

HOLY TRINITY COLLEGE



E-SAFETY AND ACCEPTABLE USE OF INTERNET POLICY

College Mission Statement

“Holy Trinity College is a Catholic Maintained school committed to high quality educational opportunities for each pupil to develop his/her unique talents to the full in a secure, caring environment”

Promoting: Inspiration, Innovation, Excellence



(Revised: September 2019)

1. Introduction:

1.1] In April 2012, all schools received access to a core set of technologies to assist and enhance teaching and learning for the benefit of staff and pupils. Along with increased broadband, a major enhancement in the new services, lies in the ability to accommodate the connection of a range of third-party access devices into the school network. This will allow the school to plan for, and exploit, circumstances where pupils might make use of their own devices to connect to the service anytime, anywhere. Schools will also have the option of opening up to pupils, social media sites they consider contribute to improved teaching and learning. These service improvements bring along with them challenges for schools in relation to their statutory responsibility for ensuring the welfare and safety of both staff and pupils.

Holy Trinity College is currently operating under the guidelines of the 360 Degree Safe Audit and are working towards achieving this recognised online internet safety mark.

2. What is E-Safety?

2.1] e-Safety is short for electronic safety.

2.2] It is the responsibility of all Staff, Parents / Guardians, and Board of Governors to mitigate risk through reasonable planning and actions. E-Safety covers not only Internet Technologies but also electronic communications via mobile phones, games consoles and wireless technology. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail and Instant Messaging
- Chat Rooms and Social Networking Sites
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

2.3] E-Safety in the school context:

- is concerned with safeguarding children and young people in the digital world;
- emphasises learning to understand and use new technologies in a positive way;

- focuses on educating all users about the risks as well as the benefits to enable users to feel confident online;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school; and
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

2.4] The rapidly changing nature of the Internet and new technologies means that E-Safety is an ever growing and changing area of interest and concern. The Holy Trinity College E-Safety Policy must reflect this by keeping abreast of the changes taking place. We have a duty of care to enable pupils and staff to use on-line systems in a safe manner.

2.5] Holy Trinity College E-Safety Policy operates in conjunction with other school policies including Positive Behaviour, Child Protection, Code of Conduct, Anti-Bullying and Acceptable Use of the Internet Policies. As ICT and on-line resources are increasingly used across the curriculum, E-safety must therefore be embedded within our curriculum and we should continually look for new opportunities to promote E-safety. Guidance however should be given to all staff on a regular and meaningful basis.

2.6] Whilst the Internet is composed of information from a vast array of sources worldwide, it includes some material that is not of educational value in the context of the school. This material includes information that may be inaccurate, abusive, profane, sexually oriented, racist or illegal. In order to guard young people from an inherent danger, it is the joint responsibility of all College staff and the parent / guardian of each pupil to educate the pupil about his or her responsibility when using the Internet.

3. Internet Safety Legislation

Sexual Offences Act 2003

Safeguarding Board Bill (being proposed)

The Byron Review 2008

Click Clever Click Safe: The First UK Child Internet Safety Strategy 2009

The Education and Libraries (NI) Order 2003

Protection from Harassment (NI) Order 1997

Malicious Communications (NI) Order 1988

The Communications Act 2003

4. Internet Terminology

Social Networking - this term covers all internet sites that are used to talk to other people, exchange pictures etc. Examples used include: Facebook, Twitter, LinkedIn, Whatsapp, Viber, Flickr, Google+. Pupils have no access to these sites through the school's internet provider (C2K) and are advised to 'think before they post'. Pupils are also informed of the consequences of inappropriate/unacceptable uses of these sites through their mobile phones.

Cyber-bullying - this form of bullying is done through the internet/mobile phone devices etc. This can take the form of nasty unwanted/hurtful comments, racial abuse, trolling, sexting etc.. If you are experiencing on-line bullying use the button, report the incident to parent/teacher or phone the Bullying UK helpline on 0808 800 2222



Data Protection - The Data Protection Act 1988 defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. There are 8 principles that schools must adhere to when dealing with information on staff and pupils. (See Parent Information Leaflet)

Freedom of Information - The Freedom of Information Act 2000 aims to promote a culture of openness and accountability amongst public sector bodies and to improve public understanding of how duties are carried out. Schools are obliged to provide information at parental request.

