St. John's Prep. & Senior School

Online Safety Policy

Last reviewed by the leadership team	Last reviewed by the advisory board
September 2018	November 2018

1. Introduction

St. John's Prep. and Senior school recognises that the internet, mobile and digital technologies provide a good opportunity for children and young people to learn, socialise and play, provided they are safe. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils and staff will be able to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in the safeguarding of children.

Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Coding

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

2. Responsibilities

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. To this end, the School maintains that students will have supervised access to Internet resources (where reasonable) through the schools fixed and mobile internet technology.

At St. John's Prep & Senior School, we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical

thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the School (such as PCs, laptops, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff brought onto School premises.

As e-Safety is an important aspect of strategic leadership within the school, the Head teachers have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The ICT Compliance Manager also has responsibility to oversee its implementation. They are to keep abreast of current issues and guidance through organisations such as Herts L.A., CEOP (Child Exploitation and Online Protection) and Childnet.
All breaches of this policy that may have put a child at risk must also be reported to the DSL.

3. Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

Outside Providers
PGL Travel Limited
321 Ski

We believe that it is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of School. We regularly consult and discuss e-Safety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

The School disseminates information to parents relating to e-Safety where appropriate in the form of:

- information and celebration evenings;
- website postings.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, GDPR, health and safety, home–school agreement, behaviour, anti-bullying, SMSC/RSE policies and the Staff Code of Conduct.

4. Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and all other visitors to the school.

Use of email

Staff should use a school email account for all official communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils may only use school approved accounts on the school system and only for educational purposes. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff and pupils should not open emails or attachments from suspect sources and should report their receipt to Paul Robinson, the school's Compliance Manager.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Head teacher with details of the site/service. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with pupils/families

Users must not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

    - Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)

- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

- Reveal or publicise confidential or proprietary information

- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses

- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school

- Use the school's hardware and Wi-Fi facilities for running a private business

- Intimidate, threaten or cause harm to others

- Access or interfere in any way with other users' accounts

- Use software or hardware that has been prohibited by the school

Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT Compliance Manager.

All deliberate breaches of prohibited behaviours detailed above will be investigated by the Head teacher and, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the Head teacher.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent is considered to be valid for the entire period the child attends this school,

although this can be changed by parents/carers at any time.

Photographs and images of pupils are only stored on the school's agreed secure networks. Rights of access to stored images are restricted to a limited range of staff. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Pupil's names will not be published alongside their image and vice-versa on the school website or any other school based publicity material.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices, but never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the Head teachers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Senior school pupils are allowed to bring personal mobile phones to school but must not use them for personal purposes within lesson time. In lesson times all such devices must be switched off. Under no circumstance should pupils use their personal mobile devices/phones to take images of

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

The school is not responsible for the loss, damage or theft on school premises of any personal mobile device.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment

before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with the Head teachers before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSL or the Head teacher. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

5. Data Security and Confidentiality

The accessing and appropriate use of School data is something that the School takes very seriously. The School follows government guidelines set out in the General Data Protection Regulations 2018.

All staff read and sign an Acceptable Use Agreement to demonstrate that they have understood the schools policy on Safe Use of the Internet and therefore, Staff are aware of their responsibility when accessing School data.

Data of a confidential nature, such as addresses, pending court cases or child protection issues, should not be accessed away from School premises.

Staff are not permitted to save any data regarding students' personal information on a USB or take any data off the School premises in the form of a hard copy unless they have been authorised by the Headteacher. Furthermore, staff are responsible for keeping the data safe whilst in School e.g. students' details are not left unattended at any time.

6. Infrastructure

Our School internet access is provided by Virgin Media and managed by a Cisco managed router.

The ICT Compliance Manager is responsible for regularly checking the websites viewed by both students and staff and the subsequently adding inappropriate keywords and websites to the filtering system.

- For example: Sites with pornographic content, sites that are considered to have extreme views and promote terrorism, any sites that are unsuitable for users under the age of 18.

St. John's Prep & Senior School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

Staff and pupils are aware that School based email and internet activity can be monitored and explored further if required.

If staff or pupils discover an unsuitable site, the screen will be switched off/ locked and the incident reported immediately to the ICT Technician (refer to flow chart at the end of this document).

