

**E-Safety Policy**

Reviewed – September 2022

**E Safety and Internet Usage**

E safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguarding and awareness for users to enable them to control their online experiences.

The school’s E safety Policy will operate in conjunction with other policies including those for Etiquette Guidance, Behaviour, Anti-Bullying, Safeguarding, Child Protection, Mobile Phone, Data Protection, Image Consent form and Security.

**Background - Why Is Internet Use Important?**

The purpose of internet use in schools is to raise educational standards, to promote pupil 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 pupils who show a responsible and mature approach to its use and St Joseph’s has a duty to provide pupils with quality internet access.

Many pupils will access the internet outside school and will need to learn how to evaluate online information and to take care of their own safety and security.

**How Does Internet Use Benefit Education?**

Benefits of using the internet in education include:

• access to worldwide educational resources including museums, libraries and art galleries

• rapid and cost effective worldwide communication

• inclusion in the National Education Network which connects all UK schools

• educational and cultural exchanges between pupils worldwide

• access to experts in many fields for pupils 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

• access to learning wherever and whenever convenient

• greatly increased skills in Literacy

• in times of lockdowns and COVID 19, internet access allows students to continue learning remotely

**How Can Internet Use Enhance Learning?**

• The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of our pupils

• Children 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 will guide pupils in online activities that will support learning outcomes planned for the pupils’ 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

**Good Habits E safety depends on effective practice at a number of levels:**

• Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies

• Sound implementation of E-safety policy in both administration and curriculum, including secure school network design and use

• Safe and secure broadband from the provider including the effective management of content filtering

• National Education Network standards and specifications

**Dangers To Consider - Some of the dangers children may face include:**

• Access to illegal, harmful or inappropriate images or other content

• Unauthorised access to/loss of/sharing of personal information

 • The risk of being subject to grooming by those with whom they make contact on the internet

• The sharing/distribution of personal images without an individual’s consent or knowledge

 • Inappropriate communication/contact with others, including strangers

• Cyberbullying

 • Access to unsuitable video/internet games

• An inability to evaluate the quality, accuracy and relevance of information on the internet

 • Plagiarism and copyright infringement

• Illegal downloading of music or video files

• The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

We must demonstrate that we provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks.

The E safety Policy that follows explains how we intend to do this.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning.  It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.  Currently the internet technologies children and young people are using both inside and outside of the classroom include:

* Websites
* Blogs and Wikis
* Podcasting
* Multimedia
* Gaming
* Mobile devices

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed.  All users need to be aware of the range of risks associated with the use of these Internet technologies.

At St Joseph’s School and Nurserywe understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, Trustees, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the school.

**Roles and Responsibilities**

As e-safety is an important aspect of strategic leadership within the school, **the DSL, supported by the Head and Trustees has ultimate responsibility to ensure that the policy and practices are embedded and monitored.**  The named e-safety co-ordinators at St Joseph’s School and Nursery is Mr Ashley Crawshaw, the Head Teacher and the DSL is Mrs E Boyer. This policy, supported by the school’s acceptable use agreement, is to protect the interests and safety of the whole school community.  It is linked to the following school policies: computing, child protection, behaviour, health and safety, anti-bullying and PHSE.

**Managing the school e-safety messages**

We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.  These messages will be appropriate to the age of the children being taught. E-safety guidelines and the SMART rules will be prominently displayed around the school.

**E-safety in the Curriculum**

The school provides opportunities within a range of curriculum areas to teach about e-safety.

Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-safety curriculum.

The teaching of e-safety focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately.

Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.

Pupils know how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as ChildLine/ CEOP report abuse button.

**Security, Data and Confidentiality**

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school’s E-safety Policy.

Staff may, in some circumstances, use cloud based storage, which is password protected to store and access information conveniently.

Staff should be aware of their responsibilities when accessing sensitive school data:

* School data will only be accessed by staff, using their own username and password.
* School data will not be duplicated onto personally owned equipment.
* Portable devices are encrypted and data can only be accessed using a secure log in.

**Managing the Internet**

Internet Access and Responsibility

• All staff must read and sign the Staff Acceptable ICT Use Agreement before using any school ICT resource

• Parents are informed that pupils will be provided with supervised internet access.

