ST MARGARET'S PREP  ST MARY'S CALNE

Online Safety Policy

Issued by:	SGT / GSM /
Last review:	September 2024
Next review due:	September 2025
Location:	Website Staff Portal

ST MARGARET'S PREP  ST MARY'S CALNE

Online Safety Policy

Contents

1. Online Safety Ethos

1.1. Aims and policy scope
St Mary's school believes that:

- Online safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
- The Internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.
- The school has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.
- That there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of St Mary's 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 technology to ensure that St Mary's school is a safe and secure environment.
- Safeguard and protect all members of the school online.
- Raise awareness with all members of the school regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and 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.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/guardians.

This policy applies to all access to the Internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

This policy must be read in conjunction with other relevant school policies including (but not limited to) Safeguarding, Child Protection, Anti-bullying, Behaviour, Data Protection, Staff Code of Conduct, Pupil IT Code of Conduct and relevant curriculum policies including Computing and Personal Development.

1.2. Reviewing

- The policy has been approved and agreed by the Senior Leadership Team and Governing Body.
- The school has appointed the Designated Safeguarding Lead; Mrs S Toland as an appropriate member of the leadership team and the online safety lead.
- The school has nominated Mrs Tricia Pearce as the member of the Governing Body to take lead responsibility for school safeguarding and online safety.
- The online safety policy and its implementation will be reviewed by the school annually or sooner if required.

1.3. Responsibilities:

1.3.1 The responsibilities of the Senior Leadership Team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Regularly reviewing online safeguarding records and using them to shape future practice.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.

1.3.2 The responsibilities of the Designated Safeguarding Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Take the lead responsibility for understanding the filtering and monitoring systems and processes in place.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Ensuring that online safety is promoted to parents and guardians and the wider community through a variety of channels and approaches.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the school's safeguarding recording structures and mechanisms.
- To report to the Senior Leadership Team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Meet regularly with the governor with a lead responsibility for online safety.

1.3.3 The responsibilities of the Director of Sitewide IT are:

- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy (in Staff Code of Conduct) which covers appropriate professional conduct and use of technology.
- To assist the DSL to ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community.
- To work with and support technical staff in monitoring the safety and security of school systems and networks and to ensure that the school network system is actively monitored.
- To assist the DSL to ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Work with the Bursar to ensure data protection and data security is in line with current legislation.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- To assist the DSL to monitor the school's online safety incidents to identify gaps/trends and use this data to update the school's education response to reflect need.
- To assist the DSL in auditing and evaluating current online safety practice to identify strengths and areas for improvement.

1.3.4 Responsibilities of the Network Manager:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the Director of Sitewide IT and the Senior Leadership Team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the school network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL and Director of Sitewide IT and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Ensuring that the school's IT infrastructure and software is secure.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all school machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced and 2FA is enabled on any system where sensitive data is stored.

1.3.5 Responsibilities for Head of Personal Development and Head of Computing

- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.

1.3.6 Responsibilities for all members of staff are:

- Reading the school Staff Code of Conduct and adhering to them.
- Taking responsibility for the security of school systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.

1.3.7 The responsibilities of the pupils:

- Contributing to the development of online safety policies.
- Reading the Pupil IT Code of Conduct and adhering to the policy.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, behaving safely and responsibly to limit those risks.

1.3.8 The key responsibilities of parents and guardians are:

- Reading the Pupil IT Code of Conduct, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

2. Online Communication and Safer Use of Technology

Section 2 of the *WSCB Social Network Policy* has been consulted when developing this policy.

2.1. Managing the school website

- The Marketing Manager will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.

2.2. Publishing images and videos online.

- The school will ensure that all images and videos shared online are used in accordance with the school Data Protection Policy.
- The school will ensure that all use of images and videos take place in accordance other policies and procedures including Data Protection Policy, Staff Codes of Conduct and Mobile Phone Usage Policy.
- In line with the Data Protection Policy, written permission from parents or guardians will always be obtained before images/videos of pupils are electronically published.

