7h Digital Responsibility (E-safety) Policy

Mission Statement

Our girls will change the world

- We are a Catholic community inspired by the vision of our founders and passionate about shaping a better future.
- We empower pupils with outstanding results, a love of learning and an alternative way of thinking.
- Augustinians are ethical leaders sowing joy, truth and courage.
- In this school freedom and generosity of spirit flourish. We seek a sustainable and prosperous future for all the world's communities.
- We cherish love for our neighbour, welcoming different faiths and cultures. Learning through dialogue we have hearts open to the whole world.

Equality Statement

At St Augustine's Priory we are committed to ensuring equality of education and opportunity for all pupils, staff, parents and carers receiving services from the School, irrespective of race, gender, disability, religion or socio-economic background. We aim to develop a culture of inclusion and diversity in which all those connected with the School feel proud of their identity and able to participate fully in School life. To that end we embrace the RADIO toolkit to equip all members of our community with the skills to participate in building a respectful culture.

Introduction

Digital responsibility encompasses any use of a digital device, smart technology 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 safeguarding and awareness for users to enable them to control their online experiences. The school's Digital Responsibility 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, Acceptable Use Policy (AUP) and Student Acceptable Use Policy.

Digital responsibility 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. We are committed to ensuring that we balance the life-giving and creative elements of this learning with an approach which brings best practice in enabling responsible behaviour for learning and well-being. The DSL has overall full responsibility.

Miss L Hales has overall responsibility.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, 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 scam

Good Habits

Digital responsibility depends on effective practice at a number of levels:

- Establishing a listening and telling culture where students know the school will act, and that when they report they will be kept informed about what is happening.
- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies. This includes the use of devices in lessons across the school. We have a `Live Teaching Etiquette' which we expect all students to abide if working remotely.
- Sound implementation of Digital Responsibility policy in both administration and curriculum, including secure school network design and use.
- Safe and secure Internet access including the effective management of content filtering.
- Regular and effective training for staff and student appropriate workshops.
- Regular review of trends, reporting and what we are learning from pupil voice.

School Digital Responsibility Policy

The Governing Board

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

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The Designated Safeguarding Lead

The DSL has overall responsibility for e-safety. The school has also appointed a Digital Responsibility coordinator in the Prep and Senior school. The Designated Safeguarding Lead is Miss L Hales, Assistant Head Co-Curricular, Deputy Designated Leads are Mrs A Lenton; Deputy Head Pastoral and Mr P McCarthy; Deputy Head Academic

The DSL (or DDSLs in her absence) takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged on MyConcern and the DSL Digital Log and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on MyConcern and the DSL Digital Log and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing board

  While the DSL/DDSL may check emails intermittently at weekends or during the holidays and pick up forensic monitoring alerts, it is the responsibility of parents to keep their child safe outside of normal school hours. If the forensic alert is deemed 'high risk', the Head will receive a telephone call and parents will be alerted as soon as possible.

The ICT Services Manager

The ICT manager is 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 pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school 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'

Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

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

St Augustine's Priory Online Safety Hub - https://sapriory.onlinesafetyhub.uk/

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

Parents will be invited to attend Parent Conversations and workshops on Digital Responsibility, either face-to-face or remotely, so that they have the knowledge and skills to help them keep their children safe online.

Pupils

- Our students:

Are involved in the review of our Digital Safety Agreement through discussion in lessons and our student e-safety forums, in an age-appropriate way.
Are responsible for following the Student Acceptable User Policy (AUP) whilst within school as agreed each academic year or whenever a new student starts at St Augustine's Priory for the first time, and required to sign that they have read and understood the rules;
Are taught to use the internet in a safe and responsible manner through, for example, Computing, PSHE /RSE lessons and assemblies as well as observing Safer Internet Day (Appendix 9);
Are provided with workshops on E-Safety from external industry experts at an age-appropriate level on a regular basis through the PSHE / RSE curriculum;
Are taught to immediately tell an adult about any inappropriate materials or contact from someone they do not know;
Are made aware of the potential use of online digital technologies to expose young people to inappropriate contact from strangers and to extremist ideas and know what to do if they encounter such issues;
Are taught and encouraged to consider the implications for misusing the internet and, for example, posting inappropriate materials to websites;
Are taught that the downloading of materials, for example music files and photographs, needs to be appropriate and 'fit for purpose', based on research for school work, and be copyright free;
Are taught to understand what is meant by digital safety through age-appropriate delivery in accordance with Education for a Connected World Framework.
Are taught that sending malicious or hurtful messages outside of school can become a matter whereby St Augustine's Priory may set sanctions or involve outside agencies such as the police;

Are taught not to put themselves at risk online or through mobile phone use and taught what to do if they are concerned, they have put themselves at risk;
Are given explicit guidelines and procedures for using mobile phones and other personal devices in school and are expected to abide by this Digital Safety Policy; and the Student Acceptable User Policy (AUP)
Are provided with a copy of the Student Digital Guide which includes a wealth of information of E-Safety and Responsible Digital Use.
A BYOD Protocol is in place to cover specific guidelines relating to the use of individual devices on the school network.
Are able to contact the IT team to ask for short-term access to blocked content. This must be in writing (email) and accompanied by rationale and a given timeframe.

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. It includes bullying that takes place outside school and can be reported via the usual channels to pastoral staff in school.

Youth Produced Sexual Imagery / Image Based Sexual Abuse and Harassment

Youth produced sexual imagery 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. Youth produced sexual imagery may also be called:

- Trading nudes
- Sexting
- Dirties
- Pic for pic

Youth produced sexual imagery can be seen as harmless or consensual 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”.

We recognise that image-based sexual harassment constitutes digital sexual violence and requires immediate intervention. We know that these practices are extremely common. We aim to embed a culture within our community where sexual harassment and sexual abuse are not tolerated.

Child on Child Abuse

Child on child 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. Child on child 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 child on child abuse, our Safeguarding Policy and Anti-Bullying Policy should be invoked. Our Safeguarding Policy and this Digital Responsibility Policy set out the procedures taken by the school to minimise the risk of child on child abuse, and the Safeguarding Policy clearly states how allegations of child on child abuse will be investigated and dealt with.

Staff receive regular training in how to manage a report of child on child sexual violence and sexual harassment with the added guidance that they must not view or forward illegal images of a child.

We are committed to proactive work with students making the most of learning from Ofsted's review of sexual abuse in schools and colleges and wider research including "Understanding and Combatting youth experiences of image based sexual harassment abuse".

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. Since COVID, the internet has become the medium through which remote learning occurs. It is no longer an add on.

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.

St Augustine's is proud to promote life-long learning which prepares pupils for the digital age and the 4.0 Industrial Revolution. We are in the midst of Education 4.0 and must equip students with the emotional skills needed.

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 Digital Responsibility lessons delivered by the ICT department, as well as through PSHEE and regular assemblies and the wider curriculum. Ms Wiley oversees E-safety in the Preps and delivers form time activities and Assemblies.
- Teaching is age appropriate and is designed to help children understand the risks posed by adults or young people who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults.
- Internet access and teaching components 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 will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- There is guidance in school planners for Preps and Senior pupils and pupils know how to report issues or concerns to the school or agencies such as CEOP.

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 Digital responsibility 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.

Filtering and Monitoring

In line with KCSIE the school ensures that appropriate filters and monitoring systems are in place to safeguard children from potentially harmful and inappropriate material on-line, but without an unreasonable level of blocking.

Smoothwall

The school employs an external forensic monitoring service which actively monitors staff and pupil online behaviour. This serves as a valuable safeguarding tool and offers invaluable information which enables early intervention. Alerts are sent to all members of the DSL team and the DSL maintain oversight of any trends and passes the information to the right member of staff for pastoral intervention. The school benefits from the national perspective and expertise of the service and their training has a high impact on the professional updates for staff and so the safety of students. We are also able to cascade this knowledge to parents. This is shared work. Any alerts that relate to a member of staff are dealt with by the Head teacher as per protocol.

