ST. JOSEPH'S COLLEGE
READING • BERKSHIRE

E-SAFETY POLICY

Policy Owner Sean Hatton Assistant Head (Wellbeing & Safeguarding)	**Associated documents** • Anti Bullying policy, • Behaviour, Rewards and Sanctions policy • Data Protection Policy for Students and Parents • Guidelines for communicating with the College • Mobile device policy • Staff Code of Conduct • The Publications Office of the EU's Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators	**Legal Framework** • Keeping Children Safe in Education (2024), • Working Together to Safeguard Children (2023), • the Maintained schools governance guide. • Part 3 of the schedule to the Education (Independent School Standards) Regulations 2014,
Review by **October 2024**	**Review frequency** Annually	**Next Review date** October 2025

Changes History:

Version	Date	Amended by:	Substantive changes:	Purpose
1.0			n/a	Previous version

2.0	30/10/23	SJAH	1. Change to structure 2. Change of roles within policy	1. Ease of reference 2. Clarity following restructure of SLT
2.1	9.8.24	SJAH	Section on Artificial Intelligence added	Consideration of emerging technology

1.

ST. JOSEPH'S COLLEGE
READING • BERKSHIRE

E-Safety Policy

This policy relates to all sections of St Joseph's College, including the Early Years Foundation Stage (EYFS).

2. Aims

2.1. By means of this policy St. Joseph's College aims to:

2.1.1. Safeguard and protect all members of the school's community online
2.1.2. Identify approaches to educate and raise awareness of online safety throughout the community
2.1.3. Enable all staff to work safely and responsibly, to model positive behaviour online and to manage professional standards and practice when using technology
2.1.4. Identify clear procedures to use when responding to online safety concerns.

3. Introduction

3.1. New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.
3.2. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

3.2.1. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:Access to illegal, harmful or inappropriate images or other content;
3.2.2. Unauthorised access to / loss of / sharing of personal information;
3.2.3. The risk of being subject to grooming by those with whom they make contact on the internet;
3.2.4. The sharing / distribution of personal images without an individual's consent or knowledge;
3.2.5. Inappropriate communication / contact with others, including strangers;
3.2.6. Cyber-bullying;
3.2.7. Access to unsuitable video / internet games;

3.2.8. An inability to evaluate the quality, accuracy and relevance of information on the internet;
3.2.9. Plagiarism and copyright infringement;
3.2.10. Illegal downloading of music or video files;
3.2.11. The potential for excessive use which may impact on the social and emotional development and learning of the young person.

3.3. The issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

3.3.1. Content: being exposed to illegal, inappropriate or harmful material; for example, pornography, racist or radical and extremist views, and in some respects fake news
3.3.2. Contact: being subjected to harmful online interaction with other users; for example, children can be contacted by bullies or people who groom or seek to abuse them
3.3.3. Commercial exploitation: for example, young people can be unaware of hidden costs and advertising in apps, games and website
3.3.4. Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying

3.4. This policy applies to all members of the College community (including staff, students, parents and visitors) who have access to the College ICT facilities both in and out of the school.

4. Roles and Responsibilities:

4.1. ***The Assistant Head (W&S)*** is responsible for monitoring its effectiveness. This is carried out via discussions with members of staff, the pastoral team, counsellors and at Safeguarding Committee meetings.

4.2. ***The Technical Support Team (including Head of IT Strategy, IT Technician and IT Apprentice)*** is responsible for ensuring that the College technical infrastructure is as secure as possible; that only registered users may access the College networks and devices; that appropriate filtering is applied and updated on a regular basis and that use of the College ICT facilities is regularly monitored to ensure compliance with the Computer Usage Policy. Furthermore, it is the team's responsibility to report any breach of Computer Usage Policy to the E-Safety Lead or Assistant Head (W&S).

4.3. ***The Designated Safeguarding Lead*** is responsible for maintaining records of E-Safety incidents and following up on any child protection issues that may arise out of an E-Safety incident. This will be in accordance with the College Safeguarding Policy.

