Online Safety Policy

Created:	October 2023
Approved by Governors:	October 2023
Next Review:	October 2024

Contents

1. Vision

Loreto College is centred in God, rooted in Christ and animated by the spirit of Mary Ward, the founder of the Institute of the Blessed Virgin Mary. Our vision is that it will be an educational community where each person has the experience of being loved and valued as a sacred individual created by a loving God; a community where students enjoy an enriching and liberating education that helps them grow into the fullness of life and empowers them to be men and women of courage who are alive to the needs of humanity and committed to making a better world.

2. Introduction

The College aims to be an educational community which gives expression to the core values of Mary Ward - freedom, justice, sincerity, truth, joy, excellence and internationality.

This policy covers issues relating to children and young people as well as adults and their safe use of the Internet, computers, smart phones, and other electronic communications technologies, both in and out of College. It provides advice for all members of the College community on risks and responsibilities and is part of the 'duty of care', which applies to everyone working with young people.

3. Preamble

The College is an educational community, which gives expression to the core values of Mary Ward - freedom, justice, sincerity, truth, joy, excellence and internationality. Loreto College has the highest expectations of

personal, academic and professional excellence. This document sets out the College's policy and guidance on the procedures it will follow in relation to Online Safety. This policy applies to all members of the Loreto College community (including staff, students, governors, volunteers, parents/carers, visitors, community users) who have access to and are users of the College's ICT systems, both in and out of the College. In doing so, the College will be mindful of its Mission, core values and its duty of care to all its staff and students and the legal responsibilities associated with this. The College will endeavour to act at all times with justice, compassion and respect for the dignity and worth of each member of the college community.

4. Aims

Loreto College aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole college community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Enable staff to work safely and responsibly, to role model positive behaviour online and to be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the college community.
- The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
    - **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
    - **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
    - **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
    - **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

5. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education 2023

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

This policy should be read in conjunction with other relevant college policies including (but not limited to):

- Anti-Bullying Policy
- Guidance for Safer Working Practice Attendance Procedures
- Code of Respect
- Student Behaviour Policy
- Prevent Policy
- Student ICT User Agreement
- Staff & Governors ICT User Agreement
- Safeguarding and Child Protection Policy

- Bring Your Own Device (BYOD) Agreement

6. Responsibilities of the College community

6.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The governing board will receive regular reports regarding safeguarding, to include online safety, provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Sr Patricia.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the college's Staff and Governors ICT User Agreement
- Ensure that online safety is a running and integrated theme in whole college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable young people, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all young people in all situations, and a more personalised or contextualised approach may often be more suitable.

6.2 The Principal and Senior Leadership team

The Principal and SLT are responsible:

- for ensuring that staff understand this policy, and that it is being implemented consistently throughout the college.
- for supporting the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- for ensuring there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.

6.3 The Designated Safeguarding Lead

Loreto College's DSL (Designated Safeguarding Lead) has overall responsibility for Online Safety. Loreto College's DSL is Andrea Pritchard.

Details of the College's designated safeguarding lead (DSL) deputies are set out in Loreto's Safeguarding and Child Protection policy as well as relevant job descriptions.

Working with the Network Manager, the Head of Information Systems and Safeguarding Manager, the DSL takes lead responsibility for online safety, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the college
- Working with the Principal, Network Manager, Head of Information Systems, Safeguarding Manager and other safeguarding staff as necessary, to address any online safety issues or incidents.
- Be an active member of the Online Safety Team, alongside the Network Manager, Head of Information Systems and Safeguarding Manager.
- Managing all online safety issues and incidents in line with the college's Safeguarding and Child Protection policy

- Ensuring that any online safety incidents are recorded on the student's Safeguarding Log and dealt with appropriately in line with this policy and the Safeguarding and Child Protection Policy
- Ensuring that any incidents of cyber-bullying are recorded on the student's Safeguarding Log and dealt with appropriately in line with the Student Behaviour policy and the Safeguarding and Child Protection Policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on safeguarding, including online safety, to the Principal and Governing Body.

6.4 The Network Manager and Head of Information Systems

The Network Manager and Head of Information Systems are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at college, including terrorist and extremist material
- Providing technical support and perspective to the DSL and Senior Leadership Group, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the college's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Monitor and react to security alerts from external and internal security services
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

6.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the Staff and Governors ICT User Agreement and ensuring that students follow the terms of acceptable use in the Student ICT User Agreement
- Working with the DSL to ensure that any online safety incidents are logged on the Safeguarding Log and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the college Student Behaviour Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.

This list is not intended to be exhaustive.

