



St John's Online Safety Policy

This policy will ensure that children, young people, staff and volunteers are able to use the internet and related communications technologies appropriately and safely and remain safe and protected from potential harm, both within and outside of their educational setting.

Reviewed by the Governing Body of St John's CofE VC Infants

Chair of Governors ...Jim Gurl.....

Date09/24.....

Proposed Date of Future Review.....09/26.....

Contents Page

- 1. Policy Development**
- 2. Scope of the Policy**
- 3. Roles and Responsibilities**
- 4. Policy Statements**
 - **Education - Pupils**
 - **Education - Parents/ Carers**
 - **Education - Wider Community**
 - **Education & Training - Staff and Volunteers**
 - **Training - Governors**
- 5. Technical – infrastructure, equipment, filtering and monitoring**
- 6. Mobile Technologies**
- 7. Aspects that the school will consider when reviewing the Online Safety Policy, Mobile Technologies Policy and Acceptable Use Agreements**
- 8. Use of digital and video images**
- 9. Data Protection**
- 10. Communications**
- 11. Social Media - Protecting Professional Identity**
- 12. Monitoring of Public Social Media**
- 13. Unsuitable / inappropriate activities**
- 14. Responding to incidents of misuse**
- 15. Illegal Incidents**
- 16. Other Incidents**
- 17. School Actions & Sanctions**
- 18. Schedule for Development / Monitoring / Review**

Appendices:

1. Acceptable Use Policy for Internet and E-mail – Staff and volunteers
2. Acceptable Use Policy for Internet and E-mail – Pupil
3. Parent / Carer Acceptable Use Agreement for pupils
4. Use of Digital Images
5. Responding to incidents of misuse
6. Record or reviewing devices/ internet sites
7. Record of Incident Form
8. Training Needs Audit
9. Privacy Notice
10. Legislation
11. Links to other organisations and documents
12. Glossary

1. Policy Development

This Online Safety policy has been developed by a working party made up of:

- Head teacher
- Computing Lead
- Staff – including Teachers, Support Staff, Technical staff
- Governors

2. Scope of the Policy

This policy applies to all members of the school community, including staff, pupils, volunteers, parents/carers and visitors.

The Education and Inspections Act 2006 empowers Head teachers 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 Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to St John's School pupils. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 Online Safety behaviour.

3. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. The governors will receive regular information about online safety incidents and monitoring reports. The member of the Governing Body responsible for safeguarding has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs

- reporting to relevant Governors and Committee meetings

Head teacher and Senior Leaders:

- The Head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Head teacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Head teacher is responsible for ensuring that other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head teacher will ensure that there is a system in place to allow for monitoring and support of those who carry out the internal online safety monitoring role, when not performed by herself. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant bodies

Online Safety Co-ordinator (Headteacher):

The Online Safety Co-ordinator:

- liaises with the network manager as appropriate
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- reports to relevant committee of Governors
- feedbacks regularly to Senior Leadership Team, school staff, pupils and parents and carers and other school stakeholders

Network Manager (Computing Cubed):

The Network Manager is responsible for ensuring that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets required online safety technical requirements and any Local Authority Online Safety Policy and guidance that may apply.
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of the network, internet, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Head teacher for investigation, action and sanction.
- monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the head teacher or Online Safety co-ordinator for investigation, action and sanction
- all digital communications with pupils, parents and carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- they need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where permitted) and implement current 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

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding 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

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- need to begin 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking and use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website information and information about national or local online safety campaigns and related literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- their use of personal devices in the school

Visitors

Visitors are not permitted to use the school wifi for security reasons and are not given access.

4. Policy Statements

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 online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside of the school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- Where internet use is pre-planned, it is best practice that 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, staff should be vigilant in

monitoring the content of the websites the young people visit.