4.4. ***Head of IT Strategy*** is responsible for the development of Computer Usage and E-Safety Policies and the monitoring, compliance and follow-up of actions contained therein. Furthermore, he is responsible for ensuring that the Technical Support Team fulfil their duties as stated above. Lastly, any E-

Safety incidents or safeguarding concerns must be forwarded to Heads of Seniors/Sixth Form or Prep Pastoral Lead and DSL for recording.

4.4.1. The Head of IT Strategy is also the **E-Safety Co-ordinator**, working with the Designated Safeguarding Lead to help ensure that staff, students and parent awareness of E-Safety information and news is current and appropriate. Furthermore, is responsible for maintaining the E-Safety policy in coordination with the DSL.

4.5. ***All staff*** are responsible for ensuring that they have an up-to-date awareness of this policy, that they adhere to the College Computer Usage Policy, that they report any suspected misuse to the Assistant Head (W&S) (DSL) as appropriate and that they help students to understand the E-Safety policy and related policies.

4.6. ***Students*** must ensure they adhere to the Computer Usage Policy. They should understand the importance of reporting to a member of staff any abuse, misuse or access to inappropriate materials. They should also understand the importance of adopting good E-Safety practice when using technology outside College and realise that the College Behaviour, Anti-Bullying and E-safety policies will cover their actions outside College if related to their membership of the College.

4.7. ***Parents*** are asked to support the College in promoting good E-Safety practice and to follow the guidelines in this policy.

5. Use of Technology in College

5.1. Acceptable Use Agreements

5.1.1. All use of the College Network, of personal devices in College and of devices owned by the College (whether on or off the College site) must comply with the Acceptable Use of IT facilities which is outlined for students in the Computer Usage Policy and for staff in the Staff Handbook (sections E4, E8 & J2) and comply with Mobile Device Policy as applicable.

5.1.2. Failure to comply with the relevant Acceptable Use agreement may result in disciplinary sanctions for students in accordance with the College Behaviour, Rewards and Sanctions Policy and for staff under the Staff Code of Conduct.

5.2. Internet

5.2.1. Student use of the Internet is limited to educational purposes, except for those specific conditions set out in the Guidelines for Computer Use.

5.2.2. Use of file-sharing sites (with the exception of Google Drive and Microsoft 365), music or video download sites and non-educational video sites is not permitted at any time.

5.2.3. At all times, Internet use must remain within the boundaries of commonly accepted respectability, and not be contrary to the ethos or interests of the College.

5.2.4. Users must not use the Internet to access or send illegal or offensive content.

5.2.5. Users must not attempt to bypass or disable the content filtering or activity monitoring systems which the College has in place.
5.2.6. Use of the Internet is carried out with the understanding that the College may monitor activity, including the sites visited, files accessed and any information which is transmitted via the Internet. This information may be shared with others at the discretion of the College.

5.3. Network Activity

5.3.1. Personal use of the computers is permitted, however people wishing to do schoolwork must be given priority. Personal printing is not permitted without prior agreement from the College.
5.3.2. At all times, computer use must remain within the boundaries of commonly accepted respectability, and not be contrary to the ethos or interests of the College.
5.3.3. Users must not share their passwords with anyone else, nor must they log on as another person.
5.3.4. Users must not attempt to bypass or disable the security which the College has in place.
5.3.5. Users must not use the network to store illegal or offensive content. This includes any information which the school is not permitted to possess, for example, copies of music or videos which the College does not own.
5.3.6. Users must not deliberately cause damage of any nature to the computers, or do anything which they believe may be harmful in any way.
5.3.7. Use of the computers is carried out with the understanding that the College may monitor any and all activity. This information may be shared with others at the discretion of the College.
5.3.8. Any information saved on or accessed using the network, including the contents of removable media, may be seen by College staff. This information may be shared at the discretion of the College.