Passwords -

Filtering - a robust filtering system is in operation which is controlled and monitored by our C2K system.

5. Monitoring

All internet activity is logged by the school's internet provider (C2K). These logs are regularly checked. Logs may also be monitored by the ICT Co-ordinator / Technician, Head of School and the College Principal.

Holy Trinity College now operate Securus, through C2K, where 9 individual areas of internet safety are monitored by the Principal and Vice-Principals on a daily basis. Meetings are held with pupils who have been identified by this system and contact is made with a parent/guardian should the need arise.

6. Breaches

A breach or suspected breach of Policy by a school employee or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach by staff is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, by the Education Authority (EA)/ Catholic Council for Maintained Schools (CCMS)

Policy breaches may also lead to criminal or civil proceedings.

7. Incident Reporting

Any security breaches or attempts and any unauthorised use or suspected misuse of

Illegal Content

Means something against the law

such as:-

- Downloading child sexual abuse images
- Passing onto others images/video containing child sexual abuse
- Inciting racial or religious hatred
- Extreme cases of cyber bullying
- Promoting illegal acts

Inappropriate Content

Examples include:

- Using another person's user name/password
- Accessing websites which are against school policy
- Using a mobile phone to take a video during lessons
- Using the technology to upset/bully

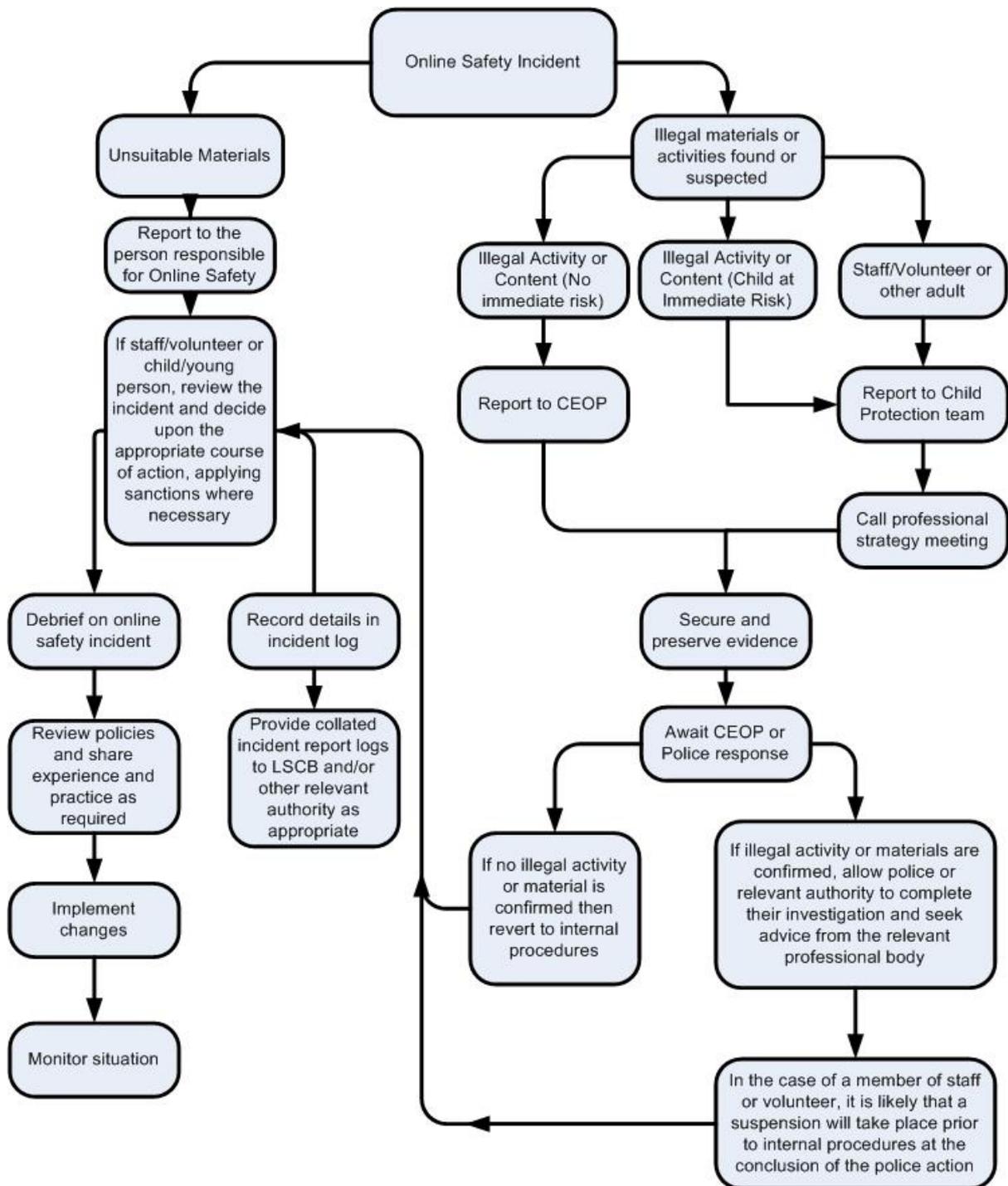
ICT must be immediately reported.