Education – Parents / Carers

Parents and carers play an essential role in the education of their children and in the monitoring and regulation of their children's on-line behaviours. Parents can underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters and newsletters
- The Online Safety section of the school website
- Parent and Carers information evenings and workshop sessions
- High profile events and links to campaigns e.g. Safer Internet Day
- Reference to relevant web sites and publications e.g. swgfl.org.uk
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

Education – The Wider Community

The school will provide opportunities for members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents/carers.
- The school website which provides relevant online safety information for the wider community
- Advice and guidance to any additional community groups in order to enhance their Online Safety provision

Education & Training – Staff and Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements.
- Staff can identify online safety as a training need within the performance management process.
- The Headteacher and Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff during appropriate staff meetings and training days.
- The Headteacher and Online Safety Coordinator will provide advice, support, guidance and training to individuals as required.

Training - Governors

Governors should take part in online safety training and awareness sessions, with particular importance for those who are members of any committees involved in technology, online safety, health and safety and/ or safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority Governors Association or other relevant organisation (e.g. SWGfL).
- Participation in any school training and information sessions for staff or parents, which could include attendance at assemblies or within lessons.

5. Technical - infrastructure, equipment, filtering and monitoring

The school staff will be responsible for ensuring that the infrastructure and 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 online safety responsibilities:

School technical systems will be managed in ways that ensure the school meets recommended technical requirements

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.

- All staff users will be provided with a username and secure password by the network manager who will keep an up to date record of users. Users are responsible for the security of their username and password and will be required to change when prompted monthly
- The administrator passwords for the school ICT system, used by the Network Manager must also be available to the School Business Manager and kept in a secure place.
- The Network Manager is responsible for ensuring that online/ software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software/online installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider SMOOTHWALL by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The Network Manager regularly monitors and ensures the safe activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate log book is in place for users to report any actual or potential technical incident, security breach to the network manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, wireless devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed procedure is in place that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed procedure is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the site unless safely encrypted or otherwise secured.

6. Mobile Technologies

Mobile technology devices may be school owned and provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network.

All users should understand that the primary purpose of the use mobile / personal devices in an school context is educational. Mobile technologies guidelines are consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's wider Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils, parents and carers gives consideration to the use of mobile technologies

The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device ¹	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	N/A	No ²	Yes	Yes
Full network access	Yes	Yes – laptops	N/A	N/A	No	No
Internet only	HT phone only	Yes – I pads/ HT tablet	N/A	N/A	yes	no
No network access			N/A	N/A	Yes	Yes

7. Aspects that the school will consider when reviewing the Online Safety Policy, Mobile Technologies Policy and Acceptable Use Agreements

a. For school owned and provided devices, the school will consider:

- Who they will be allocated to
- If personal use is allowed for work related tasks
- Levels of access to networks / internet (as above)
- Management of devices / installation of apps / changing of settings / monitoring
- Network / broadband capacity
- Technical support
- Filtering of devices
- Access to cloud services
- Data Protection
- Taking / storage / use of images

¹ Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

² The school should add below any specific requirements about the use of mobile / personal devices in school

- Exit processes – what happens to devices / software / apps / stored data if user leaves the school
- Liability for damage
- Staff training

b. For personal devices, the school will consider:

- Which users are allowed to use personal mobile devices in school (staff / volunteers/ visitors)
- Restrictions on where, when and how they may be used in school
- Storage
- Whether staff will be allowed to use personal devices for school business
- Levels of access to networks / internet (as above)
- Network / broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection
- The right to take, examine and search user's devices in the case of misuse (England only) – n.b. this must also be included in the Behaviour Policy.

- Taking / storage / use of images
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification / labelling of personal devices
- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school Online Safety education programmes.

8. Use of digital and video images

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 or 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 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. It is common for employers to carry out internet searches for information about potential and

existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, social media or local press.
- To respect everyone's privacy and in some cases protection, images of school events involving children should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers (with parental permission) are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff 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 without their permission
- Photographs published on the website, or 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.

9. Data Protection

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.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.