5.4. Safe Usage online

5.4.1. **Don't post personal** information online, like your address, your email address or mobile number. Keep personal information as general as possible.
5.4.2. **Think** very carefully before posting photos of yourself online; once your picture is online, anyone can download it and then share it or even change it.
5.4.3. **Protect** your privacy. Never let anyone have access to your passwords. Check the privacy settings on your accounts, and make sure you know how to keep your personal information private.
5.4.4. **Remember**, not everyone online is who they say they are and grooming can occur without you realising it.
5.4.5. **It's never a good idea** to meet up with someone you've met online. You should only do this if you've told a parent or carer and they can come with you.
5.4.6. **Think** carefully about what you say before you write or post anything online.

5.4.7. **Respect** other people's views – just because you don't agree with them, it doesn't mean that you have to be rude or abusive.
5.4.8. **Google** yourself every now and again. It will show you what is online about you and what others can see – and you can make changes if you don't like what you see.
5.4.9. http://cybermentors.org.uk

5.5. ***Devices owned by the College*** may be assigned to staff or students for short-term or longer-term use. Devices assigned for short-term use (for example in a particular lesson, for an exam or a school visit) must be signed in and out by the member of staff responsible.
5.6. ***Personal Devices*** and the use thereof is explained in a separate policy, namely Mobile Device Policy.

6. Technical Infrastructure

6.1. The Technical Support Team reviews and audits the safety and security of the College technical systems. This will periodically be supplemented by an external audit and review.
6.2. Servers, wireless systems and cabling is securely located and physical access is restricted.
6.3. All users are provided with a username and password by the Technical Support Team. Users are responsible for the security of their username and password.
6.4. The College monitors, controls and filters internet access for all users. Websites containing illegal, pornographic, violent, abusive, terrorist or extremist material are blocked. Instant messaging and social networking sites, as well as gaming and other similar sites, will be blocked unless specifically authorised by the Technical Support Team and any of the College Deputy Heads.
6.5. Websites visited are recorded and monitored by the Technical Support Team. The Head of IT Strategy in coordination with the Designated Safeguarding Lead and E-Safety Lead reviews sites flagged as potentially intolerant and monitors for patterns and issues of concern. Data transfer to and from the College facilities will be subjected to virus scanning and filtering.

7. Staff Awareness

7.1. All new members of staff receive information on the College E-Safety and Computer Usage Policy as part of their induction.
7.2. Teaching staff receive information about e-safety issues at staff meetings as and when required and as part of their regular safeguarding training updates.
7.3. The College has appointed an E-Safety Lead who works with the Assistant Head (W&S) to help ensure that staff awareness of, and training in, e-safety is current and appropriate.

8. Student Education and Information

8.1. All new students receive a copy of the College Acceptable Use of IT facilities. They are encouraged to discuss its contents with a parent or teacher and then to sign to confirm that they will adhere to its terms.

8.2. All areas of E-Safety are embedded across in the College's PSHEE programme rather than taught as a separate unit, to reflect that the online world is very much intertwined with everyday life. These topics can be found in blue on our PSHEE Curriculum Overview.

8.3. Key e-safety messages are delivered in assemblies, form time and ICT lessons. External speakers will also be invited to speak to students, and sometimes parents, on e-safety topics. Our Student Voice IT Committee also contribute to matters of E-Safety.

9. Data Protection

9.1. The College has a Data Protection Policy which includes electronic data and an Information Security Policy which advises staff on how best to keep information secure.

9.2. The College must ensure that appropriate security measures are taken to prevent unlawful or unauthorised processing of the personal data and against the accidental loss of personal data.

9.3. Staff must not remove Personal Data from the College premises unless it is stored in an encrypted form on a password protected computer or a memory device provided by the College, with the exception that the College data management system may be accessed remotely from password protected devices and relevant personal data about students out of College on a visit may be carried by accompanying members of staff.

