Online Safety (E-Safety)

St John's Catholic Primary School

2023/2024

This policy was adopted March 2023

This policy will be reviewed January 2025

Contents

1 Introduction

At St John's we believe that online safety (e-safety) is an essential element to safeguard students and adults in the digital world, when using technology such as computers, mobile phones or games consoles.

St John's identifies that the Internet and information communication technologies are an important part of everyday life so students must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

St John's has a duty to provide the school community with quality Internet access to raise education standards, promote student achievement, support the professional work of staff and enhance the school's management functions. St John's also identifies that with this there is a clear duty to ensure that students are protected from potential harm online.

The purpose of this online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that St John's is a safe and secure environment
- Safeguard and protect all members of the St John's community online
- Raise awareness with all members of the St John's community regarding the potential risks as well as benefits of technology
- Enable staff to work safely and responsibly, to role model positive behaviour online and to be aware of the need to manage their own standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- 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.

This policy applies to staff including the governing body, teachers, support staff, external contractors, visitors, volunteers (and other individuals who work for or provide services on behalf of St John's) as well as students and parents/carers.

This policy applies to all access to the Internet and use of information communication devices including personal devices or where students, staff or other individuals have been provided with St John's issued devices for use off-site, such as a work laptop or mobile phone.

This policy must be read in conjunction with other relevant St John's policies including (but not limited to) Safeguarding, Anti-bullying, Behaviour, Photographic Image Use, Acceptable Use, confidentiality, and relevant curriculum policies including Computing, Relationships, Health and Sex Education (RSHE) Policy.

This online safety policy has been written by St John's, building on specialist advice and input as required. It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2022, 'Working Together to Safeguard Children' 2018 and the West Sussex procedures.

St John's continues to operate in response to coronavirus (Covid-19); our safeguarding principles in accordance with 'Keeping Children Safe in Education' (KCSIE) 2022 and related guidance, however, remain the same. Where children are asked to learn online at home in response to a full or partial closure or self-isolation, will follow expectations as set out within the Child Protection Policy and in line with DfE Guidance, 'Safeguarding and remote education during coronavirus (COVID-19)' 2020.

St John's Online safety policy and its implementation will be reviewed at least every two years or sooner if required. This will be reviewed using:

• Logs of reported incidents

• Internal monitoring of data, such as web filtering, search engine queries and web-browsing history

• Surveys/ questionnaires of users

• The Safeguarding Team should be advised of any reported incidents through the normal Safeguarding process

• The E-Safety coordinator should attend appropriate training and networking events to ensure the organisation is able to respond to emerging safety concerns and technical changes

The DSL (Designated Safeguarding Lead) has overall responsibility for Online Safety, the educational aspect of online safety is overseen and directed, monitored by the Computing subject leader.

1.2 Key responsibilities

1.2.1 Key responsibilities of Senior Leadership Team are:

To ensure that there are appropriate and up-to-date policies regarding online safety; including an •acceptable use policy, which covers acceptable use of technology

• To ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks

• To ensure that online safety is embedded within the curriculum, which enables all students to develop an age-appropriate understanding of online safety

• To support the DDSL's by ensuring they have sufficient time and resources to fulfil their online safety responsibilities

• To ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support

• To ensure that appropriate risk assessments are undertaken regarding the safe use of technology

• To audit and evaluate online safety practice to identify strengths and areas for improvement

1.2.2 Key responsibilities of the designated safeguarding/online safety lead are:

• To act as a named point of contact on all online safety issues and liaise with other members of staff and agencies as appropriate

• To keep up-to-date with current research, legislation and trends

• To coordinate participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day

• To ensure that online safety is promoted to parents/carers and the wider community through a variety of channels and approaches

• To work with St John's lead for data protection (SBM) and data security to ensure that practice is in line with legislation

• To access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep students safe online

• To ensure that online safety incidents and subsequent actions are recorded as part of St John's safeguarding recording structures and mechanisms. Records will be kept in CPOMS under the heading of child protection

• To monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures

• To liaise with the local authority and other local and national bodies as appropriate

• To report online safety concerns, as appropriate, to the Senior Leadership Team and governing body if required

• To work with the leadership team to review and update online safety policies on a regular basis (at least every two years)

• To ensure that online safety is integrated with other appropriate St John's policies and procedures

• To meet regularly with the governor with a lead responsibility for online safety and Safeguarding.

