ST FRANCIS SCHOOL

E-SAFETY POLICY (I6)

1.	**Background/Rationale**	
	1.1	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. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps with learning, together with teachers and pupils learning from each other. These technologies can stimulate discussion, promote creativity and increase awareness of content to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.
	1.2	The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This school's E-Safety Policy is aimed at helping to ensure safe and appropriate use.
	1.3	The use of these new technologies can put children and 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.
	1.4	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 school policies (e.g. Behaviour, Anti-Bullying and Child Protection policies).
	1.5	As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.
2.	**Development/Monitoring/Review of this Policy**	
	2.1	This E-Safety Policy has been developed and will be annually reviewed by the E-Safety Committee: • Head of Pastoral Care who is the School E-Safety Coordinator • Headmaster • ICT Network Manager • E-Safety Governor
3.	**Schedules for Development/Monitoring/Review**	
	3.1	This safety policy has been approved by the governing body.
	3.2	The Implementation of this E-Safety Policy will be monitored by the E-Safety Committee.
	3.3	The Governing Body will receive a report, at each termly Governors' meeting, on the implementation of the E-Safety Policy generated by the E-Safety Committee.

	3.4	Should serious e-safety incidents take place, the following external persons/agencies may be consulted where necessary: • Children's Social Care • Police
	3.5	The school will monitor the impact of the policy using: • Logs of reported incidents • The Network Manager will have access to each individual's internet activity (including sites visited) • Surveys/questionnaires of: pupils, parents/carers and staff
4.	**Scope of the Policy**	
	4.1	This policy applies to all members of the school community (including staff, pupils, volunteers, parents/ carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. The Policy also applies to use of personal devices and systems out of school where behaviour is inappropriate as per 4.2 below.
	4.2	The Education and Inspections Act 2006 empowers Heads, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
	4.3	The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.
5.	**Roles and Responsibilities**	
		The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:
	5.1	Governors: Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the E-Safety Governor receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include: • Regular meetings with the E-Safety Co-ordinator • Regular monitoring of e-safety incident logs • Reporting to relevant Governors committee/meeting
	5.2	Headmaster and SLT: • The Headmaster is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator. • The Headmaster/SLT are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant. • The Headmaster/SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. • The Headmaster and Deputy Head should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
	5.3	E-Safety Coordinator: The role of the E-Safety Coordinator (this role is currently overseen by the Deputy Head Pastoral): • Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents. • Liaises with the ICT Network Manager. • Liaises with other members of the SLT to discuss e-safety matters.

		• Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place. • Provides training and advice for staff. • Liaises with the IAPS and the Local Authority. • Receives reports of e-safety incidents and creates a log of incidents to inform future e- safety developments. • Meets regularly with the E-Safety Governor to discuss current issues and review incident logs. • Chairs E-Safety Committee Meetings each term.
	5.4	ICT Network Manager: The ICT Network Manager is responsible for ensuring that: • The school's ICT infrastructure is secure and is not open to misuse or malicious attack. • The school meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority and IAPS E-Safety Policy guidance. • Users may only access the school's networks through a properly enforced password protection procedure, in which passwords are regularly changed. • The E-Safety Coordinator and the Headmaster are informed of issues relating to the filtering of the internet. • The school's filtering is applied and checked on a regular basis by the Network Manager. However, all staff should also take responsibility to ensure that the children in their care are monitored when using the internet at all times and report any malfunction of the filtering system to the Network Manager. • The post holder keeps up to date with e-safety technical information in order to effectively carry out his/her e-safety role and to inform and update others as relevant. • The use of the network/remote access/email is regularly monitored in order that any misuse/ attempted misuse can be reported to the E-Safety Coordinator/Headmaster/Head of Pastoral Care. • The monitoring of software/systems are implemented and updated as agreed in school policies.
	5.5	Teaching and Support Staff: Teaching and support staff are responsible for ensuring that: • They have an up to date awareness of e-safety matters and of the current school E-Safety Policy and practices. • They have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP). • They report any suspected misuse or problem to the E-Safety Co-ordinator/Headmaster/Head of Pastoral Care. • Digital communications with pupils (email/voice) should be on a professional level and only carried out using official school systems. • E-Safety issues are embedded in all aspects of the curriculum and other school activities. • Pupils understand and follow the school e-safety and acceptable use policy. • Pupils have a good understanding of research skills and the need to avoid plagiarism and up hold copyright regulations. • They monitor ICT activity in lessons, extra-curricular and extended school activities. • They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices. • In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
	5.6	Designated Person for Child Protection/Child Protection Officer: Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from: • Sharing of personal data • Access to illegal/inappropriate materials • Inappropriate on-line contact with adults/strangers

		• Potential or actual incidents of grooming • Cyber-bullying
	5.7	Pupils: • Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they or their parents (KS1 only) will be expected to sign before being given access to school systems. • Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. • Will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying. • Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
	5.8	Parents/Carers: Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/ mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, information about national and local e-safety campaigns/literature. Parents and carers will be responsible for: • Endorsing (by signature) the Pupil Acceptable Use Policy (KS1 only) • Accessing the school website/pupil records in accordance with the relevant school Acceptable Use Policy.
6.	**Policy Statements**	
	6.1	Education – Pupils: Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways: • A planned e-safety programme should be provided as part of ICT/LFL/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. • Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/ pastoral activities. • Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information. • Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school. • Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. • Rules for use of ICT systems/internet will be posted in all rooms and online classrooms. • Staff should act as good role models in their use of ICT, the internet and mobile devices.

