Online Safety Policy

St John's School
LEATHERHEAD

Date of issue:	September 2021
Next review:	June 2022
Responsible persons:	Deputy Head (Pastoral) and DSL
References:	Safeguarding and Protecting Children Policy and Procedures (7a8a) Staff Conduct Policy (7e) Pupil handbook and Acceptable Use Policy Anti-bullying Policy (10a) Behaviour, Rewards, Sanctions and Discipline (9a) Keeping Children Safe in Education September 2021 Sexual violence and sexual harassment between children in schools and colleges, September 2021 Sharing nudes and semi-nudes: advice for education settings (UKCIS, December 2020) Revised Prevent duty guidance (April 2021)
Appendix 1:	Acceptable, unacceptable and illegal activities
Policy number:	7h

1. Introduction

It is essential that children are safeguarded from potentially harmful and inappropriate online material. St John's School has an effective whole school approach to online safety, to protect and educate the whole community about the use of technology. This policy also sets out the mechanisms whereby school staff will identify, intervene in and escalate online safety concerns, where appropriate.

Children increasingly use electronic equipment on a daily basis to access the internet, share and view content and images via social media, gaming and communication platforms/sites. This policy applies to all members of the School community (including staff, pupils, governors, volunteers, parents/carers, visitors, community users) and to all devices that have the capacity to connect to the internet and transfer data (including but not limited to mobile phones, smart watches, laptops etc.)

Children are taught about online safety throughout the curriculum and all staff receive online safety training which is regularly updated. The Assistant Head (Digital Strategy) and online safety co-ordinator is Mark Sartorius.

The School's Governing Council will do 'all that they reasonably can' to limit children's exposure to harmful and inappropriate online material, with appropriate filters and monitoring systems in place, to safeguard staff and pupils.
The School will monitor the impact of this policy using:

- Logs of reported incidents
- Logs of internet activity (including sites visited)
- Internal data for network activity
- Surveys / questionnaires of pupils, parents / carers and staff

2. Development, Monitoring and Review of this Policy

The implementation of this Online Safety policy will be monitored by the Deputy Head (Pastoral), DSL, Assistant Head (Digital Strategy) and the IT Strategic Management Group (ITSMG).

The Deputy Head (Pastoral), DSL and Assistant Head (Digital Strategy) are responsible for the annual review of the School's approach to online safety, supported by an annual risk assessment that considers and reflects the risks our children face, which will inform policy and curriculum improvement.

The School's Governing Council will receive a report on the implementation of the Online Safety Policy as part of the annual review of safeguarding.

Should serious online safety incidents take place, the following persons / agencies should be informed: The Head, Senior Deputy Head, Deputy Head (Pastoral), Designated Safeguarding Lead and Nominated Safeguarding Governors. They will determine the course of action to be taken. If the issue involves safeguarding concerns, then the School's Safeguarding policy will be followed in order to determine whether to inform external persons/agencies. Reviews of serious incidents will inform improvements to policy and practice.

3. Roles and Responsibilities

3.1 The Governing Council

The Governing Council has overall legal responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn. The Governors will ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding, including online safety, that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

The Lead Governor for Safeguarding (Angela Wright) meets regularly with the Designated Safeguarding Lead and Deputy Head (Pastoral) and the Lead Governor for Safeguarding reports back to Governing Council as appropriate.

3.2 The Head and Senior Management Team

The Head has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Designated Safeguarding Lead and the Assistant Head (Digital Strategy).

The Head and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious allegation of online abuse or breach of this policy being made against a member of staff.

The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the Assistant Head (Digital Strategy).

3.3 The Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for all safeguarding and child protection matters at the School, including online safety, and supports all other staff in dealing with any child protection concerns that arise. The DSL is trained in online safety issues. When necessary the DSL will liaise with external agencies such as the Children's Single Point of Access (C-SPA), Early Help or Police.

3.4 Assistant Head (Digital Strategy)

- Takes day to day responsibility for online safety 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
- Is responsible for online safety education for pupils, mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- Consults stakeholders – including parents / carers and the pupils about the online safety provision
- Liaises with school technical staff
- Monitoring network / internet / incident logs with the IT Network Manager

- Receives reports of filtering/online safety incidents and passes these to the Assistant Head (Safeguarding)/DSL and Deputy Head (Pastoral)
- Production, review and monitoring of the school filtering policy and requests for filtering changes in collaboration with the IT Network Manager
- Reports regularly to Senior Management Team (in SMT meetings).