10. Social Networking

10.1. The College recognises that staff and students have lives outside the College and can and will make decisions about their own use of social networking sites. To inform these decisions, and for the protection of both staff and students, this policy is designed to be clear and explicit about appropriate behaviour in the use of social media and electronic communication and the College's responsibility to its staff and students to promote e-safety.

10.2. We take the view that all information posted on websites should be considered as published, permanent and potentially public - even if it is 'protected' in some way. Just because something is personal in nature or an individual doesn't want people to know about it does not make it private. Social networks by their nature blur the divide between public and private simply by being networks. Their purpose is to provide simple ways of sharing information as widely as possible and some will make information available to a far wider audience than might be expected or desired. Seemingly innocent information, photographs, videos, opinions or comments are

vulnerable to misrepresentation and unauthorised distribution via the internet.

10.3. Social Networking - **DO**

10.3.1. Assume everything online is permanent and effectively public
10.3.2. Make sure you consider who might see anything you post
10.3.3. Write appropriately for your expected audience
10.3.4. Make all staff / student online interactions meaningful and professional
10.3.5. Consider specifically safety and reputation before posting online
10.3.6. Take responsibility for what you post / distribute online
10.3.7. Use the internet positively for communication, collaboration and learning
10.3.8. Use and maintain privacy settings to protect personal information but do not rely on them

10.4. Social Networking - **DON'T**

10.4.1. Post anything which might damage your own or the college's reputation
10.4.2. Redistribute any material which may harm others in any way
10.4.3. Use the internet to form, or attempt to form, any relationship which would be otherwise inappropriate
10.4.4. Create an online environment which invites others to post harmful content
10.4.5. Post without thinking
10.4.6. Post without considering the safeguarding risks
10.4.7. Use screenshots to share private conversations between peers, content from lessons or for malicious reasons

11. Internet Site Filtering

11.1. The College employs a physical firewall on site to monitor and filter internet access, including social media sites. The firewall is installed immediately after the school's internet connection and prior to the College's LAN, thus ensuring all external content is monitored.

11.2. Smoothwall, the College's firewall, categorises websites based on the purpose of the website and its content. Access policies are then applied to these categories to permit or restrict access to different groups of students further based on Year groups or Sections.

11.3. Below is a list of these categories that are restricted and thus prohibited on the school network:

Category	Description
Adult & Mature Content	Sites that contain material of adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These sites include very profane or vulgar content and sites that are not appropriate for children.
Alcohol / Tobacco	Sites that promote or offer for the sale alcohol/tobacco products, or provide the means to create them. Also includes sites that glorify, tout, or otherwise encourage the consumption of alcohol/tobacco. Does not include sites that sell alcohol or tobacco as a subset of other products.

Criminal & Illegal Skills	Sites that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. Sites that provide instructions about or promote crime, unethical/dishonest behaviour or evasion of prosecution thereof. Excludes computer crime.
Cult & Occult	Sites that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers or supernatural beings.
Drugs	Drug sites that promote, offer, sell, and supply, encourage or otherwise advocate the recreational or illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia. In addition, sites that discuss or promote the use of regulated drugs and their abuse, as well as the paraphernalia associated with abuse that provide information about approved drugs and their medical use and promote the use of chemicals not regulated by the FDA.
Gambling	Sites where a user can place a bet or participate in a betting pool (including lotteries) online. Also includes sites that provide information, assistance, recommendations, or training on placing bets or participating in games of chance. Does not include sites that sell gambling related products or machines. Also does not include sites for offline casinos and hotels (as long as those sites do not meet one of the above requirements).
Hacking and Proxy Avoidance	Sites providing information on illegal or questionable access to or the use of communications equipment/software, or provide information on how to bypass proxy server features or gain access to URLs in any way that bypasses the proxy server.
Illegal Drugs	Sites that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.
Intimate Apparel / Swimsuits	Sites that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. Does not include sites selling undergarments as a subsection of other products offered.
Nudity	Sites containing nude or semi-nude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include sites containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist sites that contain pictures of nude individuals.
Pornography	Sites that contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
Sex Education	Sites that provide graphic information on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. Also includes sites that offer tips for better sex as well as products used for sexual enhancement.
Social-Networking	There are security risks associated with allowing users to connect to social networking sites that put personal and college data at risk that include identity theft through social engineering, liability from personal information, as well as viruses, spyware, and malware linked to from the social networking site.
Streaming Media & MP3	Sites that sell, deliver, or stream music or video content in any format, including sites that provide downloads for such viewers.