	6.2	Education – Parents/Carers: The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school. The school recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. The school will therefore aim to arrange discussion evenings for parents when an outside specialist advises about e-safety and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity. The school will also send out practical advice to parents with guidance from experts in the field of e-safety.
	6.3	Education & Training – Staff: It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: • A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. • All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies. • The E-Safety Coordinator/ Headmaster and Head of Pastoral Care will receive regular updates through attendance at IAPS/LA/other information/training sessions and by reviewing guidance documents released by IAP/SWGfL/LA and others. • This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/ INSET days. • The E-Safety Co-ordinator will provide advice/guidance/training as required to individuals as required.
	6.4	Training – Governors: Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in ICT/e-safety/health and safety/child protection. This may be offered in a number of ways: • Attendance at training provided by the Local Authority/National Governors Association/SWGfL or other relevant organisation, where applicable. • Participation in school training/information sessions for staff or parents. Technical – infrastructure/equipment, filtering and monitoring.
7.	**School Infrastructure**	
	7.1	The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities: • School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in this E-Safety Policy and Acceptable Usage Policy. • There will be regular reviews and audits of the safety and security of school ICT systems. • Servers, wireless systems and cabling must be securely located and physical access restricted. • The school maintains and supports a managed filtering service. • In the event of the ICT Network Manager/Headmaster needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headmaster and Network Manager. • Any filtering issues should be reported immediately to the ICT Network Manager. • Requests from staff for sites to be removed from the filtered list will be considered by the Headmaster and Network Manager. • The School ICT Network Manager regularly monitors and records the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.

		• An appropriate system is in place for users to report any actual/potential e-safety incident to the E-Safety Co-ordinator or Headmaster. • Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. • The school infrastructure and individual workstations are protected by up to date virus software. • Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
8.	**Curriculum**	
	8.1	E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum: • In lessons where internet use is pre-planned, it is best practice that students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. • Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit. • It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. • Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information. • Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
9.	**Use of internet and email**	
		Staff Staff must not access social networking sites, personal email, any website or personal email which is unconnected with school work or business from school devices or whilst teaching in front of pupils. Such access may only be made from staff members' own devices whilst in the staff room, personal offices or classrooms when children are not present. When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school. The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored. Staff must immediately report to the E-Safety Coordinator / IT Manager the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the e-Safety Coordinator / IT Manager. Any online communications must not either knowingly or recklessly: • place a child or young person at risk of harm, or cause actual harm; • bring St Francis into disrepute; • breach confidentiality; • breach copyright;

		• breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by: ● making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age; ● using social media to bully another individual; or ● posting links to or endorsing material which is discriminatory or offensive. Under no circumstances should school pupils or parents be added as social network 'friends' or contacted through social media. Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.
		Pupils VLE/Google Apps For Education All pupils have access to a VLE via Google Apps for Education. They use a combination of their own personal chromebook or school owned to access the @stfrancispewsey.org domain. They can also access this domain from their devices at home with the same level of monitoring and filtering at school. Goguardian is used to monitor the VLE and report any activity which is deemed inappropriate. There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, pupils should contact the Network Manager for assistance. Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to the E-Safety Coordinator (Deputy Head) / Network Manager / or another member of staff. The school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others. Pupils must report any accidental access to materials of a violent or sexual nature directly to the E-Safety Coordinator/Deputy Head / Network Manager / or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its wifi network is monitored. Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact the IT Manager for assistance.
10.	**Use of Digital and Video Images - Photographic, Video**	
		The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

		When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites). Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images. Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the Staff ICT Use Policy, EYFS Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes. Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Pupils must not take, use, share, publish or distribute images of others. Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website. Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
10.	**Data Protection**	
	10.1	Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be: • Fairly and lawfully processed • Processed for limited purposes • Adequate, relevant and not excessive • Accurate • Kept no longer than is necessary • Processed in accordance with the data subject's rights • Secure • Only transferred to others with adequate protection
	10.2	Staff must ensure that they: • At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse. • Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" or "locked" at the end of any session in which they are using personal data. • Transfer data using encryption and secure password protected devices.
	10.3	When personal data is stored on any portable computer system, USB stick or any other removable media: • The device must be password protected • The data must be securely deleted from the device; in line with school policy (below) once it has been transferred.

11.	**Unsuitable/Inappropriate activities**	
	11.1	St Francis will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the LSCB. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP. The school believes that the activities referred to in Appendix 1 would be inappropriate in a school context and those users should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as detailed in Appendix 1. Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures (in particular the Safeguarding Policy). The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.
12	**Links to other St Francis School Policies**	
	12.1	Child Protection Policy Anti-Bullying Policy Behaviour Policy Staff ICT Use Policy

Compiled by: KBB and E-Safety Committee	Created: May 2014	Responsibility: Deputy Head Pastoral
Reviewed by: 1. JNB Autumn 2022	Notes - a new e-safety policy is being developed after a thorough review using the SWGFL 360 review and will be ready by the end of Summer 2023.	Next revision: Autumn 2023

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					✓
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination					✓
	promotion of racial or religious hatred					✓
	threatening behaviour, including promotion of physical violence or mental harm					✓
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	

Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓	
On-line gaming (educational)			✓		
On-line gaming (non-educational)				✓	
On-line gambling				✓	
On-line shopping / commerce				✓	
File sharing				✓	
Use of social networking sites				✓	
Use of video broadcasting (YouTube) where not previously checked/saved/downloaded. Live viewing is not permitted				✓	

NB. A nominated user is an adult approved by the Headmaster.