OUR LADY'S AND ST. EDWARDS PRIMARY SCHOOL

e–SAFETY POLICY

The school's e-safety policy has been written by the Head Teacher and e-Safety Coordinator, building on the Wirral Local Authority e-safety advice. It has been agreed by the staff and approved by Governors.

The school's e-safety policy reflects the need to raise awareness of the safety issues associated with electronic communications as a whole and will operate in conjunction with other policies including those for bullying, curriculum, data protection, child protection/safeguarding and ICT policies.

SCHEDULE FOR DEVELOPMENT/ MONITORING/ REVIEW

This e-safety policy was approved by the Governors on:	4 October 2022
The implementation of this e-safety policy will be monitored by the:	Senior Leadership Team, Safeguarding Officer, Computing Coordinator
Monitoring will take place at regular intervals:	At least once a year
The Governors will receive a report on the implementation of the e-safety policy generated by the monitoring group at regular intervals:	At least once a year
The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	Summer term 2023
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LSCB Manager – Dave Robbins LSCB Designated Officer – Suzanne Cottrell Merseyside Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity

1) ROLES AND RESPONSIBILITIES

Governors
Are responsible for:

- Approving the e-Safety Policy and for reviewing the effectiveness of the policy.
- Receiving regular information about e-safety incidents and monitoring reports.

Head teacher and Senior Leadership Team
Are responsible for:

- Ensuring the safety (including e-safety) of members of the school community.
- Following correct procedures in the event of a serious e-safety allegation being made against a member of staff.
- Ensuring relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- Guaranteeing a system is in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.
- Receiving regular monitoring reports from the e-Safety Coordinator.

Safeguarding and e-Safety Coordinator
Is responsible for:

- The day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Providing training and advice for staff.
- Liaises with the Local Authority.
- Receiving reports of e-safety incidents and creating a log of incidents to inform future e-safety developments.
- Reporting regularly to Senior Leadership Team
- Being 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
  potential or actual incidents of grooming
  cyber-bullying

ICT Coordinator
Is responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.

- 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.
- They keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- Monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-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 Head teacher or e-Safety Coordinator for investigation / action / sanction.
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems.
- e-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-safety 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, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

2) TEACHING AND LEARNING

Why Internet Use is important

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for children who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How Internet Use benefits education

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient.
- Access to world-wide educational resources including museums and art galleries.

- Educational and cultural exchanges between students world-wide.
- Access to experts in many fields for students and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administration data with the Local Authority.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age and maturity of the pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the children's age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Access to the internet may be by teacher or teaching assistant demonstration.
- Pupils accessing the internet will be supervised by an adult at all times.
- When copying materials from the Internet, pupils will be taught to observe copyright.
- Pupils will be made aware that the writer of an e-mail or the author of a webpage may not be the person claimed.

3) MANAGING INTERNET ACCESS

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- All staff have an individual responsibility to protect the security and confidentiality of the school network.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.
- The Internet Service Provider (currently BT Broadband) configuration and router access control lists will be reviewed regularly.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the e-Safety Coordinator and recorded in the e-safety log.
- School will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will keep parents in touch with future ICT developments by letter and newsletter.
- Requests to unblock/block a website for use by Staff and/or Pupils for educational purposes must be logged and reviewed by the e-Safety Coordinator and approved by the Head teacher.

E-mail

- Pupils will learn how to use an e-mail application and be taught e-mail conventions.
- Pupils will only be allowed to use e-mail once they have been taught and agreed to comply with the Acceptable Use Policy agreement (AUP).
- Pupils may send e-mail as part of planned lessons but will not be given individual e-mail accounts at present.
- Pupils will have the e-mail messages they compose checked by a member of staff before sending them.
- The forwarding of chain-letters will not be permitted.
- Pupils will not be permitted to use e-mail at school to arrange to meet someone outside school hours.

Password Protection.

- Staff are encouraged to change their passwords on a regular basis.
- No use of generic passwords.
- Staff laptops should be encrypted with passwords.

Social Networking

- The school will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

- The school will work in partnership with the Local Authority and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to e-Safety Coordinator who will report it to the Local Authority and the Internet Service Provider.
- The e-Safety Coordinator / ICT Co-ordinator will ensure that regular checks are made to ensure that filtering methods selected are appropriate, effective and reasonable.

USB memory sticks & other Portable Data Storage Devices

- Staff to consider what data should be stored on USB sticks/other data storage devices.
- Sensitive data should be encrypted.

Digital Cameras

- Staff use school cameras to photograph pupils.
- Staff may only use authorised personal equipment to photograph pupils.
- Storage cards to be cleared when photographs have been downloaded.

Storage of Photographs

- Photographs to be stored in secure areas within school networks or password protected laptops.
- Photographs to remain on school premises (when practicable –i.e. off site school trips –images only to be downloaded to school network).
- Photographs to be deleted when no longer required.
- Current Local Authority policy is adhered to regarding photographing & publishing images of children.

Mobile Phones & Other Hand Held Communication Devices

- Mobile phones & other hand held communication devices should not be used for personal use in the lesson or formal school time (pupils & staff).
- See separate Mobile Device Use Policy.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the e-Safety Coordinator and ICT Co-ordinators and agreed by the Governors, before use in school is allowed.
- Mobile phones/ handheld communications devices/ gaming consoles/ will not be used for personal use during lessons or formal school time.

Published Content and the School Website

- The contact details on the website will be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Head teacher will work alongside the ICT Co-ordinator and take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will be appropriate for the context.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained annually before photographs of pupils are published on the school website.
- Work can only be published with the permission of the pupil and parents.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4) POLICY DECISIONS

Authorised Internet Access

- The school will maintain a current record of all staff and students who are granted Internet access.
- All staff must read and sign the AUP agreement before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.

- Parents will be asked to read and sign a consent form for pupil access to any ICT resource.
- Pupils must apply for Internet access individually by agreeing to comply with the AUP agreement.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wirral Metropolitan Borough Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate every 12 months.

Handling E-safety Complaints

- Complaints of Internet misuse will be dealt with by the e-Safety Coordinator or Head teacher.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection issue must be dealt with in accordance with child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with Community Police Officers/Crime Prevention Officer.

Community Use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety

4) COMMUNICATION OF POLICY

Pupils

- Pupils will be informed that Internet use will be monitored
- Instruction in responsible and safe use should precede Internet access.
- All pupils read and accept the school's AUP agreement.

Staff

- All staff will be given the school e-safety policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues
- All staff must accept the terms of the AUP agreement before using any Internet resource.
- Staff development in safe and responsible Internet use and on the school's e-safety policy will be provided as required.
- Training in e-safety will be reviewed annually

Parents

- Parents’ attention will be drawn to the school’s e-safety policy in newsletters and on the school website.
- Sessions/ workshops in e-safety will be offered to parents.

Visitors

- Visitors to school will be informed about the e-safety rules at the reception desk (i.e. use of mobile phone/smart watch/camera/film equipment etc).