3.5 IT Network Manager

The IT 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
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering is applied and updated on a regular basis
- 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 is regularly monitored in order that any misuse or attempted misuse can be reported to the Assistant Head (Digital Strategy) for investigation
- Monitoring software and systems are kept up to date.

3.6 Teaching and Support Staff

Teachers and support staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of this online safety policy and practices
- They have read, understood and agreed to the IT Acceptable Use Policy which is incorporated in the Staff Conduct Policy (section 18).
- They report any suspected misuse or problem to the Assistant Head (Digital Strategy) for investigation
- All digital communications with other staff, pupils and parents are on a professional level
- They help pupils acquire a good understanding of research skills and the need to avoid plagiarism and uphold copyright law.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

3.7 Pupils

Our pupils:

- Are involved in the development and review of this Policy through discussion in lessons and other forums, in an age appropriate way.
- Are responsible for using the School ICT systems in accordance with the Online Safety Agreement, which is signed when a pupil first joins the School and agreed each year thereafter.
- Will be expected to know and understand policies on the use of IT/connected devices and cyber-bullying.
- Should understand the importance of adopting good online safety practice when using connected technologies out of school and realise that the School's Online Safety Policy covers their actions out of school, where related to their membership of the School.

3.8 Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile/comnnected devices in an appropriate way. Parents are invited to attend online safety training, are 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
- their children's personal devices in the School (where this is allowed)

3.9 Community Users, Visitors and Volunteers

Community users, visitors and volunteers who access school systems will be expected to sign a Visitors' Acceptable Use Policy before being provided with access to school systems.

4. Policy Statement

The School will seek to keep pupils safe online by:

- appointing an online safety co-ordinator (Assistant Head (Digital Strategy), Mark Sartorius)
- providing clear guidance to staff about how to behave online, through the Staff Conduct Policy and training
- supporting pupils to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with pupils and their parents/carers
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
- reviewing and updating the security of our IT systems regularly
- ensuring that user names, logins, email accounts and passwords are used effectively
- ensuring personal information about the staff and pupils is held securely and shared only as appropriate
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

KCSIE categorises the breadth of online safety issues into four areas of risk, the four 'C's:

- CONTENT: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- CONTACT being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

- CONDUCT: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

- COMMERCE: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

The School will deal with online safety incidents in accordance with the procedures outlined in both this policy and in associated school policies, such as *Safeguarding and Protecting Children Policy and Procedure*, *Anti-Bullying* and *Behaviour, Rewards, Sanctions and Discipline.* It will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

4.1 Education - Pupils

The School is aware that for many children the distinction between the online world and other aspects of life is less marked than for some adults. Children often operate very freely in the online world and by secondary school age some are likely to be spending a substantial amount of time online.

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 is provided as part of the PSHE and RSE schemes of work and is regularly revisited.
- The school recognises that a one size fits all approach may not be appropriate for all children, and a more personalised or contextualised approach for more vulnerable children, victims of abuse and some SEND children might be needed.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities. Using materials from the National Online Safety company.
- Pupils are taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils are helped to understand the need for the Online Safety Agreement and encouraged to adopt safe and responsible use both within and outside the School.
- Pupils are helped to understand the benefits associated with social media, online posting and messaging.

- It is accepted that from time to time, for good educational reasons, pupils may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request IT support to remove those sites from the filtered list for those pupils. Any requests to do so should be audited by the IT Network Manager, and clear reasons for the need must be established and recorded.
- Staff should be aware that children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the DSL (or a deputy), will consider a referral into the Cyber Choices programme. This programme aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

4.2 Education - Parents and Carers

Parents play an essential role in the education of their children and in the monitoring/regulation of their child's online behaviour. The school provides information and awareness to parents through seminars, newsletters and the provision of online resources.