2.3 Managing email

- Pupils may only use school provided email accounts for educational purposes.
- All members of staff are provided with a specific school 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.
- Access to school email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.

2.4 Official videoconferencing and webcam use for educational purposes

- Microsoft Teams is the only platform to be used for videoconferencing, remote working and remote learning.
- Detailed guidelines for staff and students are to be found in the Staff Code of Conduct and Pupil IT Code of Conduct.

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

- Internet use is a key feature of educational access and all children 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. Please access specific curriculum policies for further information.
- The school Internet access will be designed to enhance and extend education.
- Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision; classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability
- The school will balance children's ability to take part in age appropriate peer activities online with the need for the school to detect abuse, bullying or unsafe practice by children in accordance with the national minimum standards (NMS).
- All school owned devices will be used in accordance with the school Staff Code of Conduct and Pupil IT Code of Conduct Policy, Staff Portable Device Agreement Policy and with appropriate safety and security measure in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils 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.
- The school will use the Internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

2.6 Management of Microsoft Teams

- Leaders and IT staff will regularly monitor the usage of Microsoft Teams in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using Microsoft Teams.
- Only members of the current pupil, staff and Governor community will have access to Microsoft Teams.
- All users will be mindful of copyright issues and will only upload appropriate content onto Microsoft Teams.
- When staff, pupils' etc. leave the school their account or rights to specific school areas will be disabled.
- A visitor may be invited to join a Microsoft Teams meeting. In this instance there may be an agreed focus or a limited time slot.

3. Social Media Policy

Section 2.2 of the *WSCB Social Network Policy* has been consulted when developing this policy.

3.1. General social media use

- Social media is not allowed on school devices for pupils under 13. Pupils are allowed access to social media at specific times on completion of the online safety assessment at the end of the Spring term in UIV Computing lessons.
- Expectations regarding safe and responsible use of social media will apply to all members of the school community and exist in order to safeguard both the school and the wider community, on and offline.
- All members of the school 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 school community.
- All members of the school 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.
- The school will control pupil access to social media and social networking sites whilst on site and when using school provided devices and systems (See 6.04g Content Filter – website availability which differentiates according to age).
- Any concerns regarding the online conduct of any member of St Mary's School on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil 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 relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2 Official use of social media

- St Mary's official social media channels are: Twitter Link @StMarysCalne and Facebook @stmaryscalne and Instagram @stmaryscalne. Links can be reached through the website www.stmaryscalne.org.
- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 2018, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected and two factor authentication) and where appropriate, linked to the school website.

3.3 Staff personal use of social media

- Safe and professional behaviour will be outlined for all members of staff as part of the school Staff Code of Conduct.
- Members of staff are advised to wait until an ex-pupil's 18th birthday before accepting any request on social media. The young person should no longer be a pupil at St Mary's.

- If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- All communication between staff and members of the school community on school business will take place via official approved communication channels.
- 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 to ensure that their social media use is compatible with their professional role and is in accordance with school's policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.

3.4 Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.
- 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 the school.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.

3.5 Pupils use of social media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the IT Pupil Code of Conduct.
- Personal publishing on social media sites will be taught to pupils 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.
- Pupils 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, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils 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.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils 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.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts within school specifically for children under this age. See school policy on social media access.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.

4. Use of Personal Devices and Mobile Phones (including BYOD)

4.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the school to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by the school and is covered in appropriate policies and mobile phone etiquette guide.
- St Mary's recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/guardians but requires that such technologies need to be used safely and appropriately within schools.

4.2 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.
- Use of pupil mobile devices around the school is dependent on age and the mobile device policy of the boarding house.
- Members of staff will be issued with a work phone number and email address where contact with pupils or parents/guardians is required.
- All members of the school 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 the school's policies.
- Relevant staff are required to install -authentication apps to facilitate multi-factor authentication (MFA). This allow access to CPOMS and also, when working from home, access to iSAMS and Office 365. Teachers/staff are advised not to have work information on their private phone.

