyright; students will be made aware that the composer of an e-mail or the author of a web page may not be the person claimed.

Using e-mail

Students from Year 5 onwards will learn how to use an e-mail application and be taught e-mail conventions. Staff and students will begin to use internal e-mail to communicate with others, to request information and to share information. Years 3 & 4 use the school email only for communication with teachers during a 'working from home' scenario.

It is important that communications with people and organisations are properly managed to ensure appropriate educational use and that the good name of the school is maintained.

Therefore:

- students will only be allowed to use e-mail once they have been taught the 'Rules of Responsible Internet Use' and the reasons for these rules.
- teachers will endeavour to ensure that these rules remain uppermost in the students' minds as they monitor students using e-mail;
- students all have their own school email account;
- students may send e-mail as part of planned lessons;
- students may not access or send personal e-mail during lessons;
- students will have the e-mail messages they compose as part of planned lessons checked by a member of staff before sending them;
- the forwarding of chain letters will not be permitted;
- students will not be permitted to use e-mail at school to arrange to meet someone outside school hours or for personal use.

Internet access and home/school links

Parents will be informed on MSP that students are provided with internet access as part of their lessons or during private study times. We will keep parents in touch with future ICT developments by email or letter. Annual workshops on Online Safety will be offered by the Head of Computer Science.

Parental Contact

If parents have an emergency and need to contact their daughter, then they should do this through the normal school channels by telephoning the school reception. The office staff will ensure that the message is passed on to the student. Similarly, if students need to contact home, they can get permission from their teacher and will be allowed to do so by the school receptionist.

Using phones outside of class or without teacher permission

Students are not allowed to have their phones out during the school day without the teachers permission. Please refer to the behaviour ladder for sanctions.

Sixth Form students **may** use their devices for personal use outside of lessons. This includes making and receiving calls.

Boarding, Sixth Form and Year 11 - use of personal electronic devices (BYOD)
Boarding, Sixth Form Year 11 students and those students who have laptops identified as their normal way of working can use their personal electronic devices (including but not limited to laptop, netbook, smart phone, iPad, tablet/eReader) for work related reasons in lessons in agreement with the teacher, in their common rooms or in the Friends' Cafe. The 'Thornton Wi-Fi' network must be used to sign in; this network is monitored and filtered at all times. Any attempt to bypass the network, including the use of Virtual Private Networks (VPN's) or Proxies is strictly prohibited and will result in confiscation of the device. All BYOD devices are to be registered with the IT Manager before use in line with the BYOD Policy (*Appendix 3*). All students must follow the acceptable usage instructions as detailed below.

Acceptable Use of Electronic Devices
An electronic device is defined as any device that enables staff and students to connect to the internet or other electronic devices with mobile (3G/4G), Wi-Fi or Bluetooth networks. (E.g. tablets, phones, PDA, laptop etc.)

In order to promote effective teaching and learning during lessons and create an appropriate ethos around the school during the school day, electronic devices may be used in lessons but only when explicit permission has been given by the teacher. The following instructions do not extend permission to other times of the day or areas of the school.

1. In study sessions, during the day or after school, students may use an electronic device (e.g. smartphone or tablet) for work purposes only. Permission must be obtained from the teacher beforehand.
2. If a teacher suspects a student of not using a device for work-related purposes, then the student must immediately hand it to the teacher when asked to do so and, if the device is locked, unlock the device.
3. If the device is used for non-work purposes, then a teacher will confiscate it immediately. No warning need be given.
4. The device must be in silent mode, although, with the teacher's permission, music may be listened to through headphones.
5. Text messaging or other forms of electronic communication, including any use of social media, should not take place during these sessions, even if the message is work-related.
6. No photographs are to be taken or videos recorded unless explicit permission has been given by the teacher. Such occasions where permission might be given could include:
    a. The videoing of a practical activity so that the student can review at a later stage.
    b. To capture a; picture/homework/notes from a whiteboard.

    When photographs or videos are taken it is important that other students are not captured at the same time.
7. Devices are not to be shared, passed around or used for joint work, unless explicit permission has been given by the teacher. Only the owner of a device should use it and they are fully responsible for the content on it.

