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).

Introduction

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. 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.

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;
- Unauthorised access to / loss of / sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing / distribution of personal images without an individual's consent or
- knowledge;
- Inappropriate communication / contact with others, including strangers;
- Cyber-bullying;
- Access to unsuitable video / internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this E-Safety policy is used in conjunction with other College policies such as the Safeguarding Policy, the Behaviour, Rewards and Sanction Policy, the Anti-Bullying Policy, Mobile Device Policy, Data Breach and Data Protection Policies, Computer Usage Policy and other policies and procedures referred to below.

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

Roles and Responsibilities:

The Deputy Head Pastoral 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.

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 Deputy Head Pastoral.

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.

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.

E-Safety Lead is responsible for working with the Designated Safeguarding Lead to help ensure that staff, pupils 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 Head of IT Strategy and DSL.

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 Deputy Head Pastoral (DSL) as appropriate and that they help pupils to understand the E-Safety policy and related policies.

Pupils 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.

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

Use of Technology in College

Acceptable Use Agreements: 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 pupils in the Computer Usage Policy and for staff in the Staff Handbook (sections E4, E8 & J2) and comply with Mobile Device Policy as applicable. Failure to comply with the relevant Acceptable Use agreement may result in disciplinary sanctions for pupils in accordance with the College Behaviour, Rewards and Sanctions Policy and for staff under the Staff Code of Conduct.

Internet

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

- 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.
- 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.
- Users must not use the Internet to access or send illegal or offensive content.
- Users must not attempt to bypass or disable the content filtering or activity monitoring systems which the College has in place.
- 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.

Network Activity

- Personal use of the computers is permitted, however people wishing to do school work must be given priority. Personal printing is not permitted without prior agreement from the College.
- 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.
- Users must not share their passwords with anyone else, nor must they log on as another person.
- Users must not attempt to bypass or disable the security which the College has in place.
- 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.
- Users must not deliberately cause damage of any nature to the computers, or do anything which they believe may be harmful in any way.

- 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.
- 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.

Safe Usage online

- **Don't post personal** information online, like your address, your email address or mobile number. Keep personal information as general as possible.
- **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.
- **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.
- **Remember**, not everyone online is who they say they are and grooming can occur without you realising it.
- **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.
- **Think** carefully about what you say before you write or post anything online.
- **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.
- **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.
- http://cybermentors.org.uk

Devices owned by the College may be assigned to staff or pupils 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.

Personal Devices and the use thereof is explained in a separate policy, namely Mobile Device Policy.

Technical Infrastructure

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.

Servers, wireless systems and cabling is securely located and physical access is restricted.

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.

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.

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.

Staff Awareness
All new members of staff receive information on the College E-Safety and Computer Usage Policy as part of their induction.

Teaching staff receive information about e-safety issues at staff meetings as and when required and as part of their regular safeguarding training updates.

The College has appointed an E-Safety Lead who works with the Deputy Head Pastoral to help ensure that staff awareness of, and training in, e-safety is current and appropriate.

Pupil Education and Information
All new pupils 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.

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

Data Protection
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.

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.

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 pupils out of College on a visit may be carried by accompanying members of staff.

Social Networking

The College recognises that staff and pupils 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 pupils, 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 pupils to promote e-safety.

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.

<u>Social Networking - DO</u>

1. Assume everything online is permanent and effectively public

2. Make sure you consider who might see anything you post

3. Write appropriately for your expected audience

4. Make all staff / pupil online interactions meaningful and professional

5. Consider specifically safety and reputation before posting online

6. Take responsibility for what you post / distribute online

7. Use the internet positively for communication, collaboration and learning

8. Use and maintain privacy settings to protect personal information but do not rely on them

<u>Social Networking - DON'TS</u>

1. Post anything which might damage your own or the college's reputation

2. Redistribute any material which may harm others in any way

3. Use the internet to form, or attempt to form, any relationship which would be otherwise inappropriate

4. Create an online environment which invites others to post harmful content

5. Post without thinking

6. Post without considering the safeguarding risks

7. Use screenshots to share private conversations between peers, content from lessons or for malicious reasons

Internet Site Filtering

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.

SonicWALL, 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 pupils further based on Year groups or Sections.

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.

Exceptions to the filtering are listed below:

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

Procedures for dealing with e-safety incidents involving pupils
If a pupil feels uncomfortable or worried by anything online or on a device, they should tell a member of staff or parent as soon as possible.

Any allegation, complaint, concern or suspicion that a pupil 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:

1. Possession of, or access/attempted access to a website containing, images of child abuse;
2. Possession of, or access/attempted access to a website containing, illegal (e.g. obscene or criminally racist) or terrorist or extremist material;
3. Any incident by electronic means involving 'grooming' behaviour;
4. Any other incident (which may include instances of cyber-bullying or 'sexting' or peer on peer abuse) that suggests that a pupil or another child has suffered or is at risk of suffering serious harm.

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 Deputy Head Pastoral. Such concerns will be managed in accordance with the College Behaviour Policy although referrals may be made to outside agencies as appropriate.

Any concern or allegation regarding 'sexting' (also known as 'youth produced sexual imagery') should be reported to the Deputy Head Pastoral or 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.

Any allegation of cyber-bullying which does not fall within point 4 above should be reported to the Deputy Head Pastoral 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.

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.

Procedures for dealing with e-safety incidents involving staff
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:

1. Possession of, or access/attempted access to a website containing, images of child abuse;
2. Possession of, or access/attempted access to a website containing, illegal (e.g. obscene or criminally racist) or terrorist or extremist material;
3. Any incident by electronic means involving 'grooming' behaviour;
4. Any other incident that suggests that a pupil or another child has suffered or is at risk of suffering serious harm from a member of staff.

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.

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.

Collecting and preserving evidence
If a member of staff suspects or is informed that there are indecent or obscene images of a pupil 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.

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.