1.2.3 Key responsibilities of staff are:

• To contribute to the development of online safety policies

• To read St John's Acceptable User Agreement, sign it and adhere to it

• To take responsibility for the security of St John's systems and data that they have access to

• To have an awareness of online safety issues, and how they relate to the students in their care, including understanding the key issues related to online safety; content, contact, conduct and commerce

• To ensure that they understand that technology is a significant component in many safeguarding and wellbeing issues and that children are at risk of abuse online as well as face to-face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content

• To model good practice in using new and emerging technologies and demonstrate an emphasis on positive learning opportunities rather than focusing on negatives

• To embed online safety education in curriculum delivery wherever possible. As all teachers at St John's are subject leaders this is part of their role as subject leaders who develop their own curriculums

• To identify individuals of concern, and take appropriate action by working with the DSL, DDSL's

• To know when and how to escalate online safety issues, internally and externally

• To be able to signpost to appropriate support available for online safety issues, internally and externally

• To maintain a professional level of conduct in their personal use of technology, both on and off site

• To take personal responsibility for professional development in this area.

1.2.4. Additional responsibilities for staff managing the technical environment are:

• To provide technical support and perspective to the DSL and Senior Leadership Team, especially in the development and implementation of appropriate online safety policies and procedures

• To implement appropriate security measures as directed by the Senior Leadership Team, to ensure that the IT systems are secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised

• To ensure that our filtering policy is applied and updated on a regular basis. The responsibility for its implementation is shared with the Senior Leadership Team

• To ensure that our monitoring systems are applied and updated on a regular basis. The responsibility for its implementation is shared with the Senior Leadership Team

• To ensure that appropriate access and technical support is given to the DSL (and/or DDSL's) to our filtering and monitoring systems, to enable her to take appropriate safeguarding action if/when required.

1.2.5 Key responsibilities of students are:

• To read St John's Acceptable Use Policy (AUA) and adhere to it

• To respect the feelings and rights of others both on and offline

• To seek help from a trusted adult if things go wrong, and support others that may be experiencing online safety issues

• To take responsibility for keeping themselves and others safe online

• To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies

• To assess the personal risks of using any particular technology and behave safely and responsibly to limit those risks.

1.2.6. Key responsibilities of parents/carers are:

• To read St John's AUA, encourage their children to adhere to it, and adhere to it themselves where appropriate

• To support St John's online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home

• To role model safe and appropriate uses of new and emerging technology

• To identify changes in behaviour that could indicate that their child is at risk of harm online

• To seek help and support from St John's, or other appropriate agencies, if they or their child encounters online problems or concerns

• To contribute to the development of St John's online safety policy

• To use St John's systems, and other network resources, safely and appropriately when in school

• To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies

• To report any known issues as soon as possible

• To attend offered parents information sessions to upskill themselves and safeguard their family.

2. Online Communication and Safer Use of Technology

2.1 Managing the St John's website

• St John's will ensure that information posted on the St John's website meets the requirements as identified by the Department for Education (DfE)

• St John's will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright

• The administrator account for the website will be secured with an appropriately strong password only known by SLT and the host provider

• We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

2.2 Publishing images and videos online

• St John's will ensure that all images are used in accordance with St John's Photographic Image permissions

•Permissions for photographic images and video images will be obtained as children join the school

• Parents/carers have the right at any time to withdraw their consent for images to be published of their child.

•Full names should never be included in any published picture of a child.

2.3 Managing email

• Students may only use provided email accounts for educational purposes i.e. Google Classroom or purple Mash simulator. Parents will be notified if these facilities become live and are required for an educational purpose

• All staff are provided with a specific St john's email address to use for any official communication

• The use of personal email addresses by staff for any official school business is not permitted

• The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider

• Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and/or encrypted methods. We use Voltage Secure

• Members of the St John's community must immediately tell a member of the Senior Leadership Team if they receive an offensive communication

• Sensitive or personal information will only be shared via email in accordance with data protection legislation

• Email sent to external organisations should be written carefully before sending, in the same way as a letter written on headed paper would be

• St John's email addresses and other official contact details will not be used for setting up personal social media accounts or subscribing to services.

•Parents should only contact staff members via email through the office email address. This is to ensure the school manages teachers work load and protects them from harm or potential abuse.