8. Students must use the 'Thornton Wi-Fi' network to access the internet to enhance their learning during lessons. They will be required to log on using their school network credentials.
9. Boarding students who wish to send and/or receive video conferencing calls are strictly limited to be made between boarding students and their immediate families and/or friends after school hours.
10. Taking, receiving, downloading, sharing and/or viewing photographs, videos, images or otherwise any content that contains nude or semi-nude depictions is strictly prohibited. All concerns will be referred to the DSL.
11. Boarders have their own Acceptable Use of Technology in Boarding [Appendix 4]

Security of devices

All personal devices are brought in at the student's own risk. All devices should require a password to be unlocked and this should never be divulged to any other student. Any electronic devices students bring into school must be switched off in the bottom of their bags. The school does not take any responsibility for stolen, lost or damaged devices, including lost or corrupted data on these devices. Please check with your homeowner's policy regarding coverage of personal electronic devices.

The school is not responsible for any possible device charges that may be incurred during school-related use.

Even though electronic devices may be used to promote learning, it is not a necessity for a student at Thornton College to possess an electronic device.

Security of Network and Data

The School recognises the potential of a Cyber Attack. To mitigate this risk the school takes the following steps:

- Anti-virus protection is in place.
- An External Vulnerability Scan is run on a periodic basis and any vulnerabilities are addressed where possible.
- Staff permissions in Management Information Systems are appropriate and reviewed regularly.
- Past staff and students accounts are disabled upon leaving the college.
- Regular automatically enforced password changes are implemented to all staff periodically.
- Two factor authentication is enabled for all cloud-based systems.
- Updates are actioned promptly across the network to include but not limited to:
    - Firewalls
    - Desktop Computers & Operating Systems
    - Backup Software
    - Filtering and Monitoring Software
    - Data Storage
    - Server Infrastructure

- Staff are advised to ensure that their passwords are complex, meet password complexity requirements and are kept secure.
- USB sticks are not to be used on the network – One Drive is preferred to prevent virus infection and potential data leaks.
- All staff are trained using the following link: – https://youtu.be/pP2VKWSagE0
- Staff iPads are set to six-digit pin entries and the lock screen engages quickly for safety. iPads are not left accessible to students or other staff.
- Staff refrain from ticking any boxes in systems to ensure that verification codes are saved

for several days.
- Lock screens on PCs are actioned when staff leave their desks. Staff room PCs are logged out after use.
- Encryption of sensitive business documents is in place.
- Staff have been trained and are on alert for suspicious phishing emails.
- Cyber-attack insurance protection is in place with CFC Underwriting Limited.

All this should be read concurrently with our GDPR Policy.

Visitor ICT & Wi-Fi

Visitors can use the Guest Wi-Fi available. A password will be made available to them upon request. They will be asked to read the Visitor IT & Wi-Fi Protocol *(Appendix 2).* Visitors may be given access to a restricted area on the network, governed by a password. No access will be given to databases, staff, or student areas.

Staff access to the Internet

New staff will receive training in the use of the internet through the school's induction programme. The Bursar is responsible for this aspect of the induction programme and this session is included in the general induction programme.

Staff may wish to access the internet for many purposes. Examples are:-

- to develop their teaching resources and / or to build their knowledge for supporting their teaching and learning.
- to communicate electronically with a range of individuals linked to education and the school to support the daily operation of the school.
- to receive educational publications or information of relevance to teaching and learning and / or the management of the school.
- to use "live" material on the internet directly in their teaching material.
- to use the internet for private purposes at appropriate times, provided it does not hinder any member of staff from fulfilling their duties.
- residential boarding staff may use the school network for personal use when off duty.

Staff using the internet must never:

- access information that is offensive and/ or inappropriate for use in a school, and/or save it to any medium.
- send offensive material through the school's internal or external email facilities.
- use the school's facilities to print out excessive material for private purposes.
- disclose any login username or password to anyone.
- leave their computers logged in.
- disclose any information regarding students or staff to any other person outside the school; all such information should be regarded as confidential and is covered by the Data Protection Act of 2018 as well as the schools GDPR Policy.
- download, use or upload any material from the internet, which is the copyright of others, unless an agreement has been entered into. *Please note: Any such agreements should go through the Headteacher or Bursar.*

Staff must:

- respect the privacy of other users.
- report any incident that breaches the Staff IT policy.
- Never capture images of students on their personal phones or devices. School equipment can only be used for this purpose.

