E- Safety Policy

St Mary's CE Infant School

"Together we love to learn and learn to love."

St Mary's CE Infant school is committed to inspiring every individual. We embed the Christian value of love across school life because we believe that a person who feels loved, secure and happy can flourish. We encourage everyone to achieve their potential, develop their talents, celebrate their uniqueness, and rejoice in their relationships with others.

"Do everything in love" **1 Corinthians 16:14**

Approved by:	**Joint Local Governing Body**
Date:	**11 September 2023**
Next review date:	**September 2025**

E-Safety Policy

Introduction

This E-Safety Policy has been written based on guidance provided by South West Grid for Learning, UK Safer Internet Centre, CEOP materials and ODST's Online Safety Guidance and Data Protection Policy (including GDPR). It has been adapted to reflect the school's own decisions on balancing educational benefit with potential risks.

This E-Safety Policy will be used in conjunction with our school documentation:

- Curriculum Statement for Computing and Computing Curriculum Plan & Scheme of Work
- Behaviour Policy
- Anti Bullying Policy
- Child Protection and Safeguarding Policy
- Code of Conduct for Parents and Carers and our Pupil/Parent Acceptable User Agreements
- Mobile Phones Cameras Policy
- Data Protection Policy
- PSHE Curriculum Scheme of Work

Whole school e-safety training and support takes place annually for pupils, parents and teaching staff. E-safety is explicitly taught to all year groups through termly Project Evolve lessons and is implicit throughout our Computing scheme of work (Teach Computing). E-safety is also covered in our PSHE Curriculum (SCARF PSHE). We also take part annually in Safer Internet Day (A National Awareness Event held in February each year) using materials provided by Safer Internet Centre.

The Executive Headteacher, as Deputy Designated Safeguarding Lead, will act as e-safety co-ordinator, supported by the Computing Lead. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following e-safety procedures.

Rationale

The internet and other digital technologies permeate all aspects of life in the modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies in order to enrich his/her learning.

Scope

This policy applies to all members of our St Mary's CE Infant School community including pupils, staff, parents/carers, Governors, volunteers and visitors.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's policies on Behaviour and Anti-Bullying.

The school will deal with such incidents within this policy and associated policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Objectives

Our aims are to ensure that all pupils will:

- use the internet and other digital technologies to support, extend and enhance their learning
- develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material
- develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working
- use existing, as well as up and coming technologies safely

Internet use will support, extend and enhance learning:

- Pupils will be given clear objectives for internet use
- Web content will be subject to age appropriate filters
- Internet use will be embedded in the curriculum

Pupils will develop an understanding of the uses, importance and limitations of the internet by:

- learning how to effectively use the internet for research purposes
- learning how to evaluate information on the internet
- learning how to report inappropriate web content
- developing a positive attitude to the internet
- developing their ICT capability through opportunities to engage in independent and collaborative learning
- using the internet to enhance their learning experience

Pupils will use existing technologies safely:

Pupils will be taught about e-safety both through discrete lessons (see computing and PSHE curriculum) and the implicit curriculum where e-safety remains high on the agenda.

Related Policies (available on the Policies page of the school website)

- Child Protection and Safeguarding Policy
- Data Protection Policy
- Equalities Policy
- Behaviour Policy
- Mobile Phone Camera Policy
- Code of Conduct for Parents and Carers
- Code of Conduct for Staff

Roles and Responsibilities for Internet Safety

Executive Headteacher (as part of a wider child protection role):

- be responsible for e-safety issues within the school with the support and day to day responsibility of the Assistant Headteacher.
- ensure the Governing body is informed of e-safety issues and policies
- ensure that appropriate funding is allocated to support e-safety activities throughout the school
- establish and maintain a safe ICT learning environment

- establish and maintain a school wide e-safety programme
- respond to e-safety policy breaches in an appropriate and consistent manner in line with policies and maintain an incident log
- regular monitoring of e-safety incident logs
- reporting of e-safety incidents to Governing body
- regular monitoring of filtering / change control logs with support of 123ICT Services
- develop parental awareness
- develop an understanding of relevant legislation and take responsibility for their professional development in this area