Violence, Hate and Racism	Sites that depict extreme physical harm to people or property, or that advocate or provide instructions on how to cause such harm. Also includes sites that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characteristics.
Weapons	Sites that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications. Does not include sites that promote collecting weapons, or groups that either support or oppose weapons use.

11.4. Exceptions to the filtering are listed below:

Website	**Category**	**To whom**	**Reason**
www.youtube.com	Streaming Media / MP3	Year 12 and Year 13	Students need websites to access academic content and the small number of sixth form students will not affect internet bandwidth available
www.pintrest.com	Social Media	Year 12 and Year 13	Needed for Graphics and Art A-Level subjects

12. Procedures for dealing with e-safety incidents involving students

12.1. If a student feels uncomfortable or worried by anything online or on a device, they should tell a member of staff or parent as soon as possible.

12.2. Any allegation, complaint, concern, or suspicion that a student has been involved in any of the following should be reported immediately to the Designated Safeguarding Lead and action will be taken in accordance with the College Safeguarding Policy:

12.2.1. Possession of, or access/attempted access to a website containing, images of child abuse;

12.2.2. Possession of, or access/attempted access to a website containing, illegal (e.g. obscene or criminally racist) or terrorist or extremist material;

12.2.3. Any incident by electronic means involving 'grooming' behaviour;

12.2.4. Any other incident (which may include instances of cyber-bullying or 'sexting' or peer on peer abuse) that suggests that a student or another child has suffered or is at risk of suffering serious harm.

12.3. Concerns or allegations regarding other technology related illegal activity such as fraud, copyright theft, unlicensed use of software or unlawful use of personal data should be reported to the Assistant Head (W&S). Such concerns will be managed in accordance with the College Behaviour Policy although referrals may be made to outside agencies as appropriate.

12.4. Any concern or allegation regarding 'sexting' (also known as 'youth produced sexual imagery') should be reported to the Assistant Head (W&S), who is also the Designated Safeguarding Lead. Sexting may constitute abuse or a criminal offence and will be considered in accordance with the College Safeguarding Policy and guidance published by the UK Council for Child Internet Safety: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'. Incidents involving sexting will be recorded in the safeguarding records by the DSL.

12.5. Any allegation of cyber-bullying which does not fall within point 4 above should be reported to the Assistant Head (W&S) as soon as possible. Cyber-bullying incidents will be dealt with in accordance with the College Anti-Bullying and Behaviour policies unless there is a risk of serious harm to a child and/or the incident constitutes Safeguarding Policy.

12.6. Any other misuse of the College ICT facilities not falling within one of the categories above should be referred to any of the College Deputy Heads who will take action as appropriate in accordance with the College Behaviour, Rewards and Sanction Policy.

13.Procedures for dealing with e-safety incidents involving staff

13.1. Any allegation, complaint, concern, or suspicion that a member of staff has been involved in any of the following should be reported immediately to the Head (or to the Chair of Governors if the Head is the subject of the concern) and action will be taken in accordance with the College Safeguarding Policy:

13.1.1. Possession of, or access/attempted access to a website containing, images of child abuse;

13.1.2. Possession of, or access/attempted access to a website containing, illegal (e.g. obscene or criminally racist) or terrorist or extremist material;

13.1.3. Any incident by electronic means involving 'grooming' behaviour;

13.1.4. Any other incident that suggests that a student or another child has suffered or is at risk of suffering serious harm from a member of staff.