Wi-Fi Access

Thornton College's IT network has been set up to a high degree of security to ensure that the school is protected as far as is reasonably possible from the threats associated with IT. We currently use a web-filtering system which is designed specifically to protect schools. Any access to the web will go via this system.

The school currently has a multiple wireless connection. Staff connect to Thornton-WiFi with their school network credentials.

Monitoring
The school will regularly monitor files on servers, workstations and laptops, as well as websites visited. The school is also entitled to intercept e-mails.

Staff who abuse the code set above will be liable to disciplinary action under the school's formal procedures.

Information within files in staff personal areas on the network may, on rare occasions, be accessed by the IT Manager or Bursar with the permission of the Headteacher, as part of their monitoring role. Such information cannot be assumed to be confidential. Child protection information can only be accessed by designated safeguarding persons.

Social Use of the Internet Outside School

Social Networking Sites
If staff use social networking sites, then they should take care to ensure that information available to the public is minimal and appropriate. Security on these websites should be tight, restricting open access.

It is not acceptable for members of staff to accept current students, or past students under the age of 21, as 'friends' on social networking sites, such as Facebook, Instagram, or X (formally Twitter), with the exception of staff who already have a 'friend' connection with their own child who attends Thornton College. In this instance staff should take care to adhere to any and all confidentiality agreements held by the school.
It is not acceptable for staff to make any contact with students or current parents via these personal websites. Staff should delete any such requests from their profile.

We recognise that such interactions have the potential to leave members of staff and students vulnerable.

Contact with parents via e-mail
Contact from a member of staff with parents should happen via the school e-mail only. All members of staff have a school e-mail address and this should be the one they use to correspond with parents.

Members of staff should not use their private e-mail addresses to contact parents or students.
A disclaimer must be attached to the signature of every e-mail sent by a member of staff.

Contact with parents may be carried out by alternatively using Isams or Firefly our VLE.

Contact with students via e-mail
Students are not permitted to have staff private e-mail address contact but may contact staff through their school email address at the behest of teacher. Communication with students will also be carried out using Firefly. In the Sixth Form, X (formally Twitter) can be used as a communication tool, i.e subjects may have an X account to share relevant articles. Any posts, comments or 'Tweets' used must

be appropriate and not violate the staff conduct policy.

Appendix 1

This information is available for all students and parents on MSP.

Rules for Responsible Internet Use

The school has installed computers with Internet access to help our learning. These rules will help keep us safe and help us be fair to others.

Using the computers:

- I will only access the computer system with my own username and password;
- I will not access other people's files;
- I will only bring in memory sticks or CDs from outside school to use on the school computers with permission from the ICT Teacher or Technician.
- I will not violate copyright laws.
- I will not use other people's passwords or accounts.
- I will be mindful when using limited resources including printer ink and paper.

Using the Internet:

- I will ask permission from a teacher before using the Internet;
- I will report any unpleasant material to my teacher immediately because this will help protect other students and myself;
- I understand that the school may check my computer files and may monitor the Internet sites I visit;
- I will not complete and send forms without permission from my teacher;
- I will not give my full name, my home address or telephone number when completing forms.
- I will not download music from the Internet or store my music on school computers.
- I will not give out the personal details of others.
- I will not upload/send photographs of myself or anyone at the school.

Using e-mail:

- I will check my personal e-mail only during scheduled lunch time or boarding house sessions;
- I will immediately report any unpleasant messages sent to me because this will help protect other students and myself;
- The messages I send will be polite and responsible;
- I will only e-mail people I know, or people my teacher has approved;
- I will only send an e-mail from a lesson when it has been checked by a teacher;
- I will not give my full name, my home address or telephone number to people I don't know.