2.4 Official videoconferencing and webcam use

• All videoconferencing equipment in the classroom will be switched off when not in use and where appropriate, not set to auto answer

• Videoconferencing contact information will not be posted publicly by staff

• Videoconferencing equipment will not be taken off the premises without prior permission from a DSL

• Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure

• Students will not use, or have access to, videoconferencing equipment without permission and under direct supervision from a member of staff. The DSL must always be informed if pupils are expected to engage for any reason in video conferencing.

Users

• Students will ask permission from a teacher before making or answering a videoconference call or message

• Videoconferencing will always and at all times be supervised

• Parents'/carers' consent will be obtained prior to students taking part in videoconferences with anyone outside of the school

• Videoconferencing will take place via official and approved communication channels following a robust risk assessment

• Unique log on and password details for the educational videoconferencing services will only be issued to staff and kept secure.

Content

• When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference

2.5 Appropriate and safe classroom use of the Internet and associated devices

• St John's Internet access will be designed to enhance and extend education

• Students will use age and ability appropriate tools to search the Internet for content

• Internet use is a key feature of educational access and all students will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum

• St John's will ensure that the use of Internet-derived materials by staff and students complies with copyright law and acknowledge the source of information

• All staff are aware that they cannot rely on filtering alone to safeguard students and supervision, classroom management and education about safe and responsible use is essential

• Students will be appropriately supervised when using technology

• All St John's owned devices will be used in accordance with St John's AUA and with appropriate safety and security measure in place. These devices are centrally managed by JSPC

• Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

• St John's will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community

• in a remote learning environment St John's use the Internet to enable students and staff to communicate and collaborate in a safe and secure environment using Google Classroom as the main tool

• Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

• The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum

• Staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

3. Social Media Policy

3.1. General social media use

• Expectations regarding safe and responsible use of social media will apply to all members of the St John's community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others

• All members of the St John's community will be encouraged to engage in social media in a positive, safe and responsible manner at all times

• Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the St John's community

• All members of the St John's community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others. For staff this could lead to a disciplinary matter

• St John's will control students and staff access to social media and social networking sites whilst on site and using St John's provided devices and systems

• The use of social networking applications during St John's hours for personal use is not permitted except during staff breaks whilst they are in the staffroom

• Any concerns regarding the online conduct of any member of the St John's community on social media sites should be reported to the Senior Leadership Team and will be managed in accordance with existing St John's policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection

• Any breaches of St John's policy may result in criminal and or disciplinary action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with the relevant St John's policies, such as anti-bullying, whistleblowing, behaviour and safeguarding/child protection.

3.2 Official use of social media

• Official use of social media sites by St John's will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement, raise the profile of the school to promote increased pupil numbers, publicity, community events, celebrate achievements

• Official use of social media sites as communication tools will be risk assessed and formally approved by the Headteacher

• Official St John's social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes

• Staff will use St John's provided email addresses to register for and manage official St John's approved social media channels

• Staff running official St John's social media channels will ensure that they are aware of the required behaviours and expectations of use. They will ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation

• All communication on official St John's social media platforms will be clear, transparent and open to scrutiny

• Any online publication on official St John's social media sites will comply with legal requirements will not breach any common law duty of confidentiality, copyright etc.

• Official social media use by St John's will be in line with existing policies, including: anti-bullying and child protection

• Images or videos of students will only be shared on official St John's social media sites/channels in accordance with St John's Photographic Image Use agreement

• Information about safe and responsible use of St John's social media channels will be communicated clearly and regularly to all members of the St John's community

• Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the St John's website and take place with written approval from Senior Leadership Team

• Senior Leadership staff must be aware of account information and relevant details for social media channels in case of emergency such as staff absence

• Parents/carers and students will be informed of any official St John's social media use, along with expectations for safe use and St John's action taken to safeguard the community

• Public communications on behalf of St John's will, where possible, be read and agreed by at least one other colleague. The same procedure will be followed when posting images to ensure all pupils without permission have been removed from the image

• St John's will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

3.3 Staff official use of social media

• If staff are participating in online activity as part of their capacity as an employee of St John's, then they are requested to be professional at all times and that they are an ambassador for St John's

• Staff using social media officially will disclose their official role/position, but always make it clear that they do not necessarily speak on behalf of St John's.

• Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared

• Staff using social media officially will always act within the legal frameworks they would adhere to within St John's, including: libel; defamation; confidentiality; copyright; data protection as well as equalities laws

• Staff must ensure that any image posted on St John's social media channels have appropriate permission

• Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of St John's unless they are authorised to do so

• Staff using social media officially will inform their line manager, St John's online safety (e-safety) lead and/or the Headteacher of any concerns such as criticism, or inappropriate content posted online

• Staff will not engage with any direct or private messaging with students or parents/carers through social media and should communicate via St John's communication channels

• Staff using social media officially will sign St John's AUA before official social media use will take place.