It is the responsibility of the School, by delegation to the ICT Technician, to ensure that Anti-virus protection is installed and kept up-to-date on all School machines.

Pupils are unable to download programmes on to their computers by security settings.

7. Curriculum

Online safety is embedded within our curriculum. The school provides a comprehensive curriculum for online safety which enables pupils to become informed, safe and responsible.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. An external speaker from CEOP visits the school annually to speak at both sites about staying safe online. The school also has a framework for teaching e-Safety at both the Prep and the Senior School. The Prep school are taught during SMSC and ICT lessons and the Senior School pupils are taught e-Safety during their ICT lessons. Our School Counsellor, Anita Lonsdale, also reinforces the idea of e-Safety during her lessons at both schools. Curriculum work will also include:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity

- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment

- Developing critical thinking skills in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)

- Understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, school details, IM/email address) and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of

others

- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images
- What constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

Refer to the Computing policy for further information.

8. e-Safety skills development for staff:

Staff are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

- Child protection and E-Safety training completed by all staff on July 2018 and is due to be renewed in July 2019.
- Our staff receive regular information and training on E-Safety issues in the form of in house training and in staff meetings.
- New staff receive information on the School's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the School community.
- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas.

9. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides an annual meeting with a representative from CEOP for parents to update them with online safety information.

Parents/carers are asked on an annual basis to read, discuss and co-sign with each child the Acceptable Use Agreement. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities. The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe.

10. Webcams

The school uses CCTV for security and safety

We do not use publicly accessible webcams in school
Webcams in school are only ever used for specific learning purposes, for example, monitoring bird's nests; we never use images of children or adults.

11. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

12. e-Safety Officers:

The e-Safety officers are responsible for ensuring that the "Safe use of the internet" policy is followed by all members of staff, students and visitors. Furthermore, any e-Safety incident/concern should be reported to one of the e-Safety Officers.

Prep School:
Mrs. Tardios (Headteacher)
Mrs. Robinson-Farenden (Deputy Headteacher)
Mr. Robinson (ICT Compliance Manager)
Mr. Brandon (Head of Computing & CEOP Ambassador)

Senior School
Mr. Andrew Tardios (Headteacher)
Mr. Alexander Tardios (Deputy Headteacher)
Mr. Robinson (ICT Compliance Manager)

13. Appendices of the Online Safety Policy

A. Online safety acceptable use agreements for staff;
B. Online safety acceptable use agreements for pupils
C. Guidance on cyberbullying incidents for staff, parents and pupils
D. Guidance on negative comments on social media by parents, pupils, and staff
E. Online safety incident reporting form
F. Online safety incident log
G. Flowchart for managing E-Safety incidents
H. Sanctions and procedures following an E-Safety incident

14. Review & Monitoring

This policy will be reviewed every twelve months and consideration is given to the implications for future whole school planning. This policy will also be amended if new technologies are adopted of Central Government change the orders or guidance in any way.

Current Legislation

Acts relating to monitoring of staff email
Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The Telecommunications (Lawful Business Practice)
(Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to School activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to eSafety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust.

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Appendix A - Online Safety Acceptable Use Agreement - Staff

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the Head teachers. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Paul Robinson, Deputy Heads or the Head teachers.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Head teacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become ‘friends’ with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils. including former pupils who are also known to be ‘vulnerable’ young people up to the age of 25.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow requirements for data protection as outlined in GDPR policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the Head teacher
- Personal or sensitive data taken off site must be encrypted

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Head teacher.

I will not access secure school information from personal devices.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the Head teacher.

Promoting online safety

I understand that online safety is the responsibility of all staff and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, visitors, pupils or parents/carers) to a member of the DSL.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.
If I am using the internet to teach about controversial issues I will secure, on every occasion, approval

in advance for the material I plan to use with the Head teacher.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment.

Signature ……..…….…… Date ……

Full Name ……..... (printed)

Job title ……

Appendix B - Acceptable Use Agreement: Pupils – E-Safety Rules

- ✓ I will only use ICT in School for School purposes.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible. I will be kind and respectful at all times.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone offline.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of School staff is concerned about my E-Safety.
- ✓ I will ensure that my online activity including the use of social media/networking sites, both in School and outside School, will adhere to the School rules.
- ✓ I will ensure that I do not use a mobile device to cyber bully, take inappropriate images or send inappropriate images.