Appendix 2

Visitor IT & Wi-Fi Protocol

Thornton College's IT network has been set up to ensure a high degree of security to ensure that pupils are protected as far as is reasonably possible from the threats associated with ICT. We currently use a web-filtering system which is designed specifically to protect schools. Any access to the web will go via this system.

As a visitor to Thornton College, you are welcome to use the school's wireless connections that are located around the school, on the following conditions:

1. You should login using the Guest Wi-Fi with a wireless key provided to access the wireless connection. This must be destroyed once you leave school and should not be passed on to any other user; it will not be passed on to any other person but will be for your sole use whilst you are visiting the school. Passwords to this area are changed regularly.
2. Ideally, you will use your own hardware device
3. If you do use the school's hardware, then you will log out when you are away from the machine, being ever vigilant of the security of the network.
4. You are responsible for protecting your own property.
5. The school will not be held responsible for damage to your property whilst on the school site.
6. You must never deliberately access information that is offensive and/ or inappropriate for use in a school, and/or save it to any external drive or cloud facility, neither on a school workstation or laptop.
7. You must not send offensive material through the school's internal or external email facilities.
8. You may not use the school's facilities to print out excessive material for private purposes.
9. You understand that you will not be able to access certain social networking sites.
10. You understand that the websites available will be monitored by the firewall system and searches for particular information will be visible by the Executive Team.
11. You will not contact any pupils by e-mail or exchange any personal contact information with them.

Appendix 3

Thornton College
Bring Your Own Device (BYOD) Policy

1. Introduction

The BYOD policy at Thornton College establishes guidelines for students bringing personal electronic

devices onto the school premises. This policy underscores the importance of network security by collecting users' device MAC addresses and emphasizes the need for security software to be installed on BYOD devices, acquired, and managed by the device owner.

2. Scope

This policy applies to all students bringing personal electronic devices, including smartphones, tablets, laptops, etc., onto the school premises.

The information requested in this document does not give Thornton College the ability to monitor the devices when they are taken off the premises.

3. Device Usage Guidelines

3.1. Acceptable Use:

- Devices are to be used for educational purposes during class time or as directed by teachers.
- Students are expected to exhibit respectful and responsible behaviour when using personal devices, following the school's code of conduct.

3.2. Network Access:

- Students are permitted to connect their devices to the school's Wi-Fi network, Thornton-Wi-Fi, using their school credentials.
- The school retains the right to monitor and filter internet usage to maintain a safe and secure learning environment.
- Students shall make no attempts to circumvent the school's network security. This includes setting up proxies and downloading programs to bypass security such as VPN's.
- Students shall not distribute pictures or video or any other material relating to students or staff without their permission (distribution can be as small as emailing/texting to one other person or as large as posting image or video online).

3.3. Security Software:

- All BYOD devices must have security software installed, including up-to-date antivirus and anti-malware protection.
- The responsibility for obtaining and maintaining security software lies with the device owner.
- Students must check their personal ICT device daily to ensure the device is free from unsuitable material and free from viruses and malware before bringing the device into school.
- If your device is identified to be utilising VPN/Proxy software on it, then it may be removed from the Thornton College wireless network as this can present a security risk to the schools network. It can also flood the schools firewall with traffic, causing it to be intermittent and unavailable to everyone for a prolonged period.

    - The device will only be allowed back onto the school's wireless network if proof of disablement and/or removal has been provided. Once the IT Team is satisfied that the software has been disabled and/or removed, the device will be allowed back on the network. However, if a second event is detected from the same device, then the device will be removed and not allowed back on for safety/security reasons.

4. Collection of MAC Addresses

4.1. Purpose:

- To enhance network security and manage network traffic effectively, the school will collect and store the MAC addresses of all devices connecting to the school's Wi-Fi network.

4.2. Procedure:

- At the beginning of each academic year or upon enrolment, students must register their device(s) with the school's IT department.
- The MAC address, along with the student's name and device information (device make, model and device name) will be recorded in a secure database.
- Any changes to the registered devices or if a new/replacement device is brought in, they must be promptly reported to the IT department before connecting to the school's Wi-Fi network.