6.5 Students

Students are expected to:

- Read and adhere to the Student ICT User Agreement and Bring Your Own Device (BYOD) Agreement

- Respect the feelings and rights of others both on and offline.
- Seek help from a trusted adult if things go wrong, and support others that may be experiencing online safety issues.
- Take responsibility for keeping themselves and others safe online.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

6.7 Parents and Carers

Parents/carers are expected to:

- Support Loreto's online safety approaches by discussing online safety issues with their son/daughter and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate uses of new and emerging technology.
- To identify changes in behaviour that could indicate that their son/daughter is at risk of harm online.
- Seek help and support from Loreto, or other appropriate agencies, if they or their son/daughter encounters online problems or concerns.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Report any known issues as soon as possible.
- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their son/daughter has read, understood and agreed to the terms of acceptable use in the Student ICT User Agreement and Bring Your Own Device (BYOD) Agreement

Parents/ carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent / carer resource sheet – Childnet International

6.7 Visitors and members of the community

Visitors and members of the community who use the college's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

7. Educating students about online safety

Students will be taught about online safety as part of the curriculum via the Assembly, Tutorial and RE programmes. Topics will include:

- MyLoreto and e-learning
- Keeping Safe: Relationships and Consent
- Mental Health: It's ok not to be ok
- Mental Health: Staying healthy physically and mentally
- PREVENT week
- Self Esteem
- Keeping Safe: Crime and Exploitation
- Gambling, Debt and Finance

- Coming of Age
- Online Safety
- Keeping Safe: CCE

This list is not intended to be exhaustive.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

8. Educating parents/ carers about online safety

The College will raise parents'/ carers' awareness of internet safety in newsletters, the Parents/ Carers Welcome Conference, Parent Portal and in information via our website This policy will also be made available to parents/ carers via the Parent Portal.

The College will let parents/carers know:

- The college uses systems to filter and monitor online and offline ICT use on the college network and devices
- That throughout the academic year staff are likely to ask their son/daughter to go online to access teaching resources, research topics, complete homework etc.
- All staff on their son/daughter's timetable may interact with them online (i.e. organised webinars, remote lessons), as part of their programme of study.
- Details of their son/daughter's teaching staff are on their timetable, which is available for parents/ carers to check on the Parent Portal and is subject to change.

If parents/ carers have any queries or concerns in relation to online safety, these should be raised in the first instance with their son/daughter's Head of Hall.

Concerns or queries about this policy can be raised with a Head of Hall or any member of the college Senior Management Team.

9. Cyber-bullying

9.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Anti-Bullying policy.)

9.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The college will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be, as part of the tutorial programme.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The college also provides resources on the college website and parent portal to parents/ carers so that they are aware of the signs, how to report it and how they can support their son/daughter if they have been affected.

In relation to a specific incident of cyber-bullying, the college will follow the processes set out in the Student Behaviour and Safeguarding and Child Protection policies. Where illegal, inappropriate or harmful material has been spread among students, the college will use all reasonable endeavours to ensure the incident is contained.

The DSL (A. Pritchard) will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

9.3 Examining electronic devices

The Principal, and any member of staff authorised to do so by the Principal can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in college policies as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the college or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Principal/ other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent/ carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Student Behaviour Policy

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the college complaints procedure.

10. Technology

Loreto College uses a range of software and hardware. In order to safeguard staff and students, and in order to prevent loss of data we employ the following technologies:

- Internet Filtering –unauthorised or inappropriate access to illegal websites is controlled via web filtering. The web filtering is reviewed annually by the Online Safety Team, or in response to an incident, whichever is sooner. The DSL, Head of Information Systems and Network Manager are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Principal.
- Loreto recognises that many students have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means it is not possible to prevent via technology the possibility that some students, whilst at college, may sexually harass their peers via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content.
- Device Monitoring – all college owned computers including laptops have device monitoring software installed which alerts an external team of trained Safeguarding professionals to potential safeguarding issues. This enables the monitoring of college computer usage both on premises and remotely.
- The college uses additional technologies to generate safeguarding alerts to the safeguarding team.
- Email filtering – all emails are analysed by third party security features to protect end users from malware, phishing and spam.
- Anti-virus – All capable devices have anti-virus installed. This software is updated automatically for new virus definitions.
- Passwords – all College systems and devices require a unique username and password. Password requirements follow industry best practice. Passwords must be changed following compromise.
- Multi-factor authentication – this is required for staff and student access to college systems outside of college premises.

11. Acceptable use of the internet in college

All students, staff, volunteers and governors are expected to sign the appropriate ICT user agreement regarding the acceptable use of the college's ICT systems and the internet as defined in the Student ICT User Agreement and the Staff and Governors ICT User Agreement. Visitors will be expected to read and agree to the college's terms on acceptable use if relevant.

Use of the college's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

12. Students using mobile devices in college

Students may bring mobile devices into college, but should not use them, unless requested to do so by a member of staff, during:

- Lessons
- Tutor group time
- Assemblies

Any use of mobile devices in college by students must be in line with the Bring Your Own Device (BYOD) Policy.

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the Student Behaviour Policy.

13. Staff using personal devices to access college systems

All staff members will take appropriate steps to ensure their devices remain secure. Staff must enrol their device via the college portal – only devices meeting the security compliance criteria will be able to access college systems.

If staff have any concerns over the security of their device, they must seek advice from the Network manager.