Additionally, all lost or stolen equipment or data, virus notifications, unsolicited e-mails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the College Principal.

A Reporting Log (**See Appendix 1**) will be completed and the incident recorded.

{See flow chart on next page}

Responding to incidents of misuse - flow chart



- Inform PSNI
- Confiscate laptop/device
- Disable user account
- DO NOT view or copy, hand over as evidence



Flowchart relating to an inappropriate e-safety incident

The safeguarding/e-safety coordinator and/or Principal should:

Record in the school safeguarding or e-safety incident log and keep any evidence

If member of staff has:

- Behaved in a way that has, or may have harmed a child,
- Possibly committed a criminal offence,
- Behaved towards a child in a way which indicates s/he is unsuitable to work with children.

Contact PSNI immediately on 101

Review evidence and determine if the incident is accidental or deliberate.

Decide upon the appropriate course of action.

Follow school disciplinary procedures (if deliberate) and contact the Principal.

If the Principal is involved contact the **Chair of Governors**.

Yes

Did the incident involve a member of staff?

Incident could be:

- Using another person's user name and password,
- Accessing websites which are against school policy e.g. games,
- Using a mobile phone to take video during a lesson,
- Using the technology to upset or bully (in extreme cases could be illegal).

No

Pupil as victim

Was the pupil the victim or the instigator?

Pupil as instigator

- Review incident and identify if other pupils were involved.
- Decide appropriate sanctions based on school rules/guidelines.
- Inform parents/carers if serious or persistent incident.
- In serious incidents consider informing the school **Child Protection Officer** as the child instigator could be at risk.
- Review school procedures/policies to develop best practice.

Users must know to switch off their monitor, or close laptop if they find something unpleasant or frightening and then talk to a member of staff and/or the e-safety co-ordinator.

8. Safe and Acceptable Use of the Internet

1.1] Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management, information and business administration systems.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is a privilege and not a right
- Pupils should show a responsible and mature approach to its use.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

1.2] How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils world-wide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Improved communication between pupils and staff
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with DENI, CCMS, SELB and other relevant external agencies ;
- Access to learning wherever and whenever convenient.

1.3] The Internet can enhance learning in the following ways:

- Holy Trinity College Internet access will be designed expressly for pupil use and will be accessed via two different sources
 - a) a filtered Internet service and a filtered e-mail service through C2K
 - b) a filtered wireless (wi-fi) internet access via - staff access only
- During school hours, teachers will guide pupils towards appropriate materials.
- Pupils will always be supervised by a member of staff while using ICT facilities. However, it is at all times the pupil's responsibility to ensure that only appropriate material is accessed.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Staff will guide pupils in on-line activities that will support the learning outcomes of assigned lessons.