Governing Body

- our named Safeguarding Governor will ensure that safety is included as part of the regular review of child protection and health and e-safety policies
- support the Head of School and/or Computing Lead in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment
- attend relevant training provided by ODST Academy
- participate in school training sessions for staff, pupils or parents (this may include attendance at assemblies/lessons)

Teaching and Support Staff should ensure they:

- have read the ODST Code of Conduct for Staff before using technology equipment in school
- adhere to pupil acceptable user agreements (Appendix A & B)
- have read the current E-Safety Policy
- take responsibility for the security of data as set out in Data Protection Policy (with particular reference to GDPR)
- develop an awareness of e-safety issues and how they relate to pupils in their care
- support regular teaching of e-safety in the curriculum
- deal with e-safety issues they become aware of and know when and how to de-escalate potential incidents
- maintain a professional level of conduct in their personal use of technology, both within and outside school
- all digital communications with other members of staff, pupils and parents/carers should be on a professional level and only carried out using official school systems including school email address
- report any suspected misuse or problem to the Executive Headteacher at the earliest opportunity, using the e-safety reporting log (Appendix D)
- guide pupils to sites checked as suitable when internet use in lessons is pre-planned and respond quickly and appropriately for dealing with any unsuitable material that is found in internet searches

All Staff and Governors should be familiar with the school's policy including:

- safe use of email, using only school provided email addresses for school related communication
- safe use of the internet
- safe use of social networking sites in private time
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/ photographs on the school website
- procedures in the event of misuse of technology by any member of the school community (see appendices)

The E-Safety Policy will be shared with new staff and Governors as part of their induction.

E-safety information and Pupil Acceptable User Agreements (Appendix A & B) are available on the shared drive and sent to families when children join the school. Pupil Acceptable User Agreements (KS1 & KS2) are also displayed in classroom and referred to regularly.

Pupils

Pupils have a role to play in ensuring that their learning is supported by the safe and secure use of the internet, new technologies and mobile devices. To remain both safe and legal when using the internet, they will need to understand the appropriate behaviours and critical thinking skills and show that they:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable User Agreements KS1 & KS2 (Appendix A & B)
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- know and understand policies on the use of mobile devices and digital cameras
- know and understand appropriate taking/use of images and what is considered to be cyber-bullying at an age appropriate level (Appendix G)
- understand the importance of adopting good e-safety practice when using digital technologies out of school and know which adults they can ask for help if/when something goes wrong

Parents and Carers

Parents and carers 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 encourages parents and carers to support the school in promoting good e-safety practice:

- Discuss e-safety issues with their children, support the school in its e-safety approaches and reinforce appropriate behaviours at home
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Liaise with the school if they suspect or have identified that their child is conducting risky behaviour online
- Use digital and video images taken at school events for their own personal use only
- Adhere to the guidelines set out in the school's Mobile Phone Camera Policy
- Inform the school if their child needs to bring a mobile phone/device to school for safe- keeping during the school day

The school will seek to provide information and awareness to parents and carers and the wider community through:

- parent/pupil information events held at school
- curriculum activities
- newsletters and website
- e-safety page on the school website with further information
- Pupil Acceptable User Agreement
- National events: Safer Internet Day
- Reference to relevant websites/publications eg
  www.saferinternet.org.uk/
  www.childnet.com/parents-and-carers

Technical – Infrastructure Equipment, Filtering and Monitoring
St Mary's CE Infant School has a managed ICT service provided by 123ICT since 2012. It is the responsibility of the Governing Body to ensure that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved are implemented.

It is also the responsibility of the Governing Body to ensure that 123ICT are effective in carrying out their e-safety responsibilities:

- there will be regular reviews and audits of the safety and security of our 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
- the administrator password for the school ICT system must be available to the school Business Manager and stord securely on the shared drive.
- the School Business Manager with the support of 123ICT will be responsible for ensuring software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- internet access is filtered for all users and content lists are regularly updated and internet use is logged and regularly monitored
- there is a clear process in place to deal with requests for filtering changes
- the school has provided enhanced/differentiated user-level filtering
- regular monitoring and recording of the activity of users on the school technical systems

See Meeting digital and technology standards in schools and colleges audit (Appendix C)

E-Safety Curriculum Provision
Computing and on-line resources are increasingly used across the curriculum. At St Mary's CE Infant School we believe the education of pupils in e-safety is an essential part of the school's curriculum provision. We believe that our pupils need the help and support of both our school community and a well-planned curriculum to recognise and avoid e-safety risks and build their resilience. We ensure that the e-safety curriculum used at St Mary's is broad, age relevant and appropriate, and provides progression with opportunities for creative activities.