Staff must ensure that they:

- At all times take care to ensure the safe keeping 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” at the end of any session in which they are using personal data.
- Transfer data using secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff		Allowed		Allowed with staff permission	Not allowed
Communication Technologies								

Mobile phones may be brought to the school / school								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on mobile phones								
Taking photos on school cameras / I pads								
Use of other mobile devices e.g. tablets, gaming devices								
Use of personal email addresses in school or on school network								
Use of school / school email for personal emails								

Use of messaging apps								
Use of social media								
Use of blogs								

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with school policy, 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.
- Any digital communication between staff and parents / carers (email, Class Dojo, social media etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

11.Social Media - Protecting Professional Identity

All academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Providing training including: acceptable use; social media risks; checking of settings;

data protection; reporting issues.

- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents, carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in the school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

12. Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the Headteacher to ensure compliance with school policies.

13. Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school / school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978				X

communicate or pass on, material, remarks,	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	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				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / school				X	
	Infringing copyright				X	
	Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
	Creating or propagating computer viruses or other harmful files				X	
	Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
	On-line gaming (educational)		x			
	On-line gaming (non-educational)				x	

On-line gambling				X	
On-line shopping / commerce (adult)		X			
File sharing (adult)			X		

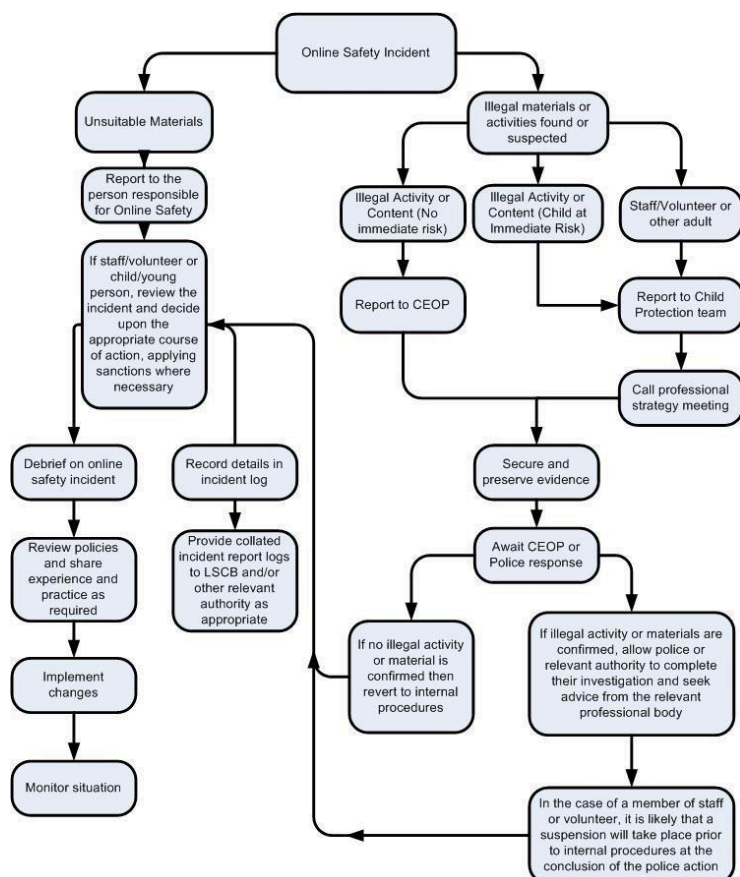
Use of social media (adult)		X			
Use of messaging apps (adult)		X			
Use of video broadcasting e.g. Youtube (adult)		X			

14. Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

15. Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately.



16. Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority / School Group or national / local organisation (as relevant).
 - Police involvement and/or action
- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism

- o other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

17.School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with

18. Schedule for Development / Monitoring / Review

The implementation of this Online Safety policy will be monitored by the Online Safety Coordinator and Online Safety group. Monitoring will take place at regular intervals.

The Governors Wellbeing Committee will receive a report on the implementation of the Online Safety Policy generated by the monitoring group, which will include anonymous details of online safety incidents annually.