Monitoring

It is the responsibility of St Augustine's Priory to ensure appropriate systems and technologies are in place to monitor and maintain the safeguarding and security of everyone using the School network. St Augustine's Priory will monitor the use of online technologies and the use of the internet by students and staff. The Designated Safeguarding Lead, Computer Science teachers and members of SLT will conduct regular audits with students to assess their knowledge and understanding of issues related to Digital Safety and act on any areas of vulnerability.

To audit digital safety and the effectiveness of this policy, the following questions should be considered:

- Has recording of e-safety incidents been effective – are records kept?
- Did the school feel able to respond effectively to any incidents?
- Were incidents resolved to the best of the school's ability?
- Do all students demonstrate an awareness of e-safety appropriate to their age?
- Have complaints or concerns with the policy been recorded and addressed?

- Have there been significant developments in technology that should be addressed either within the curriculum or as part of staff awareness training?
- Is the policy clear to all staff and seen as appropriate and working?
- Is the current wording fit for purpose and reflective of technology use at St Augustine's Priory?
- Do all members of our school community know how to report a problem?
- Is Digital Safety observed in teaching and present in curriculum planning documents?

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.
- Students are taught about the importance of e-mail etiquette such as use of language, dangers of phishing and links within an email and the need to protect email addresses at times using BCC for example. Emails sent by pupils to staff should follow the protocols instructed in Computer Science or ICT lessons.

Prevent

The school has an active approach to the use of social media for online radicalisation. 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 (Smoothwall) 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 who follows the school's procedures for Safeguarding Children as outlined in our Safeguarding Policy.

Social Networking and Social Media

- We actively promote a culture of listening, using NSPCC training to review what stops students reporting and what might stop adults listening.
- St Augustine's Priory filters access to social networking sites unless a specific use is approved. The Digital Responsibility 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. These privacy settings are discussed and communicated with students on a regular basis.
- 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 and how to recognise when something has, or is about to cross the line into 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, PSHEE, INSET, Assemblies and so on.
- Staff are also trained in areas of digital responsibility that covers the sharing of explicit images and the challenges that children face when using social media platforms.

Video Conferencing/livestreaming

- Pupils and staff receive regular training related to the use of video-based platforms such as Google Meets and Microsoft Teams.
- Pupils follow an agreed school protocol surrounding the use of video-based learning platforms when signing the AUP.
- When using video conferencing in school, pupils will only use 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. Priory Sixth pupils may use their mobile phones within the 6th Form Common Room at lunchtime only. From time to time we understand that girls may need to use mobile devices for learning and this must only be done with the permission of a teacher. If a pupil has their mobile phone confiscated, they will be given a one-hour Friday detention after school. Staff may use their mobile phone in the common room only.

- The sending of abusive or inappropriate messages is forbidden.
- 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.
- Pupils are aware of the fact that smart watches are not to be used in school.
- The school considers carefully how to manage 3G, 4G and 5G accessibility – risk is managed by regular reminders to students, swift follow up to reported incidents, the locking of devices during the school day where required, the application of pastoral support or sanctions as required and close contact with parents and carers.
- Staff will be issued with a school phone where contact with pupils is required, e.g. when taking school trips. Staff will not create WhatsApp groups with girls.
- Any sanctions related to this are referenced in the school's 9a Promoting Good Behaviour Policy.

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.
- The school website includes a visible link to CEOP where students can report instances of online abuse, cyberbullying etc.
- Pupils will not adapt, doctor or alter any published content including images, photos and videos of staff or other pupils.

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. Prevent guidance expects school to ensure that children are safe from terrorist or extremist material when accessing the internet through school systems. The school cannot accept liability for the material accessed, or any consequences of internet access but the school actively monitors internet use through the forensic monitoring software and acts swiftly if any student is considered to be at risk. Staff receive regular training in this.