4.3 Pupils use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by children will take place in accordance with the Pupil IT Code of Conduct.
- Pupil's personal mobile phones should not be brought into lessons, unless in the Sixth Form where the device should be out of sight in the classroom.
- Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or any personal device which may send and receive data during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's behaviour or bullying policy or could contain nude and semi-nude images and/or videos. The phone or device may be searched by a member of the Leadership team and content may be deleted or requested to be deleted, if appropriate. Searches of mobile phone or personal devices will only be carried out in accordance with the school's policy. See Pupil IT Code of Conduct: *I understand that if I am suspected of breaking the policy agreement the school can search my personal laptop, iPad, phone or USB device. I will only use my personal devices in lessons with the express permission of the teacher and I will be discreet in using devices outside lessons in order to check my timetable or prep (in line with the mobile phone etiquette guide).*

4.4 Staff use of personal devices and mobile phones

- Members of staff are advised not use their own personal accounts for contacting pupils and their families within or outside of the school in a professional capacity.
- Staff should not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and should only use work-provided equipment for this purpose. See School Data Protection Policy, Staff Code of Conduct.

4.5 Visitors use of personal devices and mobile phones

- Use of mobile phones or personal devices by visitors and parents/guardians to take photos or videos must take place in accordance with the school's Data Protection Policy.
- In accordance with guidance from the Information Commissioner's Office, parents/guardians may take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). 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/guardians comment on any activities involving other pupils in the digital/video images.

The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	Yes		Yes	
Internet only				Yes		Yes
No network access						Yes

5. Policy Decisions

5.1. Reducing online risks

- St Mary's is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- St Mary's is working towards the *Online Safety Mark* using the *360 Safe* platform.
- The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. The school uses Bitdefender anti-virus software, Smoothwall for website filtering, Exchange 365 for email filtering, and the school's Internet provider, Oakford's firewall.
- For content that may be accessible which the web filter cannot detect (i.e. 3G, 4G, 5G or files already installed on a student's device) engagement approaches will be used to educate students (see section 6.1).
- The school 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 always possible to guarantee that access to unsuitable material will never occur via a school computer or device.

5.2 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign the relevant IT Code of Practice before using any school resources.
- Parents will be asked to read the Pupil IT Code of Conduct for pupil access and discuss it with their child, where appropriate.

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

5.3 Audit / Reporting

- Logs of filtering change controls and of filtering incidents will be made available to: The Designated Safeguarding Lead, The Deputy Designated Safeguarding Leads.

6. Engagement Approaches

6.1 Engagement and education of children and young people

- An online safety curriculum will be embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible Internet use amongst pupils.
- Education about safe and responsible use will precede Internet access.
- Pupils input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Pupils will be supported in reading and understanding the Pupil IT Code of Conduct in a way which suits their age and ability. This takes place in the IT Induction for all new starters.
- All users will be informed that network and Internet use will be monitored.
- Online safety will be included in the PD and Computing programmes of study, covering both safe school and home use. See the relevant schemes of work.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the school's internal online safety (e-Safety) education approaches. Such as visits from external experts.

6.2 Engagement and education of staff

- The Online 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 our safeguarding responsibilities.
- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
- 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 in a variety of ways, on a regular basis.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. 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.

6.3 Engagement and education of parents and guardians

- St Mary's School recognise that parents/guardians have an essential role to play in enabling children to become safe and responsible users of the Internet and digital technology.
- Parents' attention will be drawn to the school Online Safety Policy and expectations in newsletters, letters and on the school website.
- IT safeguarding topics will be included in the safeguarding section in the E-lily.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent talks, transition events and sports days.

7. Managing Information Systems

7.1 Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- Full information regarding the school's approach to data protection and information governance can be found in the school's Data Protection policy.