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Should serious online safety incidents take place, the following external persons / agencies should be informed: LADO and the police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity

- Surveys / questionnaires of
 - students / pupils
 - parents / carers
 - staff

Appendices

1. Acceptable Use Policy for Internet and E-mail – Staff and volunteers
2. Acceptable Use Policy for Internet and E-mail – Pupil
3. Parent / Carer Acceptable Use Agreement for pupils
4. Use of Digital Images
5. Responding to incidents of misuse
6. Record or reviewing devices/ internet sites
7. Record of Incident Form
8. Training Needs Audit
9. Privacy Notice...
10. Legislation
11. Links to other organisations and documents
12. Glossary

St John's Infants School Staff (and Volunteer)

Acceptable Use Policy

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 information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, iPads etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so.
- I will not use chat and social networking sites in school.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

St John's School

Acceptable Use Policy for Internet and Email for Pupils

Digital technologies have become integral to the lives of children and young people, both inside and outside of the school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Guidelines:

1. Pupils must obtain the permission of parent(s)/guardian(s) before they can be allowed to use the Internet or education email service. The Parental Permission Form must be signed and returned to the school.
2. Pupils should only use the school computer systems for those activities and services (Internet and Email), which they have been given permission to use.
3. Pupils must only use the school computers with the permission and under the supervision of a member of staff.
4. Activities which use the Internet during taught lessons will be directly related to school work. Use of the Internet outside of taught lessons is at the discretion of a member of staff who will set guidelines and rules for its use.
5. Pupils must only use the user name and password that they have been given.
6. Pupils should not download and use material or copy and paste content which is copyright. Most sites will allow the use of published materials for educational use. Teachers will give guidelines on how and when pupils should.

7. The Internet access provided in Somerset primary academies is filtered to stop access to unsuitable material. As no filtering system can be 100% effective, it is important that parents are aware that users of the system are required to act responsibly. Under no circumstances should pupils attempt to view, upload or download any material that is likely to be unsuitable for children or the school. Pupils have a responsibility to inform the member of staff supervising them if they have accidentally accessed inappropriate content.
8. Pupils will be taught to respect the privacy of files of other users. They will be taught not to enter, or attempt to enter without permission, the file areas of other pupils or staff.
9. Parents are asked to explain the importance to their child of these rules for the safe use of the Internet and to sign and return to the school the Parental Permission Form. No disks from home can be used on systems in school unless they have been virus scanned.

Failure to comply with these rules will result in one or more of the following:

- A ban, temporary or permanent, on the use of the Internet at school.
- A letter informing parents of the nature and breach of rules.
- Appropriate sanctions and restrictions placed on future access to school facilities to be decided by the school.

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both inside and outside of the school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents and carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Parent / Carer Permission Form

Parent / Carers Name: _____

Pupil Name: _____

As the parent / carer of the above pupils, I give permission for my son / daughter to have access to the internet and to ICT systems across the school.

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of their educational setting.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet

and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: _____

Date: _____

Digital Images Policy and Guidance

(with reference to Somerset Council Media Guidelines)

School guidance for the taking, displaying and publication of child images

The term 'images' includes photographs, digital photographs, film, webcam/video conferencing, CCTV and mobile/camera phones

The school believes that the responsible use of children's images can make a valuable contribution to the life and morale of the school. The use of photographs in school publicity materials can increase a child's motivation and help parents and the local community identify and celebrate the school's achievements.

The school will only use images that the Headteacher and Governing Body consider suitable and which appropriately represent the values of the school and the range of activities the school provides.

The policy is intended to minimise the risks that young people can be exposed to through the misuse of images. The policy takes account of data protection and child protection issues.

Data Protection

- Photographs and video images of children and staff are classed as personal data under the terms of the Data Protection Act 1998.
- We will not use images of either identifiable individual, for school materials without the consent of the individual or, in the case of children, their parents/carers.
- Images will be kept securely and held by the school for the duration of the child's time there, after which they will be destroyed.