4.3 Education - 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 arranged and overseen by the Assistant Head (Digital Strategy), recorded as having taken place as follows:

- Training is made available to staff and is regularly reinforced. The Assistant Head (Digital Strategy) ensures that an audit of the online safety training needs of all staff carried out regularly with support of independently provided training resources.
- All new staff are informed of their obligations with regard to online safety as part of their induction, fully understand and agree to the IT Acceptable Use Policy, section 18 of the Staff Conduct Policy.
- The Assistant Head (Digital Strategy) and DSL will receive regular updates through attendance at external training.
- This policy and its updates will be presented to and discussed by staff as part of Inset training.
- Updates regarding current online threats will be communicated to all staff.

4.4 Education - Governors

The Safeguarding Governors take part in online safety training/awareness sessions:

- Attendance at training provided by any relevant organisation
- Monitoring of school training and information sessions for staff or parents.

5. Technical – infrastructure / equipment, filtering and monitoring

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems including reviews by independent experts.
- 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 users will be provided with a username and secure password by IT who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password at set intervals.
- The "master / administrator" passwords for the school ICT system, used by the IT Network Manager (or other person) must also be available to the Head or other nominated senior leader and kept in a secure place (e.g. school safe).
- The IT Network Manager is responsible for ensuring that 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 installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation's Child Abuse Image Content (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.
- The school has provided enhanced / differentiated user-level filtering.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the IT Acceptable Use Agreements.

- The online Help Desk is in place for users to report any actual / potential technical incident / security breach to the relevant person (the IT Network Manager).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile 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 procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place through the network use policy that forbids staff from downloading executable files and installing programmes on school devices.

6. Remote teaching and learning: Safeguarding and Microsoft Teams

The safeguarding of both pupils and staff must be maintained in remote spaces. All the same policies, rules and guidelines remain in place and adherence to all statutory guidance is demanded. The virtual learning space, notably video-conferencing, creates a new set of challenges, however, for which there are specific St John's School guidelines. These are, as follows:

For pupils:

- Recording or screen-shots of staff and/or pupils during a virtual lesson is prohibited.
- Pupils should select the location of their video-conferencing carefully and adhere to the following rules:
    - It must not be a bedroom.
    - There should be nothing which identifies the life of or location of the household in any detail.
- School organised video-conferencing should only be used for lessons and staff communication and not for pupil-to-pupil communication, and can only take place from Monday to Friday between the hours of 09.00 and 17.00 (i.e. the School's normal teaching hours).

For staff:

- Staff should select the location of their video-conferencing carefully and adhere to the following rules:
    - It must not be a bedroom. The room should be well lit and the visible background area should be checked to ensure that there is nothing which identifies the life of or location of the household in any detail.
    - Other members of the household must not be in the room during any St John's video-conferencing: they must not have access to other St John's pupils via video or audio.
- The Senior Leadership Team and IT Department will be able to access all Microsoft Teams and Heads of academic departments will be able to access their own departments' Teams for monitoring and safeguarding purposes. This should be seen by all parties as a virtual parallel to drop-ins and lesson observations.
- Teaching via video-conference or other online communication means must only take place from Monday to Friday between the hours of 09.00 and 17.00 (i.e. the School's normal teaching hours).
- Staff should record details (e.g. names, date, time/duration, purpose, outcome) and submit to the Deputy Head (Academic) and Head of department any additional conference calls to individual students to support their learning.
- Deputy Head (Academic) will circulate a list of any pupils that are withdrawn from video-conferencing by their parents.

7. Mobile Technologies - BYOD

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop, smartwatches or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other

relevant school polices including but not limited to the Safeguarding and Protecting Children Policy, Behaviour Rewards Sanctions and Discipline, Anti-bullying Policy, Staff Conduct Policy (includes IT Acceptable Use), and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education programme.

Mobile phones may be brought to school. Lower School, Fourth Form and Fifth Form must hand in phones during the School Day. Only Sixth Form may retain their phones during the day and after lights out when boarding.