We continually look for ways to promote e-safety through:

- delivery of e-safety teaching specifically through computing and PSHE schemes of work as well as partaking in the National Safer Internet Day as a whole school event each February
- responding to need and opportunities to educate pupils on the dangers of technologies that may be encountered outside school
- teaching about copyright and the need to respect other people's information and images
- regular distribution of pupil questionnaires on issues of safety, including e-safety
- involving school council to represent pupil voice on issues and concerns around e-safety
- raising awareness of the impact of cyber bullying through Collective Worship, PSHE, work around anti-bullying strategies and the display of pupil posters
- providing pupils with a safe message of "tell a trusted adult" if they experience problems or need advice over internet and related technologies use
- helping pupils to understand the need for the Pupil Acceptable User Agreement (Appendix A & B) and the need to adopt safe and responsible use both within and outside school

- teaching children how to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussion and the computing curriculum
- staff acting as good role models in their use of digital technologies, the internet and mobile devices

Seesaw

In September 2023, St Mary's adopted Seesaw, an accessible, digital learning platform well suited to primary school aged children to deliver homework provision and remote learning should this be required in the future.

To support e-safety in using this platform:

- pupil log ins are shared electronically with parents via class teacher emails and paper copies are also sent home
- parental consent is required (Appendix H) and pupil access is disabled if this consent is not received
- parents and pupils are advised that pupil log in details should not be shared on social media or any other public forum (Appendix H)
- pupils are regularly reminded to keep their codes safe
- pupils are reminded of the importance of signing out of their account once their work is finished
- individual pupil home learning codes only give access to a pupil's own account
- class teacher Seesaw accounts are set up with their school email address
- parents are given details of Seesaw Privacy, Safety and Security (Appendix I)
- class accounts are set up to disable:
    - pupils ability to comment on their own and others work
    - pupils cannot see each others work
    - new items submitted require teacher approval before review
    - family access is disabled
    - pupil blog facility is disabled

Managing Internet Access

- Parents and children will together read, sign and return a Pupil Acceptable User Agreement upon commencement of school and at the beginning of KS2 (Appendix A & B as appropriate).
- Pupils will be taught to use the internet responsibly and to report any inappropriate content to a responsible adult.
- Pupils will have staff supervised access to Internet resources
- Staff will preview any recommended sites before use
- Staff will be vigilant in monitoring the content of the websites used by pupils
- Raw image searches are discouraged when working with pupils
- Specific sites that have been previously checked by a teacher will be suggested for homework activities.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported using the e-safety log Form (Appendix D) available via the shared drive and reported immediately to the Executive Headteacher. A request to 123ICT for the site to be blocked will be actioned.
- Any new games and internet sites that become available and are deemed to be inappropriate can also be blocked by 123ICT on teacher request via the e-safety log Form (Appendix D) available via the shared drive.
- The school will ensure that relevant filtering and anti-virus protection is installed and kept up-to- date on all school machines by 123ICT

E-mail

- staff are provided with a school email account to communicate with staff, parents, Governors and the education community when using the school network
- pupils are encouraged to tell a parent or member of staff if they receive inappropriate email communications
- pupils will only use e-mail for approved activities

Communication and Mobile Technology
Pupils are only allowed to have mobile phones or other personal handheld technology in school with the permission of the Executive Headteacher and must be kept in the school office during school hours.
When pupils are using mobile technology (their own or that provided by the school) they will be required to follow the school's Mobile Phone Cameras Policy.
Such items can be confiscated by school staff if they have reason to think that they are being used to compromise the wellbeing and safety of others. (Education and Inspections Act 2006, Sections 90, 91 and 94).