Dear Parent/ Carer

ICT including the internet, email and mobile technologies, etc has become an important part of learning in our School. We expect all children to be safe and responsible when using any ICT.

The School is proud of its high standards and ethos. The internet and social media should not be used to share complaints about the School. When negative or inaccurate comments online are drawn to our attention, we will invite the person to discuss their concerns with the School by following our complaints procedure. Where this is not possible, the School will take legal action to remove defamatory or libellous remarks, particularly where individuals at the School are named.

Please read and discuss these E-Safety rules with your child and sign the bottom of the page. If you have any concerns or would like some explanation please contact the ICT Department.

We have discussed this and …….....(child's name) agrees to

follow the E-Safety rules and to support the safe use of ICT at St. John's School.

Parent/ Guardian Signature ……

Class …… Date ……

Form Teacher ……

Appendix C - Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, Head teacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the Head teacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix D - Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

  As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

  If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the head teacher will need to follow the school's safeguarding procedures.

  If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

  Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

  Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

  The meeting must:

  - Draw attention to the seriousness and impact of the actions/postings;
  - Ask for the offending remarks to be removed;
  - Explore the complainant's grievance;
  - Agree next steps;
  - Clarify the correct complaints procedures.

  If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;

- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

Appendix E - Online safety incident reporting form

Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to a member of the DSL.

Name of person reporting incident:				
Signature:				
Date you are completing this form:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young people	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of acceptable use agreement, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence available but do not attach.

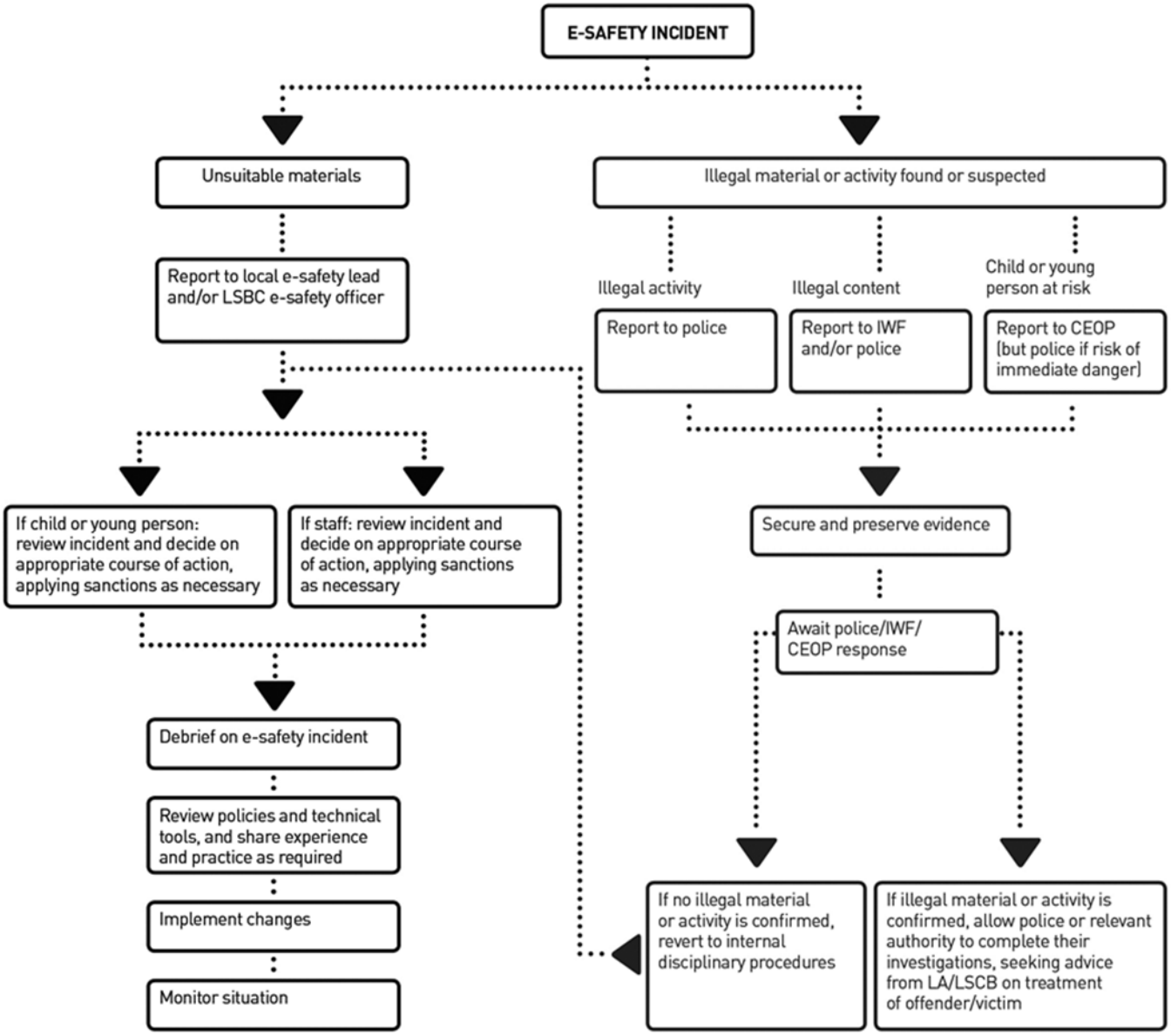
Thank you for completing and submitting this form.