7.2 Security and Management of Information Systems

- The security of the school information systems and users will be reviewed regularly.
- Virus protection is installed and is updated regularly.
- Personal data sent over the Internet will be encrypted or accessed via appropriate secure remote access systems.
- Unapproved software will not be allowed in work areas or attached to email.
- All files will be stored using Microsoft cloud servers and are monitored. All backup will be through Barracuda Cloud-to-Cloud services.
- All users will be expected to log off or lock their screens/devices if systems are unattended.

7.3 Password policy

- Staff and pupils must always keep their password private and must not share it with others or log in as another user at any time.
- All members of staff and pupils will have their own unique username and private passwords to access school systems. Members of staff and pupils are responsible for keeping their password private.
- We require staff and pupils to use strong passwords for access into our system.
- We require staff and pupils to change their passwords every 120 days.

7.4 Filtering and Monitoring

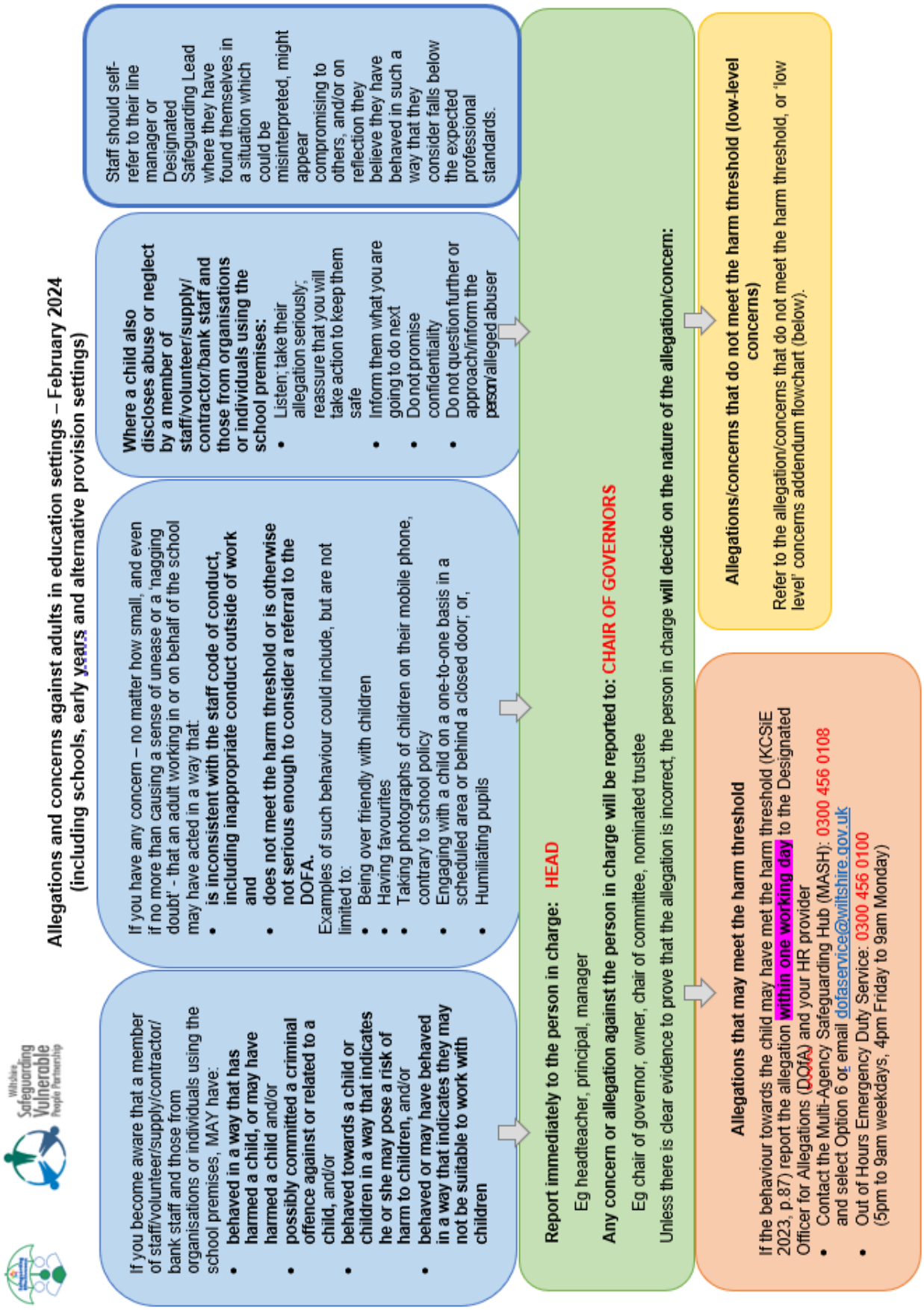
- The governors will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.
- The school's Internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- All monitoring of school owned/provided systems will take place to safeguard members of the community.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The school uses a private leased line with secure broadband connectivity; the leased line also has a spam and virus filter.
- The school uses Smoothwall web filter which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, and social media sites for the younger years.
- The school has a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
- The school's web filter will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
- Parents will be informed of the school's expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