1.4] Staff and pupils at Holy Trinity College **know and understand** that no Internet user is permitted to: **

- retrieve, send, copy or display offensive messages or pictures;
- use obscene or racist language;
- harass, insult or attack others;
- damage computers, computer systems or computer networks;
- damage any ICT equipment;
- violate copyright laws;
- use another user's password;
- trespass in another user's folders, work or files;
- intentionally waste resources (such as on-line time and consumables);
- use the network for unapproved commercial purposes;
- bring any indecent/obscene/offensive messages or images into school via USB drives, mobile phones, email attachments etc;
- purposefully attempt to bypass security measures /firewalls etc;
- place coursework / school work on social networking sites;
- upload images from a mobile phone / other device to school folders

**this list is not exhaustive.

1.5] Access to the Internet requires parental permission and a signed Acceptable Use Agreement signed by parents and pupils agreeing to the school rules for use of the Internet. **(See Appendix 2)**

1.6] Holy Trinity College will ensure that all pupils understand how they are to use the Internet appropriately and why the rules exist. This will be done during individual ICT lessons by the class teacher.

1.7] When using ICT, all users must comply with all copyright, libel, fraud, discrimination and obscenity laws or other statutory obligations.

1.8] Pupils are responsible for good behaviour on the Internet/VLE/Email just as they are in the classroom or a school corridor. Daily school rules and procedures apply at all times. This behaviour also applies to the use of Internet through mobile phones/iPads/Tablets etc..

1.9] The responsibility for monitoring the use of digital media and access to the internet at home lies with those with parental responsibility. Holy Trinity College will work constructively with parents/guardians to ensure that best practice is followed at all times.

2] Examples of Acceptable and Unacceptable Use

2.1] In Holy Trinity College, on-line activities which are encouraged include, for example:

- the use of email and computer conferencing for communication between colleagues, between pupil(s) and teacher(s), between pupil(s) and pupil(s), between schools and industry;
- use of the Internet to investigate and research school subjects, cross-curricular themes and topics related to social and personal development;
- use of the Internet to investigate Careers and Further and Higher education;
- the development of pupils' competence in ICT skills and their general research skills.

2.2] In Holy Trinity College, on-line activities which are not permitted include, for example:

- uploading, downloading images of members of the school community (this refers to all staff, pupils, names)
- searching, uploading, viewing and/or retrieving materials that are not related to the aims of the curriculum or future careers;
- copying, saving and/or redistributing copyright protected material, without approval;
- subscribing to any services or ordering any goods or services, unless specifically approved by the school;
- playing computer games or using other interactive 'chat' sites, unless specifically assigned by the teacher;
- using the network in such a way that use of the network by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages);
- publishing, sharing or distributing any personal information about a user (such as: home address; email address; phone number, etc.);
- any activity that violates a school rule.

9. Sanctions for Unacceptable use of the Internet

On occasions, where students have been deemed as abusing their privileges of using the internet the matter will be dealt with immediately and sanctions put in place to address the matter. They may be:-

- a student is immediately denied access to the internet/the use of a computer;
- parent/guardian will be informed and a meeting arranged to discuss the matter;
- a student could be suspended for a minimum of 5 days to a maximum of 45 days, depending on the severity/nature of the offence;
- a student and his/her parent/guardian could be asked to attend a meeting with a sub-committee of the board of Governors.

A list of further sanctions has been compiled for pupils to ensure the Internet is used in the most appropriate manner. (See Appendix 3)

Any breaches of internet safety or unacceptable uses of the internet by a member of staff will be reported to the Principal and the matter dealt with immediately.

