LAUS SEMPER JESU ET MARIAE

JM

THORNTON

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 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 Virgin and monitored by Sophos to prevent access to material inappropriate for students;

- 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).
- 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 Network Manager will monitor the effectiveness of Internet access strategies;
- the Network 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 a number of levels. Responsibility for handling incidents involving students will be taken by the Head of IT and Network Manager, in consultation with the 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 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 Network Manager will be informed. The Network Manager will report the URL (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 Network 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 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 Network Manager and IT Technician will up-date virus protection regularly (this is automated), will keep up-to-date with IT news developments and work with the IT Network Service Company to ensure system security strategies to protect the integrity of the network 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 begin to 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-wifi, logging on using their own ID. 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.

Students will be receive e-safety training in Year 7 and regularly 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 (inc 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 on it. In particular, they 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 writer of 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 lockdown scenario.

It is important that communications with persons 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 in our school prospectus 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.

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 found using an electronic device (including text messaging, games or silent ringing) or whose phone rings during the school day will have their equipment confiscated. The device will then be held securely in the school safe and will only be returned on the following Monday to the parent / guardian.

Refusal to hand over a device when reasonably requested to do so by a member of staff will result in behaviour sanctions being implemented.

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

Sixth form and Year 11 - use of personal electronic devices (BYOD)
In the Sixth Form and Year 11, the students 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 wifi' network must be used to sign in; this network is filtered at all times. Any attempt to bypass the network is strictly prohibited and will result in confiscation of the device. All students must follow the acceptable usage instructions as detailed below.

Acceptable Use of Electronic Devices
An electronic device is defined as any personnel device that enables the students to connect with mobile or wifi 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 has to 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-wifi’ wifi network to access the internet to enhance their learning during lessons. They will be required to logon using their normal network id and password.

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 they 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 the 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:

- Sophos Anti-virus protection is in place
- An External Vulnerability Scan is run and any vulnerabilities are addressed where possible.
- Staff permissions in Management Information Systems is appropriate and reviewed regularly.
- Past staff and students accounts are disabled on leaving the college.
- Regular automatically enforced password changes are implemented to all staff each half term.
- Two factor authentication for Office 365 and iSams is in place.
- Updates are actioned promptly across the network to include:
    - Sophos XG Firewall
    - Netscaler
    - Windows patching
    - Veeam
    - Fast Vue
    - Synology
    - Nimble
    - iLO
- Staff are advised to ensure that their passwords are not easily guessable and are kept secure.
- USB sticks are not to be used on the network – One Drive is preferred to prevent virus infection
- All staff have been trained using the following link: – https://youtu.be/pP2VKWSagE0
- Staff ipads are set to six digit pin entry and that the lock screen engages quickly for safety. iPads are not left accessible to students or other staff.
- That you refrain from ticking the box in iSams to ensure that the verification code is saved for 7 days.
- Lock screen on PCs are actioned when staff leave their desks. Staff room PCs are logged out after use.
- Encryption of sensitive business documents are in place.
- Staff are on alert for suspicious phishing emails.
- Cyber attack insurance protection is in place.

All this should be read concurrently with our GDPR Policy.

Visitor ICT & Wi-Fi

Visitors can use the wifi available. A password key will be made available to them. They will be asked to read the Visitor IT & Wifi 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 that 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 1998
- 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

Wi-Fi Access

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

The school currently has a many wireless connections. Staff connect into Thornton wifi; the network logon is to be used.

Monitoring
The school will regularly monitor saved 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 Network 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 using 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 18, as 'friends' on social networking sites such as Facebook or MSN. 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, twitter can be used as a communication tool. The Tweets used MUST be appropriate and not violate the staff conduct policy.

Appendix 1

This sheet is incorporated into the school diary, where it is signed within.

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.

Student’s Name ____________________________ Form ________________
(please print)

Student’s Signature _____________________________ Date ________________

Parent’s Signature _____________________________ Date ________________

Appendix 2

Visitor IT & Wi-Fi Protocol

Thornton College's IT network has been set up to ensure with 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 called 'Sophos' 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 thornton-guest which will be given a wireless key 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 Sophos 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.

As a visiting user of the Internet, I agree to conditions laid out above and understand what is expected.