All aspects of internet safety or alerts received via forensic monitoring are reported termly to the governors' Safeguarding Committee. Trends are identified and any learning required is addressed swiftly.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. Safeguarding Leads may come across such images. Staff will never intentionally view an indecent image of a child

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

- The DfE's latest guidance on screening, searching and confiscation

UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

- The Promoting Good Behaviour Policy

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

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Promoting Good Behaviour and Acceptable Use Policy (AUP). 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 school'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 procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

Handling Digital responsibility 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).

See also

- Promoting Good Behaviour Policy
- Pupil Code of Conduct
    - clear guidance on the use of technology in the classroom and beyond for all users, including staff, pupils and visitors that references permissions/restrictions and agreed sanctions;
    - mention of the school's technical provision/infrastructure and safeguards in place to filter and monitor inappropriate content and alert the school to safeguarding issues; (school
- Staff Code of Conduct

Communication of Policy

Pupils

- The student AUP is available on the website and in pupil planners
- In the student AUP pupils are informed that ICT use will be monitored
- Students are asked to complete a digital acceptance form showing that they have read, understood and agree to adhere to the points outlined in the student AUP

Staff

- All staff will be given the School Digital Responsibility Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user, and that all screens are monitored by the school's monitoring service provider. Discretion and professional conduct are 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.
- All staff receive regular Digital Responsibility training at INSET or in staff meetings, and at least biennially.

Parents

- As first educators of their child, parents' participation in our work on digital responsibility is key.
- Parents' attention will be drawn to the School Digital Responsibility 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.
- Parents will be offered workshops at school in digital responsibility on a regular basis and at least biennially.

Review of Policy

Regular pupil focus groups, questionnaires and triangulation of patterns or trends take place weekly or termly to ensure to ensure vigilance and to embed the knowledge that it could happen here.

To be read in conjunction with

- Safeguarding Policy
- Promoting Good Behaviour Policy for policies on Mobile Technology
- IT Acceptable Use Policy
- Complaints procedure
- Code of Conduct for Staff.
- AI Policy

Appendix 1 - St Augustine's Priory Student ICT Acceptable Use Policy

- I will be considered responsible for any content I post online (including outside of school time) or send in an email.
- I understand my responsibility for maintaining the reputation of the school.
- I will only use my school email address in relation to educational purposes and web sites (e.g. website registration, communication purposes etc.)
- I understand that staff will reject/refuse invitations or and/or requests from pupils to partake in discussion forums, instant messaging and webcams and other forms of social media other than those which form communication based on educational purposes (use of Google Classrooms, meets, Microsoft Teams etc).
- I will not use my mobile phone/tablet (other similar device) in school (6th Form may use theirs in the Common Room at lunch time only) for any purpose other than has been agreed by members of staff. My phone must be placed inside a secure locker and not used within the school grounds.
- I will not use any device to record videos or take photos of students or staff when on the school site or when on a school trip, unless specifically instructed by a member of staff for school purposes. I will not share any images that I take of other students or staff without their prior permission.
- I will not share any images of students or staff that I find on school platforms or the school website on social networking sites.
- I will only take a photograph or video of other students or staff if specifically instructed to by a member of staff when on the school site or when on a school trip for educational purposes.
- I will take all reasonable steps to ensure the safety and security of School ICT equipment which I take off site and will remove anything of a personal nature before it is returned to school.
- I will take all reasonable steps to ensure that all laptops and other devices are fully virus protected and that protection is kept up to date.
- I will report any accidental access to material which might be considered unacceptable immediately to a member of staff who will pass the concern onto the Senior Leadership Team and ensure it is recorded.
- I will support the school's approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community. I will not like, repost or forward or interact in a way that encourages any such content.
- I will inform my form teacher, Head of Year or IT staff members if my online data becomes insecure (e.g. my password has been shared) or if I accidentally, or purposefully, share confidential information online to a member of staff.
- I am aware that photos of me may be posted on school platforms or other educational platforms or platforms used by the school for educational purposes; these photos will not include my name and cannot be searched for via search engines.
- I will not share my password nor allow a student or member of staff to log in to the school system on my behalf.
- I will use the photocopiers and other school hardware devices responsibly.
- I will monitor my email inbox and other message services carefully. I will take care when opening links within messages.
- I understand that the school monitors all use of ICT equipment and electronic communications on the school network.
- The monitoring software we use (Smoothwall) will monitor Chrome web activity on personal devices used on other networks (such as home and public networks). This applies to devices where a student's school Google account has been used to sign into the Chrome browser.