3.4 Staff personal use of social media

• Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction (safeguarding training) and will be revisited and communicated via regular staff training opportunities

• Safe and professional behaviour will be outlined for all staff (including volunteers) as part of St John's AUA

• All staff are advised not to communicate with or add as 'friends' any current or past students or current or past students' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the DSL/Senior Leadership Team

• If ongoing contact with students is required once they have left St John's roll, then members of staff will be expected to use existing alumni networks or use official St John's provided communication tools

• All communication between staff and members of the St John's community on St John's business will take place via official approved communication channels (such as St John's email addresses or phone numbers). Staff must not use personal accounts or information to make contact with students or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Headteacher

• Any communication from students/parents received on personal social media accounts will be reported to a DSL

• Information that staff have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social media sites

• All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential

• All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with St John's policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework

• Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis

• Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in St John's

• Members of staff are encouraged not to identify themselves as employees of St John's on their personal social networking accounts. This is to prevent information on these sites from being linked with St John's and also to safeguard the privacy of staff and the wider St John's community

• Members of staff will ensure that they do not represent their personal views as that of St John's on social media

• St John's email addresses will not be used for setting up personal social media accounts

• Members of staff who follow/like St John's social media channels will be advised to use dedicated professionals accounts where possible to avoid blurring professional boundaries

3.5 Students use of social media

• Personal publishing on social media sites will be taught to students as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes

• Students will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, St John's attended, Instant messenger contact details, information through photographs, email addresses, full names of friends/family, specific interests and clubs etc.

• Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present

• Students will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications

• Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

The widespread ownership of mobile phones and a range of other personal devices, including wearable technologies, among children, young people and adults will require all members of the St John's community to take steps to ensure that mobile phones and personal devices are used responsibly and do not cause a Safeguarding risk.

• The use of mobile phones and other personal devices by young people and adults will be decided by St John's. In the simplest terms- children may carry a mobile phone to school and from school. It must be handed into the office before children enter the building and collected from the office at the end of the day. Children are not permitted to wear apple watches or any wearable device that takes photographic images. Children are permitted to wear a fitness tracker, such as a Fitbit as long as it cannot record audio or visual information.

• St John's recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but requires that such technologies need to be used safely and appropriately. It is part of our job to educate the children and parents about how to stay safe.

4.2 Expectations for safe use of personal devices and mobile phones

• Electronic devices of all kinds that are brought into St John's are the responsibility of the user at all times. St John's accepts no responsibility for the loss, theft or damage of such items. Nor will St John's accept responsibility for any adverse health effects caused by any such devices either potential or actual

• Mobile phones and personal devices are not permitted to be used in certain areas within the St John's site. Mobile phones should not be used to answer phone calls in classrooms or corridors during school hours

• The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the St John's community and any breaches will be dealt with as part of the St John's discipline/behaviour policy

• Members of staff will be issued with a St John's/work phone when on a trip in case there is a need to call a parent

• All members of the St John's community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage

• All members of the St John's community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared

• All members of the St John's community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene St John's policies

• St John's mobile phones and devices must always be used in accordance with the AUA

• St John's mobile phones and devices used for communication with parents and students must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Students use of personal devices and mobile phones

• Students will be educated regarding the safe and appropriate use of personal devices and mobile phones

• All use of mobile phones and personal devices by students will take place in accordance with the Acceptable Use Agreement

• Mobile phones and personal devices will be switched off and kept in the office during school and club hours

• Wearable technologies, such as smart watches, headphones and other smart devices, are not allowed in school

• If a student needs to contact his/her parents/carers he/she will be allowed to use a St John's phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the St John's office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the Headteacher (for example diabetic monitoring)

• Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences

• If a student breaches the policy, the phone or device will be confiscated and will be held in a secure place:

• Staff may confiscate a student's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (Youth Produced Sexual Imagery)

• Searches of mobile phone or personal devices will not be carried out by the school

• Mobile phones and devices that have been confiscated will be released to parents or carers or the police

• If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation

• Where students' mobile phones or personal devices are used when learning at home, such as in response to local or full lockdowns, this will be in accordance with our Acceptable Use Agreement