Use of Digital and Video Images
As a school, we are aware that 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 cyberbullying to take place
- remain available on the internet forever
- cause harm or embarrassment to individuals in the short or longer term

Our e-safety curriculum teaches pupils about these risks with the intention of reducing the likelihood of the potential for harm. Pupils in particular should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

Images of children in school and on educational visits should only be taken on school equipment. Images of children included on the school website/social media accounts are done so with parent/carer consent via the Data Protection Sheet when their child starts school. Pupil names are not attached to or captured within the images themselves. Parents/carers are reminded at events eg class assemblies, performances that the taking of videos and digital images of their children must be for their own personal use and not be published or made publicly available on social networking sites.

Data Protection
Our school aims to ensure that all personal data (paper and electronic format) collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the

General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 as set out in the Data Protection Bill. Please refer to the Data Protection Policy including GDPR (available on the school website) for detailed information.

Roles and Responsibilities for Data Protection

Executive Headteacher
The Executive Headteacher acts as the representative of the data controller on a day-to-day basis – she is supported in this by the School Business Manager.

The Governing Body
The Governing Body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data Protection Officer (DPO)
Julian Hehir (ODST DPO) is the first point of contact for individuals whose data the school processes.

All Staff
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with GDPR regulations (see Data Protection Policy including GDPR 2018)
- Informing the school of any changes to their personal data
- Ensuring that staff laptops are password protected and details of these kept by the School Business Manager securely in the school office
- Contacting Julian Hehir (ODST DPO) in the following circumstances:
    - With any questions about the operation of the ODST Data Protection Policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that the ODST Data Protection Policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

Systems Security
ICT systems will be reviewed regularly with support from our School Network provider and 123ICT.

Training for School Leadership Team and Governors
The Executive Headteacher, Head of School, Computing Lead and a member of the Governing Body will attend/receive regular e-safety training and updates provided by the ODST Academy.

Web Filtering
The school will work with 123ICT to ensure that appropriate filtering is in place. Pupils are encouraged to report any inappropriate content accessed (deliberate or accidental) to an appropriate member of staff and this will be recorded on the e-safety Incident reporting log (Appendix D) and reported to the Headteacher. Staff can also request a site to be blocked and record this on the same reporting log and to be actioned by 123ICT.

E-safety Complaints/Incidents

- instances of pupil internet misuse should be reported to a member of staff
- the Executive Headteacher will be trained to deal with e-safety incidents. They must log incidents reported to them (Appendix D) and if necessary refer the matter to the police (Appendix E & F)
- instances of staff internet misuse should be reported to and will be dealt with by the Executive Headteacher (Appendix E & F)
- pupils and parents will be informed of the consequences of internet misuse

- the Governing Body will be regularly informed of e-safety issues and policies
- the school will work in partnership with pupils and parents to educate them about cyberbullying and what to do if they or anyone they know are a victim of cyberbullying (Appendix G)
- all cyberbullying incidents should be recorded (Appendix D) and investigated (Appendix E)

Working with External Agencies and Other Professionals

We work with and draw on the expertise of a number of external agencies and professionals to support with e-safety. This includes:

- NSPCC to inform on staying safe and protecting personal safety
- Police and Police Community Support Officer(PCSO)
- External agencies to support the delivery of regular e-safety awareness for pupils and parents
- Safeguarding team for advice / no names consultation

Review of Policy

The policy will be monitored and evaluated by:

- Executive Headteacher
- Computing Lead
- Safeguarding Governor
- School Council
- School Committee (Governors)

The policy will be:

- reviewed every 2 years and consideration will be given to the implications for future whole school development planning
- amended if new technologies are adopted or any guidance or orders are updated.

Appendices

The following appendices sit alongside the school E-Safety Policy and some are referred to in this policy:

Appendix A

Pupil Acceptable User Agreement for EYFS and KS1

Appendix B

Pupil Acceptable User Agreement for KS2

Appendix C

Meeting digital and technology standards in schools and colleges (completed at least annually supported by Executive Headteacher, nominated governor and school IT support)

Appendix D

E-Safety Incident Reporting Log
(Access on School Shared Drive)

Appendix E

Responding to Incidents of Misuse Record form
(Access on School Shared Drive)

Appendix F

Responding to incidents of misuse flow chart

Appendix G

Advice for Children on Cyberbullying

Appendix H

Parents Seesaw GDPR Consent Letter

Appendix I

Seesaw Privacy, Safety and Security