- I understand that I must make use of appropriate online video etiquette during remote learning, for example, muting when asked, being appropriately dressed, leaving a classroom when the teacher asks me to and following any other requests from my teacher to help my learning and the education of other students. Further guidelines are discussed in ICT and Computing lessons.
- I will do my best to ensure that my device has sufficient battery to last throughout the day and I will bring a charger to school with me on a day-to-day basis. I will bring headphones to school and all lessons.
- When not in use, I will either lock my device in my locker (using my padlock) or keep it in my bag in my possession. This does not apply to my mobile phone which must be secured in my locker throughout the school day.
- I understand that loss of or damage to my device is not covered by the school's insurance.
- I understand that I must use my device in a responsible manner based on learning needs. For example, I will not use my device to watch TV shows, carry out online shopping, use social media etc during school hours.

I confirm that I have read and understood the St Augustine's Priory ICT AUP as outlined above and that I will use all means of electronic communication equipment provided to me by the school and any personal devices, which I use for school activity, in accordance with the document. I understand that I am part of creating a school environment which feels safe and inclusive for everyone in the community, whether pupils or staff.

I understand that by not following these rules I may be subject to the school's disciplinary procedures.

NAME IN BLOCK CAPITALS: _____

Signature:_____

Date_____

Appendix 2 - Social Media Do's and Don'ts

Managing your personal use of social media

- 'Nothing' on social media is truly private.
- Social media can blur the lines between your professional and private life. Don't use the school logo and or branding on personal accounts.
- Check your settings regularly and test your privacy.
- Keep an eye on your digital footprint.
- Keep your personal information private.
- Regularly review your connections – keep them to those you want to be connected to.
- When posting online, consider: scale, audience and permanency.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?

Know how to report a problem.

The Do's

- Check with a senior member of staff before publishing content that may have controversial implications for St Augustine's Priory;
- Use a disclaimer when expressing personal views;
- Make it clear who is posting content;
- Use an appropriate and professional tone;
- Be respectful to all parties;
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author;
- Express opinions but do so in a balanced and measured manner;
- Think before responding to comments and, when in doubt, get a second opinion;
- Seek advice and report any mistakes using St Augustine's Priory reporting process; and
- Consider turning off tagging people in images where possible.

The Don'ts:

- Don't make comments, post content or link to materials that will bring St Augustine's Priory into disrepute;
- Don't publish confidential or commercially sensitive material;
- Don't breach copyright, data protection or other relevant legislation;
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content;
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content; and
- Don't use social media to air internal grievances.

Appendix 7 - Email etiquette Email best practice

Write well-structured emails and use short, descriptive subjects.

- Sentences can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. The use of internet abbreviations and characters such as smileys is not encouraged.
- Signatures must include your name, job title and school name. Users must spell check all mails prior to transmission.
- Only mark emails as important if they really are important.
- Avoid long strings of messages; start new conversations.
- Consider your use of manners. How would you feel to receive your email.

Do not

- Write it in an email unless you would put it on a noticeboard in the office or in a newspaper.
- Write anything that is libellous, defamatory, offensive, racist or obscene - you and the school can be held liable
- Forward confidential information - you and St Augustine's Priory can be held liable.
- Forward a message with sensitive information without acquiring permission from the sender first.
- Send email messages using another person's email account.