8. Use of digital and video images

Please also see the Staff Conduct Policy, section 17. 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 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.
- In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital / video images.
- As per the School's Staff Conduct Policy (section 17), staff and volunteers should avoid using personal mobile phones/tablets to take images of children and should, where possible, only use School phones, tablets, video, and photography equipment. School cameras can be borrowed from the MIS Manager. If no school equipment is available, images should be transferred straight onto the school network and deleted from the personal device and from personal cloud storage areas and staff should report to the Deputy Head (Pastoral) that this has taken place. All images of children should be stored securely and only accessed by those authorised to do so. Staff should delete any images from their personal media once the picture has been downloaded and stored on the school network.

When taking photos or videos the following should be considered:

- The purpose of the activity must be clear;
- All images should be open to scrutiny to ensure that they are appropriate;
- Images should not be made during one-to-one situations;
- Ensure that the pupil or pupils are appropriately dressed;
- Ensure that the pupils understand why the picture is being taken;
- Images must not be taken secretively;
- 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;
- Written permission from parents will be obtained before photographs of pupils are published on the school website;
- Pupil's work can only be published with the permission of the pupil and or parent.

Staff should not record pupils when using Microsoft Teams, staff wishing to record an online lesson must seek permission from the Deputy Head (Academic).

9. Data Protection

The School has a Data Protection Policy and Compliance Procedures for Staff and an Information Security Policy which all staff should be familiar with, to make sure that personal data is kept safe when working in school or off-site and using personal devices. Please refer to those policies for further detail. Regular staff and pupil training on information security is provided.

10. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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

- The official School email service may be regarded as safe and secure. Users should be aware that email communications may be monitored.
- Users must immediately report, to the IT Network Manager, the HR Manager or their Line Manager (as appropriate) 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 pupils or parents (email, chat, VLE 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.*
- Staff must not contact pupils at home unless absolutely necessary. In such circumstances the School email or Microsoft Teams must be used and communication should be restricted to the hours **0730-2130.**

11. Social Media - Protecting Professional Identity

The School has a duty of care to provide a safe learning environment for pupils and staff. The School 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, disability (or other protected characteristics) or who defame a third party may render the School liable to the injured party.

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
- Training is provided including: acceptable use, social media risks, checking of settings, data protection, reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.

School staff should ensure that:

- No reference should be made in social media to pupils, parents 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.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The School's official social media accounts are managed and monitored by the Communications Department to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Please also refer to section 16 of the Staff Conduct Policy.

12. Responding to online safety incidents

The following 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; please see Appendix 1 for clarification of acceptable / unacceptable / illegal online activities.

Advice for schools on how to respond to the sharing of "nudes and semi-nudes" (formerly referred to as 'sexting' and 'youth produced sexual imagery') is in section 24 of the School's Safeguarding and Protecting Children Policy and Procedures. The full guidance from the UK Council for Internet Safety (UKCIS) can be found here.

The latest advice from UKCIS (December 2020) defines this activity as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline. Alternative terms used by children and young people may include 'dick pics' or 'pics'.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated.

This guidance does not apply to adults sharing nudes or semi-nudes of under 18-year olds. This is a form of child sexual abuse and must be referred to the police as a matter of urgency.

If an incident comes to your attention report it to the DSL immediately.

Never view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**.

