7f E-Safety Policy

Mission Statement

We are an all-through, inclusive Catholic girls' school, with boys in the Nursery, committed to preparing girls for life long effectiveness and success. As part of their journey girls will learn of intellectual risk taking and emotional strength, reflection and self-knowledge, persuasiveness and team building as well as a cultural curiosity for an enriched enjoyment of life.

In our stunning 13 acres of grounds, girls have a physical freedom unique in central London. We aim to instil in them the emotional freedom to grow intellectually and spiritually and to understand the truth about themselves, others and our complex world. We will give them the courage to be ambitious and compassionate and we will provide a secure, happy and nurturing community in which to explore all of the above.

To this end we seek, develop and retain the best teachers who value well-being and the individual progress of each girl as much as they are relentless in their pursuit of academic excellence. Their goal is life-long success for each girl and they set the pace of energy and dynamism within which the girls flourish.

Introduction

E-Safety encompasses any use of a digital device and/or wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The school's E-Safety policy will operate in conjunction with other policies including those for Anti-Bullying, Teaching and Learning, Data Protection, Safeguarding and Child Protection and the Staff Code of Conduct and Acceptable Use Policy (AUP).

E-Safety is a priority at St Augustine's Priory. While we actively embrace all of the benefits of the internet, we are equally vigorous in embedding safe working practices amongst the whole school community.

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of E-Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of content filtering.
- Regular and effective training for staff

School E-Safety Policy

The school has appointed an E-Safety coordinator; this is the Head of ICT who works in conjunction with the Deputy Head (Seniors). The Designated Safeguarding Leads are Mrs M-H Collins); for Juniors Mrs K Knowles and Preps and Pre-Preps Miss L Keane.

Cyberbullying

Cyberbullying is bullying which occurs though media and communication devices: these include mobile phones, and tablets. As a school, we will not tolerate cyberbullying and take all allegations seriously. We will invoke our Anti-Bullying Policy to deal with each case individually. Those found to be bullying will be interviewed and receive appropriate sanctions and guidance. Other staff members and parents will be informed as appropriate.

It includes the sharing of illegal material; the sharing of images of children and young people of an explicit nature; the sending of malicious communications to another person.

Sexting/Youth Produced Sexual Imagery

Sexting is when someone shares sexual, naked or semi-naked images of themselves or others, or sends sexually explicit messages. They can be sent using mobiles, tablets, smartphones, laptops – any device that allows you to share media and messages. Sexting may also be called:

- Trading nudes
- Dirties
- Pic for pic

Sexting can be seen as harmless by young people but creating or sharing explicit images of a child or young person is illegal, even if the person doing it is a child. A young person is breaking the law if they:

- Take an explicit photo or video of themselves or a friend
- Share an explicit image or video of a child, even if it is shared between children or young people of the same age
- Possess, download or store an explicit or video of a child, even if the child or young person gave their permission for it to be created

In the most recent guidance produced by the UK Council for Child Internet Safety, Sexting in Schools and Colleges Resource Pack, sexting is referred to as "youth produced sexual imagery", although KCSIE (September 2016) still refers to "sexting".

Peer on Peer Abuse

Peer on peer abuse can manifest itself in many ways and can include, but is not limited to, bullying, cyberbullying, sexting, gender based violence and sexual abuse. It often manifests itself through the use of mobile devices and the internet. Peer on peer abuse is not tolerated at St. Augustine's Priory and it should not be passed off as "banter" or "part of growing up". In the case of peer on peer abuse, our Safeguarding Policy and Anti-Bullying Policy should be invoked. Our Safeguarding Policy and this E-Safety Policy set out the procedures taken by the school to minimise the risk of peer on peer abuse, and the Safeguarding Policy clearly states how allegations of peer on peer abuse will be investigated and dealt with.

Why is internet use important?

The purpose of internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Our school has a duty to provide pupils with quality internet access when deemed necessary for educational purposes.
Pupils will use the internet outside school and will need to learn how to evaluate internet information and to take care of their own safety and security.

How does internet use benefit education?

