Learning to love
Loving to learn

Philosophy

Today's children and young people are growing up in a digital world. As they grow older, it is crucial that they learn to balance the benefits offered by technology with a critical awareness of their own and other's online behavior and develop effective strategies for staying safe and making a positive contribution online. At St Mary's First School we provide children with the resilience and competence to use the internet safely and effectively. Online safety is embedded throughout computing planning and will provide children with the opportunity to learn how to be responsible users online. This will be covered across 4 key areas: pupil behaviour, parental engagement, staff awareness and curriculum development. This is included in the progression of skills from EYFS to Year 4. We use the Education for a Connected World framework published by UK Council for Child Internet Safety (UKCCIS) to help develop the skills and competences that children and young people need to have at different ages and stages in order to be able to navigate the online world safely and responsibly.

Monitoring

The school will monitor the impact of this policy using:
- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

The policy applies to all members of the school community including staff, children, volunteers, parents, visitors and community users who have access to the school ICT systems, both in and out of school.

Roles and Responsibilities

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 Curriculum Committee receiving regular information about online safety incidents and monitoring reports. Margaret Sherwin is our Online Safety Governor. The role of the Online Safety Governor will include:
- regular meetings with the Head teacher
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to the curriculum committee

Headteacher:
- has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Officer.
- and (at least) another member of 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.
- is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- 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.

Network Manager (Staffs Tech) is responsible for ensuring:
- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety Guidance that may apply.

- that users may only access the networks and devices through a properly enforced password protection policy
- 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 and email is regularly monitored in order that any misuse can be reported to the Headteacher and online safety coordinator for investigation
- that monitoring systems are implemented and updated as required
- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices

School Staff are responsible for ensuring that:
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher
- all digital communications with students / 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
- children understand and follow the Online Safety Policy and Acceptable User Agreement
- children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned children 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

Children:
- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking and use of images and on cyber-bullying
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

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

Community:
Community users will be expected to sign a Community User Agreement.

Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating children

to take a responsible approach. The education of children in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum should be provided as part of Computing and other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Children should be taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information
- Older children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Children 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
- Children 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 children 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 children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the children visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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.

Many parents have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents.

It is essential that all staff and Governors receive online safety training and understand their responsibilities.

Technical – equipment, filtering and monitoring

The school will be responsible for ensuring that the network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will be effective in carrying out their online safety responsibilities There will be regular reviews and audits of the safety and security of school technical systems:

• Servers, wireless systems and cabling must be securely located and physical access restricted.

• All users will have clearly defined access rights to school technical systems and devices.

• All users will be provided with a username and secure password by the Office Manager, who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every year.

• The "master or administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.

• The office manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software

installations (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 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.
• Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
• The school has provided differentiated user-level filtering (allowing different filtering levels for different groups of users – staff, children etc)
• 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.
• An appropriate system is in place for users to report any actual or potential technical incident or security breach to the relevant person, as agreed.
• 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 place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
• An agreed policy is in place regarding the extent of personal use that staff users and their family members are allowed on school devices that may be used out of school. All staff must seek permission before downloading executable files and installing programmes on school devices.
• An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the 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 children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and children need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.
When using digital images, staff should inform and educate students / 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 eg on social networking sites. Further information can be found on the school's Mobile Phone and Digital Technology Policy.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the GDPR and the Data Protection Act 2018. Personal data must be:
•   Fairly and lawfully processed
•   Processed for limited purposes
•   Adequate, relevant and not excessive
•   Accurate
•   Kept no longer than is necessary
•   Processed in accordance with the data subject's rights
•   Secure
•   Only transferred to others with adequate protection.
The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Staff must ensure that they:
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:
- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred, or its use is complete

Communications

When using communication technologies the school considers the following as good practice:
- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and parents must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while children at KS2 and above will be provided with individual school email addresses for educational use.
- Students / pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

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

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:
- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

- Risk assessment, including legal risk.

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

Unsuitable / inappropriate activities

The school believes that the activities referred to in appendix 1 would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as identified.

Appendix 2 highlights steps to be taken 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.

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

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

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. 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
- 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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

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

members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour or disciplinary procedures.