10. Support, Education and Advice on Using the Internet

STAFF - All staff receive appropriate online safety training and regular online safety information. Staff can recognise and are aware of online safety risks and know the protocol for reporting breaches or other internet concerns. The Director of ICT along with the Designated Teacher for Safeguarding have a higher level of expertise around online safety and inform staff regularly on issues pertaining to safe internet use.

PUPILS – Pupils and staff at Holy Trinity College are informed of different websites that can provide support and advice when using the Internet appropriately. The school website features a list similar to that below:-

- www.bbc.co.uk (Stay Safe)
- www.childline.org.uk
- www.iwf.org.uk
- www.thinkuknow.co.uk
- www.ceop.gov.uk
- www.cybermentors.org.uk
- * www.kidscape.org.uk
- * www.niabf.org.uk
- * connectsafely.org. uk

Staff and pupils have engaged in 2 drama productions regarding Internet Safety through C2K competitions. These have been viewed by staff and pupils and are uploaded onto the College's website.

Pupils receive age-appropriate online safety messages that are relevant and engaging. Holy Trinity College actively promotes online safety messages for pupils on how to stay safe; how to protect themselves online; and how to take responsibility for their own and others' safety.

Online safety is actively promoted with Holy Trinity College through PD/ICT curriculum, year group assemblies, talk and seminars given by external agencies eg. PSNI, NEXUS etc.. Each week the College has an e-Safety Focus which is reinforced at assembly and registration daily. The College also takes part in events such as Safer Internet Day and competitions organised by EA/C2K (as previously mentioned).

PARENTS - the College makes parents and carers aware of important online safety messages through our website and facebook account. Online safety resources are shared with parents through this medium and information talks by outside agencies are also held.

Appendices



INTERNET ACCEPTABLE USE POLICY

**Internet Use Agreement for pupils at Holy Trinity College
September 2019/2020**

Please read this document carefully before signing

1. Introduction

Internet access is available to pupils and teachers in Holy Trinity College. We are pleased to bring this access to all pupils and believe the Internet offers vast, diverse and unique resources to both pupils and teachers. Our aim in providing this service is to promote educational excellence by facilitating resource sharing, innovation and communication.

2. What is the Internet?

The Internet is an electronic highway connecting thousands of computers across the world and millions of individual subscribers. With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the school setting. However, we believe that the valuable information and interaction available on this worldwide network far outweigh the possibility that users may obtain material that is not consistent with our educational aims.

3. Terms and Conditions

Users within Holy Trinity College must adhere to strict guidelines. These guidelines are provided so that you are aware of the responsibilities you are about to acquire. In general, this requires efficient, ethical and legal use of Internet resources. If an individual user violates any of these provisions, future access could be denied. Violations of this agreement will be referred to appropriate school officials for disciplinary action. Violations of UK law will be referred to the appropriate authorities. The signatures at the end of this document are legally binding and indicate that the parties who signed have read the terms and conditions carefully and understand their significance.

Parents: It is important that you and your child read this agreement and discuss it together. When your child is given a login ID and is allowed to use the computers, it is extremely important that the rules are followed. As a parent, you are legally responsible for your child's actions. You are responsible for supervision of your child's Internet use when not in a school setting.

A. Acceptable Use

The use of the School's account must be in support of education and research and consistent with the educational aims of Holy Trinity College. Transmission of any material in violation of any legal regulations is prohibited; this includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by a trade secret.

B. Privileges

The use of the Internet is a privilege, not a right, and inappropriate use will result in the cancellation of those privileges. Staff will deem what is inappropriate use and their decision will be final. *The school reserves the right to monitor and filter all files and/or e-mail to determine whether the facility is being used in a manner that is consistent with this agreement.* The ICT Co-ordinator may prohibit or terminate any pupil's use of the Internet at any time as required. The

revoking of Internet access will only result after consultation with the School Principal. Pupils accessing the Internet within Holy Trinity College must consent to such monitoring.