Appendix F - Online safety incident log

Summary details of ALL online safety incidents will be recorded on this form by the online safety coordinator or other designated member of staff. This incident log will be monitored at least termly and information reported to both Head teachers.

Date & time	Name of pupil or staff member Indicate target (T) or offender (O)	Nature of incident(s)	Details of incident (including evidence)	Outcome including action taken

Appendix G – Flowchart for Managing an E-Safety Incident



Taken from 'AUPs in Context' BECTA (2009)

Local Authority Safeguarding Team 0208 379 5555

Police (Non-emergency) 101

Professionals' Online Helpline (Office Hours only) 0844 381 4772

Child Exploitation and Online Protection (CEOP)(Office Hours only) .. 0870 000 3344

Appendix H – Sanctions and Procedure following an E-Safety incident:

The School believes that the activities referred to in the following section would be unacceptable in a School context and that the users should not engage in these activities in the School or when using School equipment or systems. The head teacher will use his/her discretion when sanctioning both students and staff, taking into account the user's previous transgressions.

User Actions		Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or make 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.		✓
	criminally racist material.		✓
	pornography.	✓	
	promotion of any kind of discrimination.	✓	
	promotion of any 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.		✓	
Revealing or publishing confidential or proprietary information (e.g. financial/ personal information, databases, computer/network access codes ad passwords).		✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.		✓	
Creating or propagating computer viruses or other harmful files.		✓	

Incidents	Warning	Inform Form Teacher and Head Teacher	Refer to member of ICT staff	Inform parents or guardians	Further sanction e.g. detention or exclusion	Refer to police
Deliberately accessing or trying to access material that could be considered illegal (see list on previous page).		✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons.	✓		✓			
Receipt or transmission of materials that infringes the copyright of another person or infringes the Data Protection act.	✓		✓			
Unauthorised use of social networking, instant messaging or personal emails.	✓		✓			
Unauthorised use of social networking, instant messaging or personal emails containing abuse/swearing.		✓	✓	✓	✓	
Unauthorised downloading or uploading of files.		✓	✓	✓	✓	
Allowing others to access School network by sharing username and passwords.		✓				
Attempting to access or accessing the School network using another student's account.		✓	✓		✓	
Attempting to access or accessing the School network using a member of staffs account.		✓	✓	✓	✓	
Corrupting or destroying the data of other users.		✓	✓	✓	✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature.		✓	✓	✓	✓	
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School.		✓	✓	✓	✓	
Using proxy sites or other means to subvert the Schools' filtering system.		✓	✓	✓	✓	
Accidentally accessing offensive or pornographic material and failing to report it.			✓			
Deliberately accessing or trying to access offensive or pornographic material.		✓	✓	✓	✓	
Deliberately attempting to access protected areas of the School network (hacking).		✓	✓	✓	✓	

All incidents must be logged in the E-Safety Incident Log and the Behaviour Log.

The above is the Schools' general position. However, management of the School, led by the headmaster reserve the right to step away from the strict application of the procedure if the particular circumstances so require.