Agreed by staff and governing body – October 2021
Review October 2022

Appendix 1

User Actions

		Acceptable	Acceptable at certain	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	

Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)				X	
On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce		X			
File sharing		X			
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting eg Youtube	X				

Appendix 2

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.

```
                          ┌─────────────────────┐
                          │ Online Safety Incident│
                          └─────────────────────┘
            ┌──────────────┘                    └──────────────┐
  ┌──────────────────┐                              ┌──────────────────────┐
  │ Unsuitable Materials│                           │ Illegal materials or │
  └──────────────────┘                              │ activities found or  │
            │                                        │ suspected            │
  ┌──────────────────┐                              └──────────────────────┘
  │ Report to the    │          ┌───────────────┬───────────┴──────────┐
  │ person responsible│   ┌─────────────┐  ┌─────────────┐  ┌─────────────┐
  │ for Online Safety│   │ Illegal Activity│ │ Illegal Activity│ │ Staff/Volunteer or│
  └──────────────────┘   │ or Content (No │ │ or Content (Child│ │ other adult │
            │             │ immediate risk)│ │ at Immediate Risk)│ └─────────────┘
  ┌──────────────────┐   └─────────────┘  └─────────────┘         │
  │ If staff/volunteer │          │                          ┌─────────────┐
  │ or child/young    │   ┌─────────────┐                    │ Report to Child│
  │ person, review the│   │ Report to CEOP│                  │ Protection team│
  │ incident and decide│  └─────────────┘                    └─────────────┘
  │ upon the          │          │                                  │
  │ appropriate course│                                      ┌─────────────┐
  │ of action, applying│                                     │ Call professional│
  │ sanctions where   │                                      │ strategy meeting│
  │ necessary         │                                      └─────────────┘
  └──────────────────┘                                              │
    ┌───────┴────────┐          ┌─────────────┐           ┌─────────────┐
┌──────────┐  ┌─────────────┐   │ Record details│         │ Secure and  │
│ Debrief on│  │ Record details│ │ in incident log│        │ preserve evidence│
│ online    │  │ in incident log│└─────────────┘          └─────────────┘
│ safety    │  └─────────────┘          │                        │
│ incident  │          │         ┌─────────────┐           ┌─────────────┐
└──────────┘           │         │ Provide collated│       │ Await CEOP or│
    │                  │         │ incident report│        │ Police response│
┌──────────┐           │         │ logs to LSCB   │        └─────────────┘
│ Review    │          │         │ and/or other   │     ┌──────┴────────┐
│ policies  │          │         │ relevant       │ ┌─────────────┐ ┌─────────────┐
│ and share │          │         │ authority as   │ │ If no illegal│ │ If illegal   │
│ experience│          │         │ appropriate    │ │ activity or  │ │ activity or  │
│ and       │          │         └─────────────┘  │ material is  │ │ materials are│
│ practice  │          │                          │ confirmed    │ │ confirmed,   │
│ as required│         │                          │ then revert  │ │ allow police │
└──────────┘           │                          │ to internal  │ │ or relevant  │
    │                  │                          │ procedures   │ │ authority to │
┌──────────┐           │                          └─────────────┘ │ complete     │
│ Implement │          │                                          │ their        │
│ changes   │          │                                          │ investigation│
└──────────┘           │                                          │ and seek     │
    │                  │                                          │ advice from  │
┌──────────┐           │                                          │ the relevant │
│ Monitor   │          │                                          │ professional │
│ situation │          │                                          │ body         │
└──────────┘           │                                          └─────────────┘
                       │                                                 │
                       │                                          ┌─────────────┐
                       │                                          │ In the case of│
                       │                                          │ a member of  │
                       │                                          │ staff or     │
                       │                                          │ volunteer, it│
                       │                                          │ is likely    │
                       │                                          │ that a       │
                       │                                          │ suspension   │
                       │                                          │ will take    │
                       │                                          │ place prior  │
                       │                                          │ to internal  │
                       │                                          │ procedures at│
                       │                                          │ the conclusion│
                       │                                          │ of the police│
                       │                                          │ action       │
                       │                                          └─────────────┘
```

Flowchart: Online Safety Incident

- **Online Safety Incident** branches into:
  - **Unsuitable Materials**
    - Report to the person responsible for Online Safety
    - If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
      - Debrief on online safety incident
        - Review policies and share experience and practice as required
          - Implement changes
            - Monitor situation
      - Record details in incident log
        - Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
  - **Illegal materials or activities found or suspected** branches into:
    - **Illegal Activity or Content (No immediate risk)**
      - Report to CEOP
    - **Illegal Activity or Content (Child at Immediate Risk)**
      - Report to Child Protection team
    - **Staff/Volunteer or other adult**
      - Report to Child Protection team
        - Call professional strategy meeting
          - Secure and preserve evidence
            - Await CEOP or Police response
              - If no illegal activity or material is confirmed then revert to internal procedures
              - If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
                - In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action