8. Responding to Online Incidents and Safeguarding Concerns

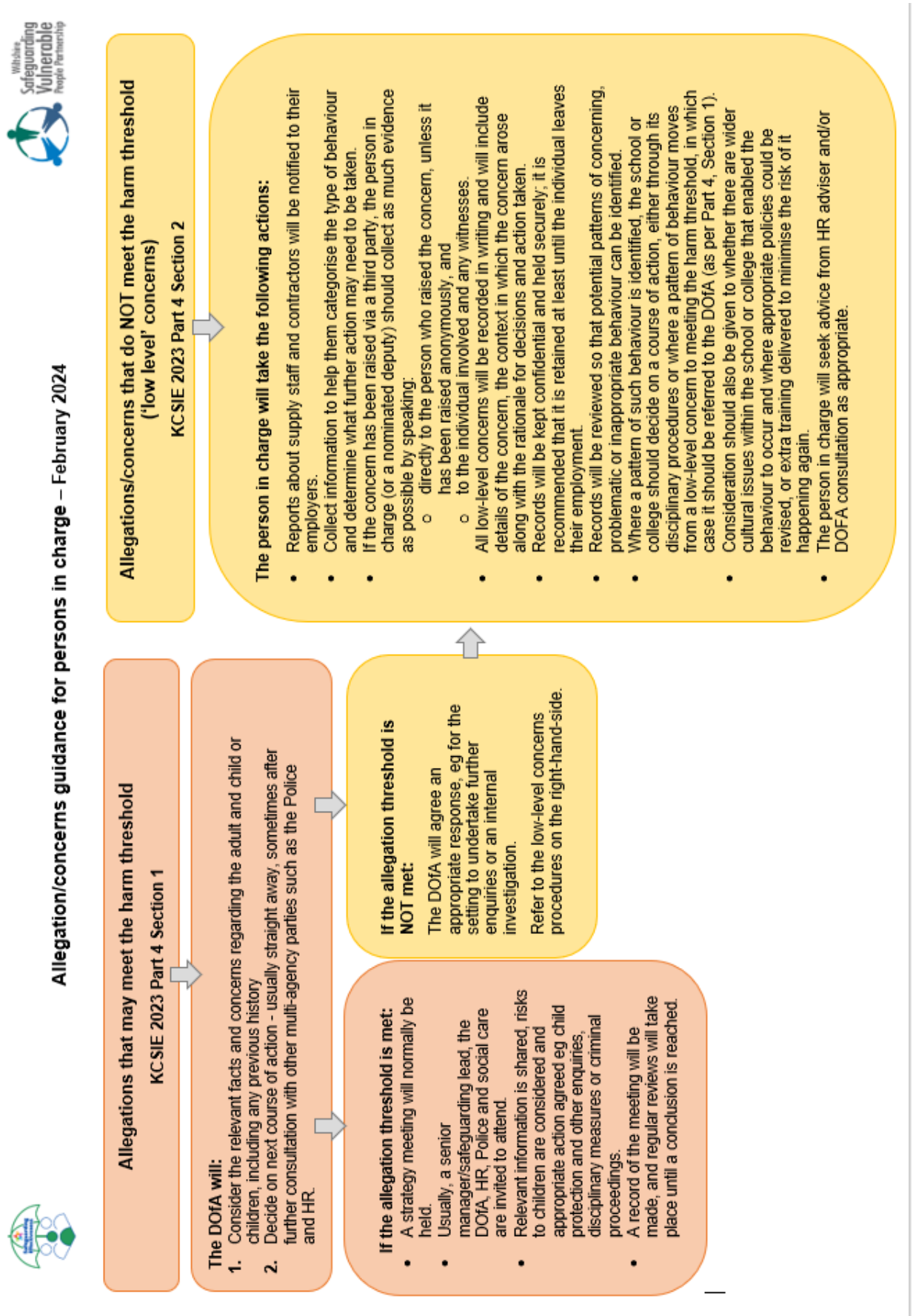
Section 2.8 of the *WSCB Social Network Policy* has been consulted when developing this policy.