13.2. Concerns or allegations regarding other technology related illegal activity such as fraud, copyright theft or unlawful use of personal data should be reported to the Head or the Bursar immediately. Such concerns will be managed in accordance with the College Whistleblowing Policy and disciplinary procedures and will be referred to the police as appropriate.

13.3. Any other misuse of the College ICT facilities not falling within one of the categories above should be referred to the Bursar who will take action as appropriate in accordance with the College disciplinary procedures.

14.Collecting and preserving evidence

14.1. If a member of staff suspects or is informed that there are indecent or obscene images of a student or another child on a device, the member of staff should not attempt to search for or print off such images as this may in itself constitute a criminal offence. The device should be confiscated, secured and handed directly to the Designated Safeguarding Lead. The Designated Safeguarding Lead and another member of SLT, Head of Seniors/Sixth Form or Prep Pastoral Lead will investigate further, using guidelines developed by CEOP (Child Exploitation and Online Protection centre) and the UK Council for Child Internet Safety.

14.2. For guidance on collecting and preserving electronic evidence in other instances, particularly where there has been an allegation of cyber-bullying. The Head of IT Strategy can also be consulted to assist in establishing, capturing or preserving relevant data or other evidence.

15.Artificial intelligence (AI)

15.1. Introduction

15.1.1. At St Joseph's College, we recognize the growing influence of Artificial Intelligence (AI) in education and its potential to enhance learning and administrative processes. However, we are also aware of the associated risks

and ethical considerations. We aim to ensure the responsible use of AI within our school environment, safeguarding the privacy, security, and well-being of all students, staff, and stakeholders.

15.2. Purpose

15.2.1. The purpose of this section is to outline the guidelines for the use of AI technologies within the College, ensuring that their application aligns with our commitment to e-safety, data protection, and ethical practices. This policy applies to all students, staff, and third-party service providers who interact with AI systems or technologies on the College premises or through school-provided platforms.

15.3. Definitions:

15.3.1. To ensure a clear understanding of this Agreement, we provide definitions for key terms related to AI and data use in education. These definitions are based on the "Ethical Guidelines on the Use of Artificial Intelligence (AI) and Data in Teaching and Learning for Educators" document published by the European Commission in September 2022.

15.3.1.1. Artificial Intelligence (AI): AI refers to systems that display intelligent behaviour by analysing their environment and taking actions to achieve specific goals. In the context of education, AI can be used in various ways, such as assessing progress, personalising learning, and analysing educational data.

15.3.1.2. Data: In the context of this Agreement, data refers to information collected about students' learning and behaviour in the educational environment. This can include grades, attendance, online activity, and other relevant information.

15.3.1.3. Ethical Use: Ethical use refers to the use of AI and data in a manner that respects individual rights, promotes fairness, and prevents discrimination. It also involves using these technologies in a way that is transparent, accountable, and respects privacy.

15.3.1.4. Privacy and Data Governance: This refers to the practices and procedures in place to protect the privacy of individuals and ensure the secure and ethical handling of data.

15.3.1.5. Technical Robustness and Safety: This refers to the reliability and safety of AI systems. It involves ensuring that these systems function correctly, are secure from cyber threats, and do not cause harm to users or the educational environment.

15.3.1.6. Human Agency and Oversight: This refers to the need for human involvement in the use of AI systems. It involves ensuring that decisions made by AI systems can be understood and overseen by humans, and that there are mechanisms in place for human intervention when necessary.

15.3.1.7. Societal and Environmental Wellbeing: This refers to the impact of AI and data use on society and the environment. It involves considering the broader implications of these technologies, including their potential effects on social interactions, wellbeing, and the environment.

15.4. Use of AI in Education

15.4.1. **Educational Enhancement**: AI tools may be used to support personalized learning, automate administrative tasks, and provide insights into student progress. These tools must be vetted for safety, accuracy, and educational value before implementation.