Consent to take images

- Written permission from parents or carers will be obtained before images of children are taken for any purpose
- Written parental consent will be sought to use photographs for professional, marketing and training purposes
- Parental permission will be sought on admission, and then on an annual basis thereafter
- A record of all consent details will be kept securely on file
- Permission can be withdrawn by parents/carers at any time, and for particular events and in retrospect. All relevant images will be removed and disposed of and the record will be updated accordingly

Taking Images

- Only official school owned equipment will be used to capture images of children for official purposes
- Members of staff will model positive behaviour to the children by asking permission before they take any photos

- Careful consideration will be in place before taking photos or recordings of very young or vulnerable children
- Images will not be taken of any child against their wishes - a child's right not to be photographed is to be respected
- Photography is not permitted in sensitive areas such as changing room, toilets, swimming areas etc
- The school will only use images of children who are appropriately dressed
- The Headteacher reserves the right to view any images and to withdraw a member of staff's authorisation to take images

Storing Images

- All images will be securely stored with encryption enabled on removable devices including laptops, tablets, cameras, USB memory sticks etc where possible with images immediately transferred to secure or encrypted areas if this is not possible
- Photographs will be deleted when the child leaves the school

Use of Images

- Images or videos will be selected carefully when used
- Images of children's work will only be published with their permission and their parents' consent
- Staff should check if they have permission to use the images for the purpose intended
- Children's' first names will only be used on images

Training and procedures

- Staff will receive information regarding the safe and appropriate use of images as part of their safeguarding training and responsibilities
- All members of staff will ensure that all images are available for scrutiny and will be able to justify any images in their possession
- Any apps, websites or third party companies used to share, host or access children's images will be risk assessed prior to use. The school will ensure that images are held in accordance with the Data Protection Act and suitable child protection requirements are in place

Images for School publications

- The school will only take and use images that are appropriate and are considered not to be open to misuse.
- Children will be made aware of why their picture is being taken and how it will be used
- Where possible, photos will be taken of groups of children rather than individuals.
- Where a photograph of an individual is used, we will not name the child.
- Where the child is named, we will not use their photograph.
- Images will show children in appropriate dress. The Headteacher and Governing Body retain responsibility for all published materials relating to the school and will use their professional discretion to monitor and remove inappropriate photographs.
- We will ensure that personal details are not used in captions, tags or file names

Images for the internet e.g. school website, Instagram and Facebook page

- We will adopt the same principle as outlined above when publishing images on the Internet. However, the school recognises that there is no control over who may view the images and consequently there is a greater risk of misuse of the images, via the Internet.
- We will therefore give specific consideration to the suitability of images for use on the school's website, Instagram or Facebook pages.
- Where possible, photos will be taken of groups of children rather than individuals.
- Where a photograph of an individual is used, we will not name the child.
- Where the child is named, we will not use their photograph.
- Images will show children in appropriate dress. The Headteacher and Governing Body retain responsibility for all materials relating to the school and will use their professional discretion to monitor and remove inappropriate photographs.
- We will ensure that personal details are not used in captions, tags or file names

Filming

- Under the terms of the Data Protection Act 1998, parents, friends and family members can take images of their children and friends participating in school activities for family and personal use.
- If the recording is not for personal use e.g. with a view to selling the video, then consent of other parents whose children may be on film would be required. Without this consent, the Data Protection Act would be breached.
- Parents are allowed to film school events such as sports days, fetes and plays so long as the performance is not disturbed.

Webcams/Video conferencing

- Webcams and video conferencing facilities are useful tools for learning. They can allow individuals to interact over the Internet with others, and support links between pupils in different schools, countries and cultures.
- A webcam will only be used in appropriate circumstances such as a normal class setting.
- Both children and teachers will be made aware of when a webcam is in use.

CCTV

- The school may use CCTV in some areas as a security measure. Cameras will only be used in appropriate areas and where there is clear signage indicating where in operation.
- CCTV images that are stored on digitally will only be stored for designated periods then erased.