14. How the College will respond to issues of misuse

Where a student misuses the college's ICT systems or internet, we will follow the procedures set out in Student Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the College's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff Disciplinary Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The college will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

15. Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer).

Cyber-dependent crimes include;

- unauthorised access to computers (illegal 'hacking'), for example accessing the College's computer network to look for test paper answers or change grades awarded;
- denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Students with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a student in this area, the designated safeguarding lead (or a deputy), should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

16. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through safeguarding pop-ups on myLoreto).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that students are at risk of online abuse
- Students can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and Child Protection Policy.

17. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the DSL and Head of Information Systems. At every review, the policy will be shared with the governing board.

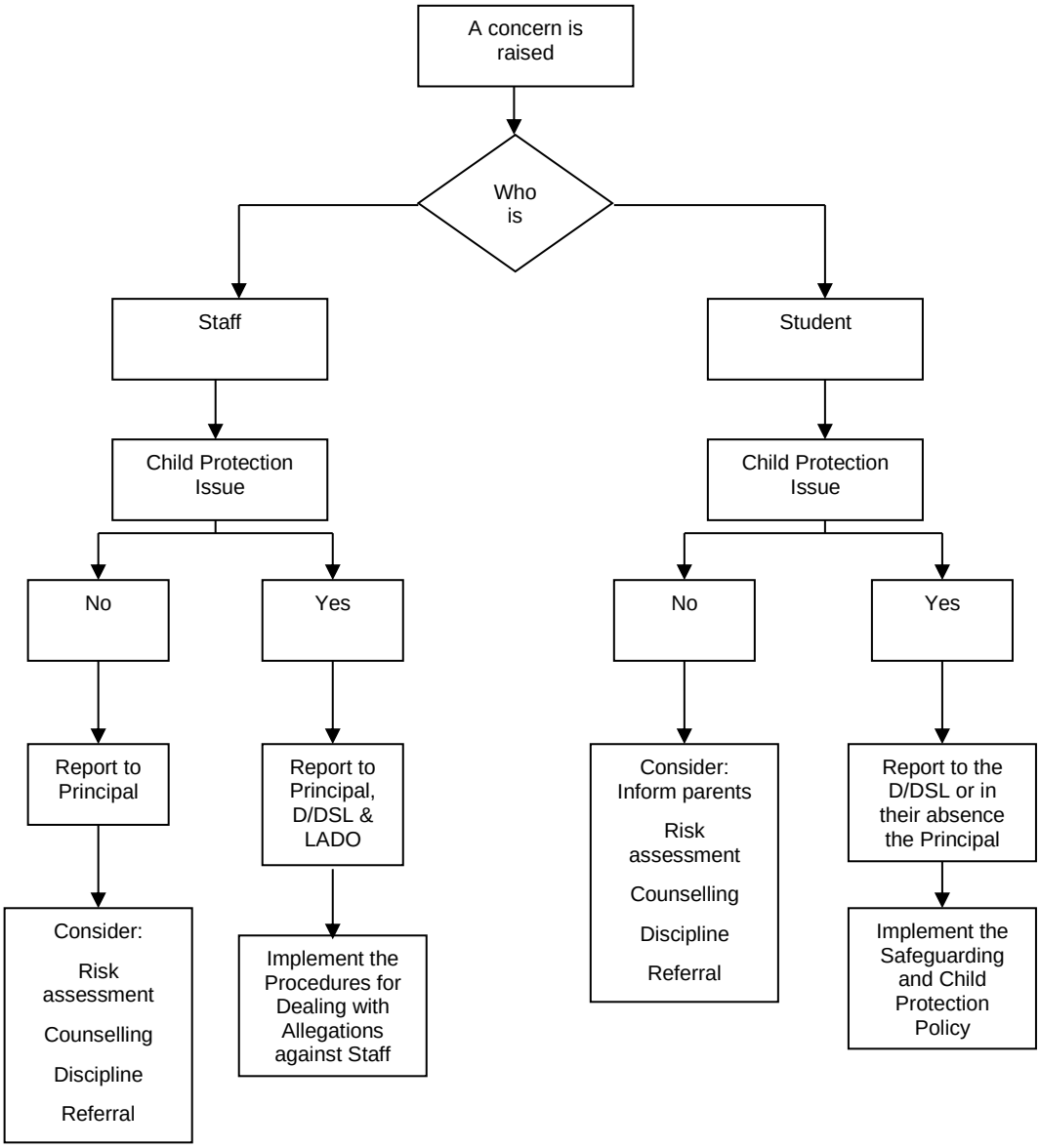
18. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection policy
- Student Behaviour policy
- Staff disciplinary policy
- Data protection policy and privacy notices
- Complaints procedure
- Social Media Policy
- Staff and Governors ICT User Agreement

- Student ICT User Agreement
- Bring Your Own Device (BYOD) Agreement
- Information Security Policy

Appendix 1 Inappropriate Activity Flowchart



Appendix 2 Illegal Activity Flowchart