- All members of the community will be made aware of the range of online risks that are likely to be encountered including consensual and non-consensual sharing of nude and semi-nude images and/or videos, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils. See St Mary's Child Protection policy and Anti-bullying policies.
- All members of the school community will be informed about the procedure for reporting online safety concerns, such as breaches of filtering, consensual and non-consensual sharing of nude and semi-nude images and/or videos, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Wiltshire Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure.
- Any complaint about staff misuse will be referred to the Head.
- Any allegations against a member of staff's online conduct will be discussed with the Wiltshire Designated Officer For Allegations (DOFA).
- Pupils, parents and staff will be informed of the school's complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school 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 school community.
- The school will manage online safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/guardians of any incidents of concerns as and when required.
- After any investigations are completed, the school 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 the school will contact the Education Safeguards Team or Wiltshire Police via 101 or 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 Wiltshire Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools in Wiltshire.
- Parents and children will need to work in partnership with the school to resolve issues.

SVPP flowchart 'Allegations against adults'

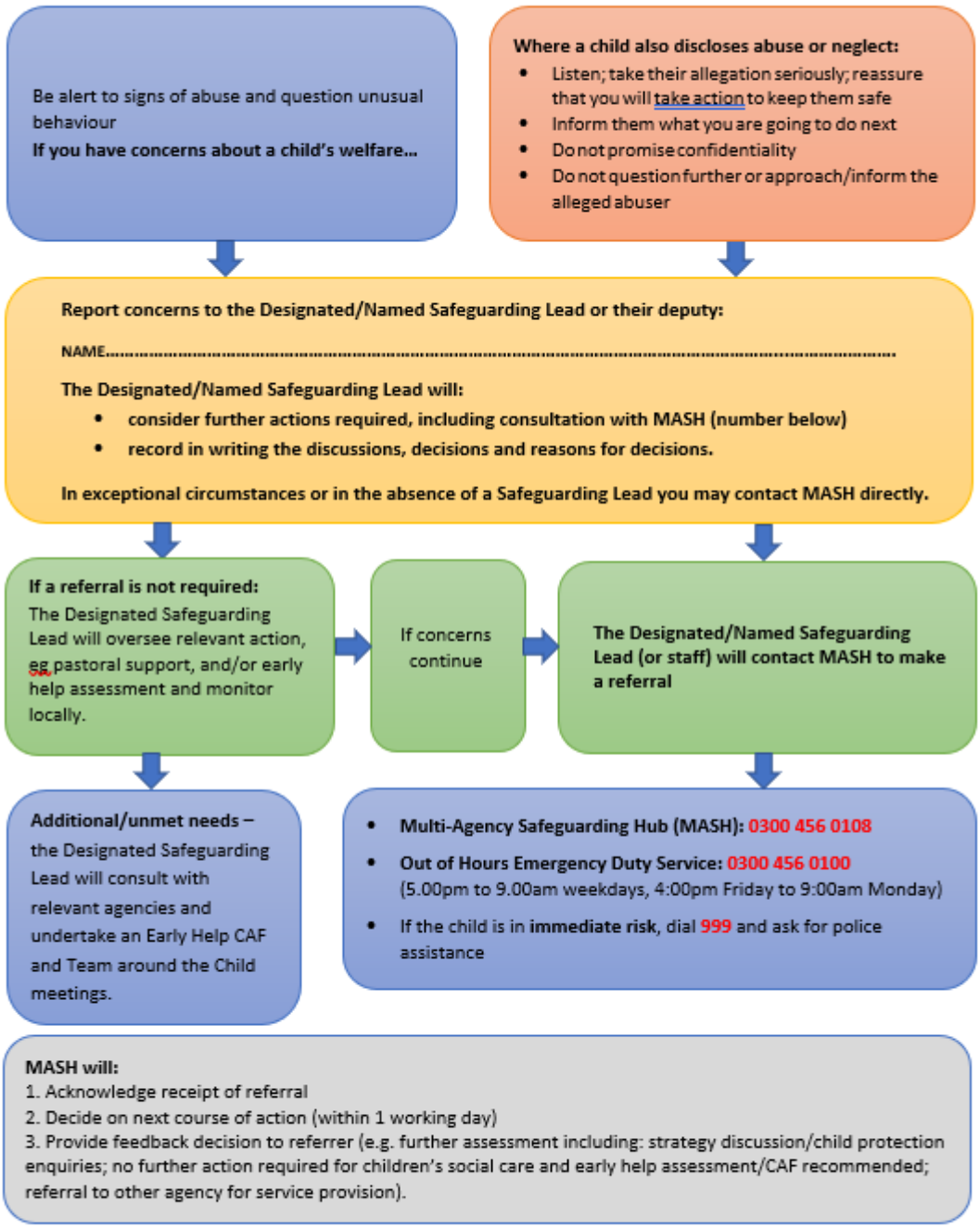


SVPP flowchart 'What to do if you're worried a child is being abused/neglected'



What to do if you are worried a child is being abused or neglected

for staff, volunteers and visitors in all agencies and settings



This flowchart is intended for use as a brief guide. Refer to the DfE Guidance What to do if you are worried a child is being abused for more information, definitions and possible indicators of abuse (including child sexual exploitation).

SVPP website: www.wiltshirescb.org.uk

Reviewed: September 2020

APPENDIX A