C. Responsibilities

You are expected to abide by the generally accepted rules of Internet use, which include (but are not limited to) the following:

- Do not use the Internet for any illegal activity (e.g. violating copyright or other contracts, gaining illegal access or entry into other computers);
- Do not use Internet for financial or commercial gain;
- Do not use your account in such a way that you would disrupt the use of the facilities by other users;
- Do not use this facility in a wasteful or frivolous manner (e.g. tying up resources with computer-based game playing, sending trivial or excessive messages, downloading excessively large files);
- Do not reveal your personal address/phone number or the personal address/phone number of a colleague;
- Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user or the Internet; this includes, but is not limited to, the uploading or creation of computer viruses;
- Respect the privacy of other individuals;
- Files/data belonging to others are to be considered private property unless explicit authorisation is given by the owner of the files;
- *Be polite. Do not be abusive in your mail messages to others. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.*

Holy Trinity College makes no warranties of any kind, whether expressed or implied, for the service that is provided and will not be responsible for any damages suffered; this includes loss of data resulting from delays or service interruptions caused by any negligence, errors or omissions. Use of any information obtained via the Internet is at your own risk. No guarantee of complete privacy is made.

4. Agreement to Comply

User: I understand and will abide by the Holy Trinity College Internet Use Agreement. I further understand that any violation of the regulations above is unethical and may constitute a criminal offence. Should I commit any violation, (1) my access privileges may be revoked and (2) school disciplinary action and/or appropriate legal action may be taken.

I understand and accept that:

- Use of the School's Internet account is a privilege, not a right;
- The Internet is to be used for educational and research purposes only, consistent with the educational aims of the School. Misuse will result in loss of the account;
- Staff may monitor pupil use of the Internet, including e-mail, to determine that use is for the stated purposes. For this and other reasons, e-mail is not private. Violations that may lead to revocation of

Internet access includes:

- playing computer-based games;
- downloading excessively large files;
- sharing password with anyone besides ICT Staff;
- subscribing to inappropriate newsgroups;
- E-mail correspondence inappropriate to educational purposes;
- any activity posing potential risks to myself or others;
- harassing other users (e.g. with unwanted e-mail messages);

- illegal activity;
- revealing my or another's home address/phone number;
- vandalism of accounts or systems;
- using abusive, vulgar, or other inappropriate language;
- failure to report known security problems;
- Using the Internet through a mobile phone device in an inappropriate manner eg. social media sites eg. Facebook, Twitter etc...
- any other inappropriate use or misuse of the facility.

Staff will deem what is inappropriate use, and their decision is final. Accounts are monitored and use of the account implies agreement to such monitoring. The Director of ICT may close an account at any time for violations.

Please complete the section below and return it to the school as soon as possible, pupils **will not** be allowed Internet access until this document has been signed and returned.

I understand and accept the conditions herein.

Pupil's Name _____ **Parent's Name** _____

Signature _____ **Signature** _____

Date _____



Pupil Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / Head of School	Refer to Principal/DT for Child	Refer to PSNI	Refer to ICT Technician for action re filtering / security etc	Inform parents/guardians	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion/Board of Governors
Deliberately accessing or trying to access material that could be considered illegal		X	X	X	X	X	x		
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised use of mobile phone / digital camera / other mobile device	X		x					X	
Unauthorised use of social media / messaging apps / personal email			X					X	
Unauthorised downloading or uploading of files					X				
Allowing others to access school network by sharing username and passwords	X							X	
Attempting to access or accessing the school network, using another pupil's account	X							X	
Attempting to access or accessing the school network, using the account of a member of staff			X						X
Corrupting or destroying the data of other users			X			X		X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X			X	X		
Continued infringements of the above, following previous warnings or sanctions			X						X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X						X
Using proxy sites or other means to subvert the school's filtering system			X						X
Accidentally accessing offensive or pornographic material and failing to report the incident			X		X		X		
Deliberately accessing or trying to access offensive or pornographic material			X	X			X		x

E-SAFETY AND ACCEPTABLE USE OF INTERNET POLICY

Signed(Chairman of Board of Governors)

Signed(Principal)

Date

Next Review Date: September 2020