4.5 Staff use of personal devices and mobile phones

• Members of staff are not permitted to use their own personal phones or devices for contacting students, young people and their families within or outside of St John's in a professional capacity. Any pre-existing relationships which could compromise this must be discussed with a DSL

• Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of students and will only use work-provided equipment for this purpose

• Staff will not use any personal devices directly with students and will only use work-provided equipment during lessons/educational activities

• Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times

• Bluetooth or other forms of communication should be "hidden" or switched off during lesson times

• Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior leadership team in emergency circumstances

• Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations

• If a member of staff breaches St John's policy then disciplinary action will be taken

• If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted and allegations will be taken seriously

• Where remote learning activities because of Covid-19 or another pandemic situation, staff will use St John's provided equipment. If this is not available, staff will only use personal devices with prior approval from the Headteacher, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Agreement.

4.6 Visitors use of personal devices and mobile phones

• Parents/carers and visitors must use mobile phones and personal devices in accordance with St John's policy.

• Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with St John's Photographic Image Use policy. We would not allow images of our children to be taken by externals without express permission from the Headteacher

• Staff will be expected to challenge concerns when safe and appropriate and will always inform the DSL of any breaches of use by visitors.

5 Policy Decisions

5.1. Reducing online risks

St John's is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

• Emerging technologies will be examined for educational benefit and St John's senior leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed

-• St John's will ensure that appropriate filtering systems are in place to prevent staff and students from accessing unsuitable or illegal content. The Computing subject leader will also be aware of these measures

• Our monitoring system and filtering system will:

- Inspect everything that is typed or done;
- Take screen shots and will report any suspicious use detected;
- Detect when proxy bypass sites have been used;
- Help stop downloads of obscene or offensive content;
- Help pick up 'cries for help' helping to:
- Reduce fears over suicide, self-harm and abuse;
- Take appropriate action quickly;
- Strengthen pastoral care.

• St John's will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a St John's computer or device.

• St John's will audit technology use to establish if the online safety (e–safety) policy is adequate and that the implementation of the policy is appropriate

• Methods to identify, assess and minimise online risks will be reviewed regularly by the senior leadership team

• Filtering decisions, Internet access and device use by students and staff will be reviewed regularly by the senior leadership team.

5.2. Internet use throughout the wider St John's community

• St John's will liaise with local organisations to establish a common approach to online safety (e–safety)

• St John's will provide an AUA for any guest/visitor who needs to access the St John's computer system or Internet on site.

5.3 Authorising Internet access

• St John's will maintain a current record of all staff and students who are granted access to St John's electronic communications

• All staff, students and visitors will read and sign St John's AUA before using any St John's ICT resources

• Parents will be informed that students will be provided with supervised Internet access which is appropriate to their age and ability

• Parents will be asked to read St John's AUA for student access and discuss it with their child, where appropriate. The AUA was last sent home in 2022 and shared with parents before it was signed by both parents and children

• When considering access for vulnerable members of the St John's community (such as with students with special education needs) St John's will make decisions based on the specific needs and understanding of the student(s).

6 Engagement Approaches

6.1 Education and engagement with learning

We will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible Internet use amongst students by:

- Ensuring education regarding safe and responsible use precedes Internet access;
- Including online safety in our RESPECT curriculum (encompasses PSHE, RSHE, RE, Citizenship, Safeguarding) Computing programmes of study (Purple Mash platform);
- Reinforcing online safety messages whenever technology or the Internet is in use;
- Educating students in the effective use of the Internet to research; including the skills of knowledge location, retrieval and evaluation;
- Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

• We will support students to read and understand the acceptable use policies in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with Internet access;
- Informing students that network and Internet use will be monitored for safety and security purposes and in accordance with legislation;
- Rewarding positive use of technology with House Points;
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments;
- Seeking student voice when writing and developing online safety policies and practices, including curriculum development and implementation;
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

6.2 Engagement and education of children and young people who are considered to be vulnerable

St John's recognises that some students are more vulnerable online owing to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

• We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students

• When implementing an appropriate online safety policy and curriculum St John's will seek input from specialist staff as appropriate, including the SENCO and ELSA.