9. Procedures for Responding to Specific Online Incidents or Concerns

Section 2.7 of the *WSCB Social Network Policy* has been consulted when developing this policy.
See St Mary's Child Protection Policy

9.1 Responding to concerns regarding consensual and non-consensual sharing of nude and semi-nude images and/or videos

- St Mary's ensures that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery.
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/guardians. (Delivered primarily through the Personal Development and Wellbeing curriculum, supported by the Computing Department and lectures.)
- St Mary's views consensual and non-consensual sharing of nude and semi-nude images and/or videos as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (Mrs S Toland).
- The school will log non-reports (those we do not report to the Police) via CPOMS. The school will also decide whether to report to MASH and Police if necessary.
- If the school is made aware of an incident involving youth produced sexual imagery the school will:
    - Act in accordance with the school's child protection and safeguarding policy and the relevant Wiltshire Safeguarding Child Boards procedures.
    - Immediately notify the designated safeguarding lead.
    - Store the device securely.
    - Carry out a risk assessment in relation to the children(s) involved.
    - Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care and/or the police (as needed/appropriate).
    - Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Implement appropriate sanctions in accordance with the school's behaviour policy but taking care not to further traumatise victims where possible.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
    - Inform parents/guardians about the incident and how it is being managed.
- The school will not view 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 (in these cases the image will only be viewed by the Designated Safeguarding Lead).
- The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school's network or devices then the school will take action to block access to all users and isolate the image.
- The school will take action regarding creating youth produced sexual imagery, regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