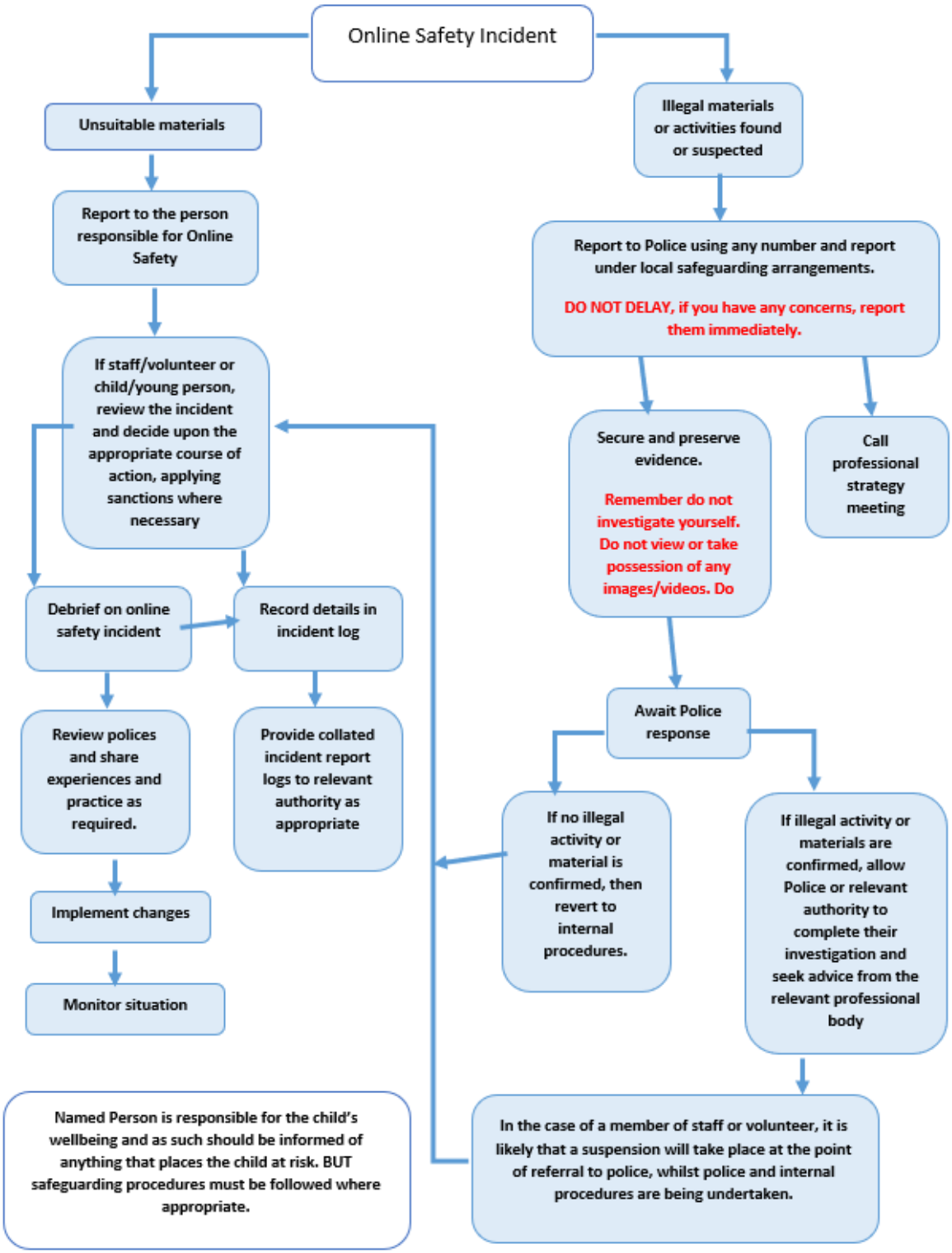
Please refer to the DSL, the safeguarding procedures and the UKCIS guidance for further information and advice.

12.1 Online Abuse

If online abuse occurs, the School will respond according to the detail of the incident and in accordance with its Safeguarding and Protecting Children Policy and Procedures. The School will provide support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation. The School will make sure its response takes the needs of the person experiencing abuse, any bystanders and the School as a whole into account. The School will review its strategies for addressing online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

12.2 Illegal Incidents

If there is any suspicion that the website(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) for responding to online safety incidents and report immediately to the police.



12.3 Responding to Other Incidents

It is hoped that all members of the School community will be responsible users of connected 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 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.**

- **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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

12.4 Allegations and Sanctions

Safeguarding allegations or concerns about Staff will be handled in accordance with the Safeguarding and Protecting Children Policy and Procedures. Staff misuse of School ICT systems will be dealt with in accordance with the Disciplinary and Dismissal Procedure.

Pupils' misuse of School ICT systems will be dealt with in accordance with the School's Behaviour, Rewards, Sanctions and Discipline Policy.

Appendix 1

Acceptable, unacceptable and illegal activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal. Other activities e.g. cyber-bullying is a serious breach of St John's School policy 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 are 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:
(see chart on next page)

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS– Sexting in schools and colleges					X
	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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices						X

• Using penetration testing equipment (without relevant permission)					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)	X				
On-line gaming (non-educational)		X			
On-line gambling				X	
On-line shopping/commerce		X			
File sharing				X	
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. Youtube		X			