We ***place our children at the heart of all we do***,
inspired by the love, life and teachings of Jesus.

"I am the way, the truth and the life."
(John 14:6)

Nurture, **Prepare**, **Support**, **Enable**

Online Safety Policy

This policy should be read in conjunction with Acceptable use of the internet policies, ICT policy, Child-Protection and Safeguarding, Tackling Extremism and Radicalisation, CAST Data Protection, Mobile Phone, CAST Social Media and Anti- Bullying Policies.

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Full Governing Body receiving regular information about online safety incidents and monitoring reports.
Mr. Bob Kiszcuk has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator / Officer
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant governors and board meetings

Headteacher and Senior Leaders

The Headteacher is the online safety lead and has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety.

The Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

The Headteacher and Senior Leaders are responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead - The headteacher is the online safety lead

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / MAT
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team

Technical staff - NCI

Technical Staff / Co-ordinator for ICT is responsible for ensuring:

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

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

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

Designated Safeguarding Lead

The Designated Safeguarding Lead and Deputy DSL should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- peer on peer abuse
- potential or actual incidents of grooming
- online-bullying

<u>Education –Pupils</u>

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety and digital literacy is therefore an essential part of the online safety provision at St. Mary's. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum should be provided as part of Computing / PHSE and should be regularly revisited. The first computing lesson in each term/topic should focus on digital literacy.
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the online safety lead or technical staff (NCi) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education –Parents

Parents and carers may have an essential role in the continuing education of their children and in monitoring their online experiences. Parents may underestimate how often children may come across inappropriate material on the internet and are often unsure about what they would do about it.

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

- Letters
- Newsletters
- Website
- Parent information meetings
- High profile events / campaigns e.g. Safer Internet Day, NSPCC
- Reference to the relevant web sites / publications e.g. *swgfl.org.uk* *www.saferinternet.org.uk/* http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school / academy Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Online Safety Lead will provide advice / guidance / training to individuals as required

Training – Governors

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

- Attendance at training provided by the Local Authority / Plymouth CAST
- Participation in school / academy training / information sessions for staff or parents (this may include attendance at assemblies / lessons).
- Online training via SSS.

Technical – infrastructure / equipment, filtering and monitoring

In conjunction with NCI and Plymouth CAST, the school will be responsible for ensuring that our infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. All procedures are managed in line with the expectations outlined in KCSIE.

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- Users are responsible for the security of their username and password and will be required to change their password regularly.
- The ICT Co-ordinator is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected

licensing costs)

- Internet access is filtered for all users**.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- There is a clear process in place to deal with requests for filtering changes
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school / academy has provided enhanced / differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. They are provided with group network access.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school / academy events for their own personal use (as such use is not covered by the Data Protection Act/GDPR regulations). 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 / carers comment on any activities involving other pupils in the digital / video images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.

Communications

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

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and children are able to use the school email service to communicate electronically with others when in school
- Staff and children need to be aware that email communications may be monitored
- Staff and children must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Teachers and children may communicate electronically via their Class Dojo and Showbie accounts. On Showbie, class discussions are available only to those children in the class and are considered safe and secure. Children are taught to use the discussion forum in a polite and respectful manner.
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class, group or individual email addresses will be used, for educational use.
- Children should only bring mobile phones into school in accordance with the school policy. The phone will be handed to a member of school staff to be kept securely during the school day.

Sexting

St Mary's School ensures that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating child produced sexual imagery (known as "sexting"). We view "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead

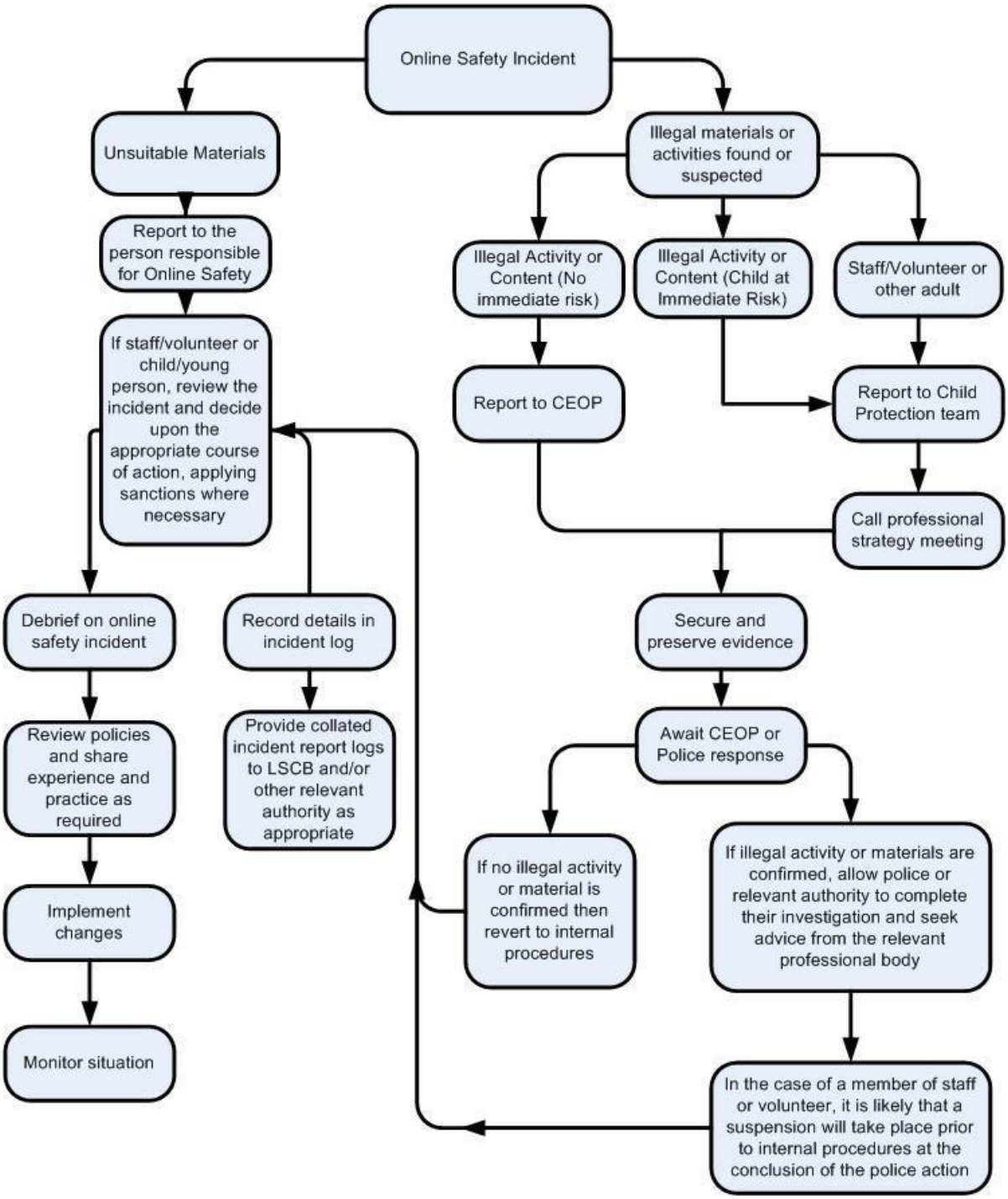
The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people'
If the school are made aware of incident involving child produced sexual imagery the school will:

- Act in accordance with the schools Child protection and Safeguarding policy
- 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 schools 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/carers about the incident and how it is being managed.
- The school will not view any images suspected of being child 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 and a senior member of staff).
- 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/settings network or devices, then the school will take action to block access to all users and isolate the image.
- We will take action regarding creating child produced sexual imagery, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
- We will ensure that all members of the community are aware of sources of support regarding child produced sexual imagery

Responding to incidents of misuse

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

Illegal Incidents



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

Other Incidents

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

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

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

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

Review and Monitoring

NCI provide the internet filtering and monitoring. Regular meetings are held with NCI to ensure that these systems are robust and fit for purpose. Any significant breaches of the filter would trigger a review

Policy September 2025

To be reviewed annually, by September 2026