9.2. Responding to concerns regarding Online Child Sexual Abuse and Exploitation

See St Mary's Child Protection Policy

- St Mary's will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/guardians.
- St Mary's views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead: Mrs S Toland.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Wiltshire Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the CSE team by the DSL.
- If the school is made aware of an incident involving online child sexual abuse of a child then the school will:
    - Act in accordance with the school's child protection and safeguarding policy and the relevant Wiltshire Safeguarding Child Boards procedures.
    - Immediately notify the designated safeguarding lead.
    - Store any devices involved securely.
    - Immediately inform Wiltshire police via 101 (using 999 if a child is at immediate risk)
    - Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care (if needed/appropriate).
    - Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/guardians about the incident and how it is being managed.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.
- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.

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

- St Mary's will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an Internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Wiltshire Police.
    - If the school is made aware of Indecent Images of Children (IIOC) then the school will:
    - Act in accordance with the school's child protection and safeguarding policy and the relevant Wiltshire Safeguarding Child Boards procedures.
    - Immediately notify the school Designated Safeguard Lead.

- Store any devices involved securely.
- Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Wiltshire police via 101 (using 999 if a child is at immediate risk) and/or the Wiltshire Designated Officer for Allegations (DOFA) (if there is an allegation against a member of staff).

- If the school is made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the Internet then the school will:
  - Ensure that the Designated Safeguard Lead 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.
- If the school is made aware that indecent images of children have been found on the school's electronic devices then the school will:
  - Ensure that the Designated Safeguard Lead 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 children's social services (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.
- If the school is made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
  - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
  - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  - Inform the Multi-Agency Safeguarding Hub (MASH) and other relevant organisations in accordance with the school's managing allegations policy.
  - Follow the appropriate school policies regarding conduct.

9.4. Responding to concerns regarding radicalisation and extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the Internet in schools and that suitable filtering is in place which takes into account the needs of pupils. iBoss advanced filter system is in operation with CIPA compliant filters to ensure safe content. iBoss also monitors Internet searches and logs emails; Impero monitors activity on Computer Room PCs.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear whether a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or Wiltshire Police.

9.5 Responding to concerns regarding cyberbullying. **See St Mary's Anti Bullying Policy**

- Cyberbullying, along with all other forms of bullying, of any member of St Mary's community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear whether a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Wiltshire Police.

- Pupils, staff and parents/guardians will be advised to keep a record of cyberbullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/guardians will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
    - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the school's anti-bullying, behaviour policy or Pupil IT Code of Conduct.
    - Parent/guardians of pupils 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

- Personal online hate at St Mary's will not be tolerated. Further details are set out in the school policies regarding anti-bullying and behaviour policies.
- All incidents of online hate reported to the school will be recorded.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.
- The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Wiltshire Police.

APPENDIX B

10. Legislation

It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

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

Data Protection Act 2018

- Full details of the at https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Freedom of Information Act 2000

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

Communications Act 2003

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

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

- It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:
- Establish the facts.
- Ascertain compliance with regulatory or self-regulatory practices or procedures.
- Demonstrate standards, which are or ought to be achieved by persons using the system.
- Investigate or detect unauthorised use of the communications system.
- Prevent or detect crime or in the interests of national security.
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
  - Ascertain whether the communication is business or personal;
  - Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-

commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

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

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

Racial and Religious Hatred Act 2006

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

Protection from Harassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 constitutes the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

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

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

- Prohibition of discrimination.
- The right to education.

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

The Education and Inspections Act 2006

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

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / guardian to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

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