Mobile / camera phones

- Mobile and camera phones can take images without the knowledge of others. As such, mobile phones that can take and transmit images will not be permitted in class or communal areas. Staff may only use mobile phones in designated staff areas at appropriate times. Visitors are asked to refrain from using their mobiles during their

time at the school, unless they are given specific instruction to use them, e.g. to take pictures/video at an school performance. All staff, parents and visitors of the school will be asked to abide by the acceptable use policy.

Media / Local press

- Photographs taken by journalists are exempt from the Data Protection Act as newspapers are subject to strict guidelines governing the press.
- The school will ensure that it politely checks that broadcasters and press who may be on the school premises are aware of the sensitivity involved in captioning, interviews and close or sports photography.
- A child's name is never given to the press without prior parental consent.

Consent

- Due to the number of occasions during a child's time at school that the school may wish to photograph or video the child, the school will seek consent from parents/carers when the child starts at the school. This policy and consent will cover the whole of the child's time at the school.
- The school will, at all times, consider the need to revisit consent in the event of a child's circumstances changing, or new applications for the use of images.

Misuse of images

Any evidence of the use of inappropriate images, or the misuse of images, will be reported to the school's designated child protection officer who may involve the LA, Social Services and police as appropriate.

Model Consent letter for the taking, displaying and publication of child images

Dear Parents and Carers,

There have been rapid changes in the technology of image reproduction. Taking and publishing pictures is now easy, and schools need to be mindful of their responsibility to monitor and control images of children.

Our school has a duty of care to provide a safe environment for our children. While we are aware of the risks of image misuse and the right of individuals to privacy, we believe that the school needs to balance this against positive value of professional, high quality images of children in celebrating and promoting the school as an enjoyable, vibrant place to learn. Good pictures of the school and its children can help in putting the school at the heart of the local community and enhance its reputation.

Please find enclosed a copy of the school's policy on the taking, displaying and publishing of child images and two copies of the consent form.

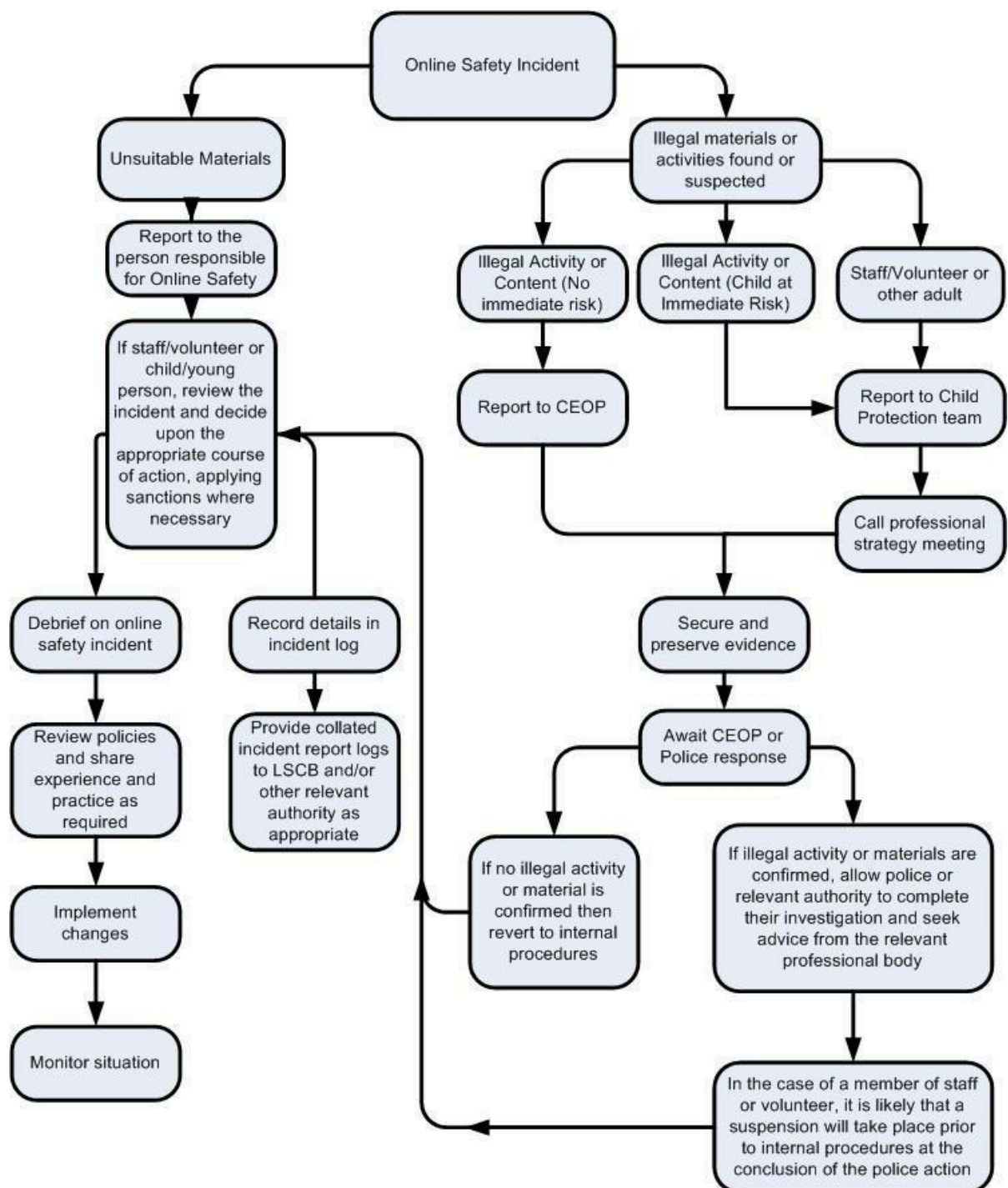
The measures in this policy are designed to ensure that the school does everything it can reasonably be expected to do to protect children from the potential harm that the misuse of images could cause.