15.4.2. **Transparency**: Students and parents will be informed when AI tools are being used in the educational process. Clear information will be provided on how these tools work, what data is being collected, and how it will be used.

15.5. Data Protection and Privacy

15.5.1. **Data Collection and Usage**: Any data collected by AI systems must comply with the UK General Data Protection Regulation (GDPR). Only necessary data should be collected, and it must be stored securely. Personal data must not be shared with third parties without explicit consent.

15.5.2. **Anonymization**: Where possible, data used by AI systems should be anonymized to protect the identities of students and staff.

15.5.3. **Parental Consent**: Parents or guardians must be informed and give consent before any AI technology that collects or processes personal data of students is used.

15.5.4. More information can be found in the College Data Protection policy

15.6. Ethical Use of AI

15.6.1. The College is committed to the ethical use of AI and data in all aspects of our educational environment. We believe that these technologies can greatly enhance teaching and learning, but they must be used in a manner that respects individual rights, promotes fairness, and prevents discrimination.

15.6.2. **Respect for individual rights**: We respect the rights of all individuals in our school community. This includes the right to privacy, the right to non-discrimination, and the right to an education that respects their individual needs and abilities.

15.6.3. **Bias and Fairness**: AI systems used in the College must be regularly reviewed to ensure they are free from bias and do not disadvantage any group of students. The College is committed to promoting fairness and equality in the use of AI.

15.6.4. **Human Oversight**: AI should support, not replace, the professional judgment of educators. All decisions that significantly impact students or staff must involve human oversight.

15.6.5. **Responsible Use**: Staff and students must use AI tools responsibly and ethically, adhering to the school's e-safety guidelines. Misuse of AI, such as

using AI to generate inappropriate content or engage in cyberbullying, will result in disciplinary action.

15.7. Key requirements for trustworthy AI

15.7.1. In line with the "Ethical Guidelines on the Use of Artificial Intelligence (AI) and Data in Teaching and Learning for Educators" document, we adhere to the following key requirements for trustworthy AI:

15.7.1.1. **Human agency and oversight**: We ensure that there is always a human in the loop when using AI systems, and that these systems are used to support, not replace, human decision-making.

15.7.1.2. **Technical robustness and safety**: We use AI systems that are reliable, secure, and safe to use.

15.7.1.3. **Privacy and data governance**: We have strong data governance practices in place to protect the privacy of our students and staff.

15.7.1.4. **Transparency**: We are transparent about our use of AI and data technologies, and we provide clear explanations about how these technologies work and how decisions are made.

15.7.1.5. **Diversity, non-discrimination, and fairness**: We use AI and data technologies in a manner that respects diversity, prevents discrimination, and promotes fairness.

15.7.1.6. **Societal and environmental wellbeing**: We consider the broader societal and environmental implications of our use of AI and data technologies.

15.8. Cybersecurity

15.8.1. **Security Measures**: AI systems must be protected by appropriate cybersecurity measures to prevent unauthorized access, data breaches, and other cyber threats.

15.8.2. **Regular Audits**: The school will conduct regular audits of AI systems to ensure they remain secure, compliant with regulations, and effective in their intended purposes.

15.9. Training and Awareness

15.9.1. **Staff Training**: All staff members will receive training on the ethical use of AI, data protection, and cybersecurity related to AI tools. This will include understanding the potential risks and how to mitigate them.

15.9.2. **Student Education**: Students will be educated on the responsible use of AI, including understanding the impact of AI on privacy, security, and their digital footprint.

15.10. Reporting and Monitoring

15.10.1. **Reporting Concerns**: Any concerns about the misuse of AI or its potential impact on e-safety should be reported immediately to the designated E-safety Lead (Assistant Head (W&S) or the Head of IT Strategy.

15.10.2. **Ongoing Monitoring**: The College will continuously monitor the use of AI technologies to ensure compliance with this policy and make adjustments as necessary to address new risks or challenges.