6.3 Engagement and education of staff

• The online safety (e-safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of St John's safeguarding practice

• To protect staff and students, St John's will implement an AUA which highlights appropriate online conduct and communication

• Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential

• Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis

• Staff with a responsibility for managing filtering systems or monitor ICT use (JSPC) will be supervised by the senior leadership team and will have clear procedures for reporting issues or concerns

• St John's will highlight useful online tools which staff should use with students in the classroom. These tools will vary according to the age and ability of the students

• Staff will be made aware that their online conduct out of St John's could have an impact on their role and reputation within St John's. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

6.4 Engagement and education of parents and carers

• St John's recognises that parents/carers have an essential role to play in enabling students to become safe and responsible users of the Internet and digital technology

• Parents' attention will be drawn to St John's online safety (e-safety) policy and expectations in communications, such as newsletters and the St John's website

• We will build a partnership approach to online safety with parents/carers by:

- Providing information and guidance on online safety in a variety of formats;
- This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days;
- Requesting that they read online safety information as part of joining our community, for example, within our home-school agreement;
- Requiring them to read our acceptable use agreement and discuss the implications with their children.

7. Managing Information Systems

7.1 Managing personal data online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. Full information can be found in St John's data protection policy.

7.2 Security and Management of Information Systems

• The security of St John's Information Systems and users will be reviewed regularly

• Virus protection will be updated regularly and managed by JSPC

• Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems

• Portable media may not be used without specific permission followed by an anti-virus /malware scan

• Unapproved software will not be allowed in work areas or attached to email

• The network manager (SBM) will review system capacity regularly

• The appropriate use of user logins and passwords to access the St John's network will be enforced for all users

• All users will be expected to log off devices if systems are unattended

Password policy

All users will be informed not to share passwords or information with others and not to login as another user at any time

• Staff and students must always keep their password private and must not share it with others or leave it where others can find it easily

• All members of staff will have their own unique username and private passwords to access St John's systems. This must not be shared with other staff. Staff are responsible for keeping their password private

7.3 Filtering Decisions

St John's senior leadership team have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit students' exposure to online risks

• The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding

• Our decision regarding filtering and monitoring has been informed by considering our specific needs and circumstances and informed by specialist providers at JSPC

• The senior leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate

• Staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

7.4 Management of applications (apps) used to record student progress

• The Headteacher is ultimately responsible for the security of any data or images held of students

• Apps/systems which store personal data will be risk assessed prior to use

• Personal staff mobile phones or devices will not be used for any apps which record and store student's personal details, attainment or photographs

• Only St John's issued devices will be used for apps that record and store children's personal details, attainment or photographs

• Staff and parents/carers will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

8. Responding to Online Incidents and Concerns

All members of the St John's community will be informed about the procedure for reporting online safety (e-safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc.)

• A DSL will be informed of any online safety (e-safety) incidents involving child protection concerns, which will then be recorded

• A DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the West Sussex Safeguarding Children Board thresholds and procedures

• Complaints about Internet misuse will be dealt with under St John's complaints procedure

• Complaints about online bullying will be dealt with under St John's anti-bullying policy and procedure

• Any complaint about staff misuse will be referred to the Headteacher

• Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer)

• Students, parents and staff will be informed of St John's complaints procedure (see website for the policy)

• Staff will be informed of the complaints and whistleblowing procedure

• All members of the St John's community will need to be aware of the importance of confidentiality and the need to follow the official St John's procedures for reporting concerns

• All members of the St John's community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the St John's community

• St John's will manage online safety (e-safety) incidents in accordance with the St John's discipline/behaviour policy where appropriate

• St John's will inform parents/carers of any incidents of concerns as and when required

• After any investigations are completed, St John's will debrief, identify lessons learnt and implement any changes as required

• Where there is cause for concern or fear that illegal activity has taken place or is taking place then St John's will contact the Education Safeguarding Team or West Sussex Police via 999, if there is immediate danger or risk of harm

• The use of computer systems without permission, or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to West Sussex Police

• If St John's is unsure how to proceed with any incidents of concern, then the incident will be escalated to the IFD

• If an incident of concern needs to be passed beyond St John's then the concern will be escalated to the IFD and the LADO

• Parents and students will need to work in partnership with St John's to resolve issues.

9. Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding Youth Produced Sexual Imagery

St John's recognises youth produced sexual imagery (previously known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy)

• We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in Schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery"

• St John's will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods

• We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery

• We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment

• We will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so;
- If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented;
- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request students to do so

• If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with our child protection policies and the relevant West Sussex Safeguarding Child Board's procedures;
- Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance;
- Store the device securely; ▪ If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of students involved; including carrying out relevant checks with other agencies;
- Inform parents/carers, if appropriate, about the incident and how it is being managed;
- Make a referral to the IFD/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance;
- Provide the necessary safeguards and support for students, such as offering counselling or pastoral support;
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible;
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance; ▪ Images will only be deleted once the DSL has confirmed that other agencies do not

need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation

- Review the handling of any incidents to ensure that best practice was implemented; the Senior Leadership Group will also review and update any management procedures, where necessary.