4.3. Security Measures:

- Access to the MAC address database will be restricted to authorized personnel only and will be password protected.
- The school is committed to safeguarding the privacy and security of collected MAC addresses.
- When a student has left Thornton College, their information in the MAC address database will be removed.

5. Consent Form

By signing this form, I understand and agree to abide by the BYOD policy outlined above. I acknowledge that it is my responsibility to install and maintain security software on my personal devices. I also consent to the collection and storage of my device's information as described in section 4.2 for network security purposes.

If I am under the age of 18, I understand that my parent or guardian must also provide consent by signing below.

Student Name: _____

Student Signature: _____

Date: _____

Parent/Guardian Consent (if the student is under 18):

I, the undersigned, as the parent or legal guardian of _____, have read and understood the BYOD policy. I give my consent for my child to bring personal electronic devices to school and agree to the terms outlined in this policy, including the collection of the device's information as described in section 4.2, and the responsibility for security software installation.

Parent/Guardian Signature: _____

Date: _____

Appendix 4

ACCEPTABLE USE OF TECHNOLOGY IN BOARDING AGREEMENT

2024-25

The boarding house encourages the use of technology to facilitate communication between boarding students and their family and friends. The school notes the potential social benefits of technology use but is also aware of the downsides and potential for misuse. Boarders are advised on positive ways to use technology and must avoid inappropriate use. Boarders are required to use their technology in accordance with the rules outlined in the Acceptable Use of Technology in Boarding Policy.

PERMITTED USES

Boarding students have access to their mobile devices as well as the computers available to them in ICT1 after school. The boarding house provides time in the evenings, in addition to study, between 16:20 – 17:30 for boarders to use the computers if needed for homework and studying. Boarders are required to hand in ALL devices every evening, to be stored in the locked boarding office overnight. Timings for device hand ins are dependent on the school year of each boarder. Year 11 and above do not need to hand in their phone on the weekend unless parents request otherwise, or unless Boarding Staff believe an alternative arrangement should be in place. Sixth Form (years 12 and 13) can always have their phones with them, unless requested otherwise by parents, or unless Boarding Staff believe an alternative arrangement should be in place.

PROHIBITED USES

School computers and mobile devices must not knowingly be used to:

- Send or receive material that is, or may be interpreted to be, obscene, derogatory, defamatory, harassing, threatening, vilifying, racist, sexist, sexually explicit, pornographic, or otherwise offensive or excessively personal.
- Send or receive material which harasses or promotes hatred or discrimination against any person or group of people
- Send or receive material relating to the manufacture, use, sale or purchase of illegal drugs or dangerous materials or to any other illegal activity
- Perform any activity using an anonymous or misleading identity
- Engage in any other illegal or inappropriate activity

IN ADDITION TO THIS

- No student may photograph or film other individuals without their consent
- No student may record a person's voice without their consent

SOCIAL MEDIA

Information boarders provide, and statements they make, on social media sites may impact on them and have significant consequences. Once information is put online, it is part of a permanent online record, even if someone attempts to remove it later.

All boarders are responsible for their words and actions. It is their responsibility to ensure that the posts made online are appropriate. If in doubt, do not post!

Boarders are not permitted to:

- Post photos of staff on social media.
- Post pictures or videos of other students without their explicit permission.
- Use the school's logo/school and boarding house name or create a school branded account for personal use which could be interpreted as representing the school.
- Contribute anything to social media which could bring staff, other students or the school into disrepute- for example, offensive blogs and photos.
- Invite staff members to join your personal social media site.
- Engage in discrimination, harassment or bullying of other students, staff and parents.
- Engage in any conduct that would not be acceptable in school/boarding house- see behaviour ladders.

WATCHING TV- IN BOARDING COMMON AREAS/ ON OWN DEVICES

Boarders are not permitted to:

- Watch any tv programmes/movies that are not their age rating. If unsure, please find a member of boarding staff.
- Listen to any music in the common areas/in boarding rooms that have explicit content**.**

Prep boarders are not permitted to use YouTube, unless supervised by a member of boarding staff (for example, for an activity).

Student Signature: _____

Housemistress Signature: _____

Parent signature: _____

Head of Boarding Signature: _____

Date: _____