- The school internet access is designed expressly for student and staff use and includes filtering appropriate to the age of pupils
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use through E-Safety lessons delivered by Mr Dellow, Head of ICT, through PSHEE
- Internet access will be planned to enrich and extend learning activities
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- Parents are offered an E-Safety Workshop annually in the Autumn Term
- There is guidance in school planners for pupils

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted internet access only via AUP signatures.
- All staff and pupils must read and sign the 'Acceptable Use Policy' before using any school ICT resource.
- All staff are required to read and sign the staff code of conduct.
- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the E-Safety coordinator or network manager.
- School will inform staff and pupils about using internet derived materials in compliance with copyright law.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. There is guidance in school planners for pupils.

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive emails or messages of any kind, or explicit sexual material involving a minor.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Prevent

In line with our commitment to minimise the risk of students being radicalised, pupils' use of school computers is monitored by an external forensic monitoring services (E-Safe Compliance) and pupils found searching websites or using search criteria that would suggest an interest in terrorism/radicalisation are immediately flagged up and investigated by the Designated Safeguarding Lead for the Senior School, who follows the school's Procedures for Safeguarding Children as outlined in our Safeguarding Policy.

Social Networking

- St Augustine's Priory will filter access to social networking sites unless a specific use is approved. The E-Safety coordinator can discuss this further.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils will be advised not to place personal photos on any social network space without due regard to privacy settings.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others.
- Pupils will be advised how to report abuse.
- Staff are trained to be aware of online grooming of all kinds and pupils are trained to be aware of these risks also, in Personal Social Emotional Development, Personal Social Health, Assemblies and so on.

Filtering and Monitoring

The school will work in partnership with all stakeholders and use the latest government guidance to ensure filtering systems are as effective as possible. Pupils are blocked from accessing social media sites on school computers. The school uses a highly effective monitoring system which reports any suspected alerts to the Headteacher. The Headteacher addresses concerns raised about staff and the DSL (Seniors) addresses concerns abut pupils.

Video Conferencing

- Pupils should ask permission from the supervising teacher before making or answering a video conference call, or using equivalent services such as Facetime.
- Video conferencing will be supervised for pupils by a member of staff, and only through school accounts.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used for personal use during lessons or formal school time. Sixth Form pupils may use their mobile phones within the Sixth Form Common Room at lunchtime only.
- The sending of abusive or inappropriate messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required, e.g. when taking school trips.
- Where the use of a mobile phone in a restricted area or time is suspected, senior staff reserve the right to confiscate the phone and may require a search to be made, with appropriate supervision by

a colleague, if harmful content or use is reasonably suspected. Both colleagues conducting a search must be female and will initially request permission from the pupil.

Published Content and the School Website

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website or blogs, particularly in association with photographs.
- Currently permission from parents or carers is obtained before photographs of pupils are published on the school website, via the Terms and Conditions, which is agreed on entry to the school. Consent will be sought from parents and pupils (where age necessitates this) as per the terms of the GDPR from May 2018. Permission slips are used for consent in the Preps and Pre Preps.

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- Security strategies will be reviewed in line with the latest Government recommendations

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and in line with the GDPR (May 2018). Consent is sought for all sharing of personal data whether through the Terms and Conditions or via separate request, where authority is not already permitted.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

The school will audit ICT use to establish if the E-Safety Policy is adequate and that the implementation of the E-Safety Policy is appropriate.

Handling E-Safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures (see Safeguarding Policy).

Communication of Policy

Pupils

- The AUP will be made available on the VLE and website
- In the AUP pupils are informed that ICT use will be monitored

Staff

- All staff will be given the School E-Safety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff code of conduct and employment manual

Parents

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school website.
- Parents will be invited at regular intervals to feedback on any aspect of this policy and to attend training events.

Original document held by:	Head's PA
Member of Staff Responsible:	Deputy Head
Last Reviewed:	February 2018

St Augustine's PRIORY

St Augustine's Priory E-Safety Rules

These E-Safety Rules help to protect all pupils (including EYFS) and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the Headteacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.