9.2. Responding to concerns regarding Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

St John's will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns

• St John's recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy)

• We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for students, staff and parents/carers

• We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally

• We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to students and other members of our community on the St John's website

• If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our child protection policies and the relevant IFD's procedures;
- If appropriate, store any devices involved securely;
- Make a referral to the IFD (if required/appropriate) and immediately inform West Sussex police via 101, or 999 if a child is at immediate risk;
- Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies);
- Inform parents/carers about the incident and how it is being managed;
- Provide the necessary safeguards and support for students, such as, offering counselling or pastoral support;
- Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary

• We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.

- Where possible, students will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/

• If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or West Sussex police

• If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL (or deputy)

• If students at other setting are believed to have been targeted, the DSL (or deputy) will seek support from West Sussex police and/or the IFD/LADO first to ensure that potential investigations are not compromised.

9.3. Responding to concerns regarding Indecent Images of Children (IIOC)

St John's will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC)

• We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site

• We will seek to prevent accidental access to IIOC by using an Internet Service provider (ISP =) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software

• If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through West Sussex police and/or the IFD

• If made aware of IIOC, we will:

- Act in accordance with our child protection policy and the relevant IFDs procedures;
- Store any devices involved securely;
- Immediately inform West Sussex police

• If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL (or deputy) is informed;
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk ;
- Ensure that any copies that exist of the image, for example in emails, are deleted (with police permission);
- Report concerns, as appropriate to parents/carers

• If made aware that indecent images of children have been found on the setting provided devices, we will:

- Ensure that the DSL (or deputy) is informed;
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk ;
- Ensure that any copies that exist of the image, for example in emails, are deleted
- Inform the police via 101 (999 if there is an immediate risk of harm) and the IFD (as appropriate);
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only;
- Report concerns, as appropriate to parents/carers

• If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the Headteacher is informed in line with our managing allegations against staff policy. Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy
- Quarantine any devices until police advice has been sought

9.4. Responding to concerns regarding radicalisation or extremism online

St John's will take all reasonable precautions to ensure that students are safe from terrorist and extremist material when accessing the Internet in school and that suitable filtering is in place which takes into account the needs of students. All staff are trained in Prevent and the DSL is Chanel trained.

• When concerns are noted by staff that a student may be at risk of radicalisation online then the DSL will be informed immediately and action will be taken in line with St John's Safeguarding policy.
• If we are concerned that staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

9.5. Responding to concerns regarding cyberbullying

Cyberbullying, along with all other forms of bullying, of any member of the St John's community will not be tolerated. Full details are set out in St John's policies regarding anti-bullying and behaviour.

• All incidents of online bullying reported will be recorded on CPOMS

• There are clear procedures in place to investigate incidents or allegations and support anyone in the St John's community affected by online bullying

• If St John's is unclear if a criminal offence has been committed, then the DSL will obtain advice immediately through the IFD and/or West Sussex police

• Students, staff and parents/carers will be advised to keep a record of the bullying as evidence

• St John's will take steps to identify the bully where possible and appropriate. This may include examining St John's system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary

• Students, staff and parents/carers will be required to work with St John's to support the approach to cyberbullying and St John's e-safety ethos

• Sanctions for those involved in online or cyberbullying may include the following;

- Those involved being asked to remove any material deemed to be inappropriate or offensive
- A service provider being contacted to remove content if those involved refuse to or are unable to delete content
- Internet access may be suspended at St John's for the user for a period of time
- Other sanctions for students and staff may also be used in accordance to St John's anti-bullying, behaviour policy or AUA

- Parent/carers of students involved in online bullying will be informed
- The Police will be contacted if a criminal offence is suspected.

9.6. Responding to concerns regarding Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at St John's and will be responded to in line with existing policies, including anti-bullying and behaviour.

• All members of the community will be advised to report online hate in accordance with relevant policies and procedures

• The Police will be contacted if a criminal offence is suspected

• If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the IFD and/or West Sussex police.

•Records of all events will be kept on CPOMS.