Please read the policy carefully and fully. Sign one copy of the form and return it to the school to indicate that you agree with the school's policy and consent to images of your child being taken and published in school material. Sign and keep the second copy for your own reference as a reminder of our shared responsibility for the safety of all children at the school.

If for any reason during your child's time at the school you wish to withdraw your consent, please inform us as soon as possible.

Yours sincerely,

Headteacher



Responding to incidents of misuse - flow chart

PRIVACY NOTICE

Privacy Notice - Data Protection Act 1998

We **St John's School** are a data controller for the purposes of the Data Protection Act. We collect information on pupils and parents and/or carers, and may receive information about pupils and parents and/or carers from previous schools and the Learning Records Service. We hold this personal data and use it to:

- support our pupils' teaching and learning;
- monitor and report on their progress;
- provide appropriate pastoral care;
- communicate with parents and carers; and
- assess the quality of our services.

This information includes their contact details, national curriculum assessment results, attendance information³ and personal characteristics such as their ethnic group, any special educational needs and relevant medical information.

We will not give information about our pupils to anyone outside the school without your consent unless the law and our policies permit it. If you want to see a copy of the information about your son/daughter that we hold, please contact the School Office.

We are required by law to pass some information about our pupils to the Department for Education (DfE) and, in turn, this will be made available for use by the Local Authority.

DfE may also share pupil level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998.

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to pupil level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit:

<https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract>

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

³ Attendance information is not collected as part of the Censuses for the Department for Education for

the following pupils / children - those aged under 4 years in Maintained schools and those in Alternative Provision and Early Years Settings.

If you need more information about how our local authority and/or DfE collect and use pupil information, please visit:

- our local authority at <http://www.somerset.gov.uk/accessing-our-information/privacy-policy/>; or
- the DfE website at <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

The Information Governance Team
Communications Division
Somerset County Council

County Hall
Taunton
TA1 4DY

Email: Informationgovernance@somerset.gov.uk
<https://www.gov.uk/contact-dfe>

Website: www.somerset.gov.uk

Phone: 0300 123 2224

Ministerial and Public

Department for Education

Piccadilly Gate
Store Street

Manchester M1 2WD

Contact form:

Website: www.education.gov.uk

Phone: 0370 000 2288

Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;

- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes 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.

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.

Protection of Children Act 1978

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

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. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance

-

[http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation\)](http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires school's to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires school's to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

UK Safer Internet Centre

Safer Internet Centre – <http://saferinternet.org.uk/>

South West Grid for Learning – <http://swgfl.org.uk/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline – <http://www.saferinternet.org.uk/about/helpline>

Internet Watch Foundation – <https://www.iwf.org.uk/>

CEOP

CEOP – <http://ceop.police.uk/>

ThinkUKnow – <https://www.thinkuknow.co.uk/>

Others

INSAFE – <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

UK Council for Child Internet Safety (UKCCIS) – www.education.gov.uk/ukccis

Netsmartz – <http://www.netsmartz.org/>

Tools for Schools

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

Bullying / Cyberbullying

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) – <http://enable.eun.org/>

Scottish Anti-Bullying Service, Respectme – <http://www.respectme.org.uk/>

Scottish Government – Better relationships, better learning, better behaviour –

<http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE – Cyberbullying guidance –

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) –

<http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work>

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

Social Networking

Digizen – [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

SWGfL - Facebook - [Managing risk for staff and volunteers working with children and young people](#)

[Connectsafely Parents Guide to Facebook](#)

[Facebook Guide for Educators](#)

Curriculum

[SWGfL Digital Literacy & Citizenship curriculum](#)

Glow - <http://www.educationscotland.gov.uk/usingglowandict/>

Teach Today - www.teachtoday.eu/

Insafe - [Education Resources](#)

Mobile Devices / BYOD

Cloudlearn Report [Effective practice for schools moving to end locking and blocking](#) NEN
- [Guidance Note - BYOD](#)

Data Protection

Information Commissioners Office:

[Your rights to your information – Resources for Schools - ICO](#)

[Guide to Data Protection Act - Information Commissioners Office](#)

[Guide to the Freedom of Information Act - Information Commissioners Office](#)

[ICO guidance on the Freedom of Information Model Publication Scheme](#)

[ICO Freedom of Information Model Publication Scheme Template for schools \(England\) ICO](#)
- [Guidance we gave to schools - September 2012](#) (England)

[ICO Guidance on Bring Your Own Device](#)

[ICO Guidance on Cloud Hosted Services](#)

[Information Commissioners Office good practice note on taking photos in schools](#)

[ICO Guidance Data Protection Practical Guide to IT Security](#)

[ICO – Think Privacy Toolkit](#)

[ICO – Personal Information Online – Code of Practice](#)

[ICO Subject Access Code of Practice](#)

[ICO – Guidance on Data Security Breach Management](#)

SWGfL - [Guidance for Schools on Cloud Hosted Services](#)

LGfL - [Data Handling Compliance Check List](#)

Somerset - [Flowchart on Storage of Personal Data](#)

NEN - [Guidance Note - Protecting School Data](#)

Professional Standards / Staff Training

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

[Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs](#)

[Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure / Technical Support

Somerset - [Questions for Technical Support](#)

NEN - [Guidance Note - esecurity](#)

Working with parents and carers

[SWGfL Digital Literacy & Citizenship curriculum](#)

[Online Safety BOOST Presentations - parent's presentation](#)

[Connectsafely Parents Guide to Facebook](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops / education](#)

[The Digital Universe of Your Children - animated videos for parents \(Insafe\)](#)

[Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide](#)

[Insafe - A guide for parents - education and the new media](#)

[The Cybersmile Foundation \(cyberbullying\) - advice for parents](#)

Research

[EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)

[Futurelab - "Digital participation - its not chalk and talk any more!"](#)

[Ofcom - Children & Parents - media use and attitudes report - 2015](#)

Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)

SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.