• If staff or pupils discover unsuitable sites, the URL, time and content must be reported to the E safety coordinator and network manager who will investigate and take appropriate action, liaising with broadband provider if necessary

 • School will ensure that the use of internet derived materials by pupils and staff 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. Email & Online Collaboration

• Pupils may only use approved email accounts on the school system

• Pupils must immediately tell a teacher if they receive offensive messages

• Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission

• Pupils may must not access others pupil’s accounts or files

• Whole class or group email addresses should be used in school

• Pupils must be responsible for their own behaviour on the internet, just as they are anywhere else in the school. This includes the materials they choose to access, and the language they use.

• Pupils must not deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the school can block further access to the site.

• Pupils are expected not to use any rude or offensive language in their email communications, and contact only people they know or those the teacher has approved. They will be taught the rules of etiquette for email and will be expected to follow them.

* Pupils must ask permission before accessing the internet and have a clear idea of why they are using it.

• Computers and school laptops should only be used for school work and homework unless permission has been given otherwise.

• No program files may be downloaded from the internet to the computer, to prevent corruption of data and to avoid viruses

• Pupils must not bring in USBs from home for use in school without permission. This is for both legal and security reasons. USBs should be virus scanned before use.

• Access in school to external personal email accounts may be blocked

• The forwarding of chain letters is not permitted

• Pupils must sign an agreement form if using school device at home which includes a code of conduct

All internet use is logged and the logs are randomly but regularly monitored.  Whenever any inappropriate use is detected it will be followed up.

The school maintains students will have supervised access to Internet resources (where reasonable) through the school’s fixed and mobile internet technology.

‘Safe search for kids’ is used to manage any internet research.

If Internet research is set for homework, staff will remind students of their e-safety training. Parents are encouraged to support and supervise any further research.

**Infrastructure**

Our broadband provision is provided and managed by Your IT.

St. Joseph’s School and Nursery P is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

If staff or pupils discover an unsuitable site, the incident should be reported immediately to the teacher and then passed on to the e-safety co-ordinator.

If there are any issues related to viruses or anti-virus software, the e-safety co-ordinator should be informed.

**Mobile Technologies**

**Personal Mobile devices (including phones)**

There is a separate policy for the possession and use of mobile phones

**Managing email**

The use of email within school is an essential means of communication for staff.

Pupils currently do not have access to individual email accounts. Staff must use the schools approved email system for any school business.

Staff must inform (the e-safety co-ordinator / Head Teacher) if they receive an offensive or inappropriate e-mail.

Pupils may be introduced to email as part of the Computing Scheme of Work.

**Social Networking**

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

• At St Joseph’s we block/filter access to social networking sites and newsgroups unless a specific use is approved

• Pupils are advised never to give out personal details of any kind which may identify them or their location

• Pupils are advised not to place personal photos on any social network space

• Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.

• Pupils are encouraged to invite known friends only and deny access to others

• Pupils and parents are made aware that some social networks are not appropriate for children of primary school age and the legal age to hold accounts on many such as YouTube or Instagram is 13 years old

The School also strongly discourages children from using age inappropriate social networking outside of school.

Should the staff be made aware of incidents or activities on these social networks that have a direct effect on the children’s behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts.

This may include discussions with parents, information letters or reporting the child’s access to the respective organisations/companies.

**Safe Use of Images**

**Taking of Images and Film**

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes field trips.  School’s own mobile devices must be used in this case.

Parents are allowed to film and take photographs and films of performances and assemblies, etc. provided they are only for their own private records and are not uploaded to social media or external websites.

**Publishing pupil’s images and work**

All parents/carers will be asked to give permission to use their child’s work/photos in publicity materials or on the school website, twitter account or mobile app.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child’s circumstances where consent could be an issue.

Parents/ carers may withdraw permission, in writing, at any time.

Pupils’ names will not be published alongside their image and vice versa on the school website, twitter account, mobile app or any other school based publicity materials.

**Storage of Images**

Images/ films of children are stored securely on the school server and / or teacher’s individual school laptops.

**Published Content & The School Website**

• The contact details on the web site should be the school address, email and telephone number. Staff or pupils personal information will not be published.

 • The Head Teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate Information System Security

• School ICT systems capacity and security will be reviewed regularly

• Virus protection will be installed and updated regularly

• Security strategies will be discussed with our technical support team and broadband provider if necessary Protecting Personal Data Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Please see our Data Protection policy.

**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. The school cannot 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

**Managing Emerging Technologies**

• Emerging technologies will be examined for educational benefit and their risks assessed

• Mobile phones will not be used for personal use during lessons or formal school time on the school site. See our Mobile Phone policy

• The sending of abusive or inappropriate text messages or photos (sexting) is forbidden

• See our Child Protection and Safeguarding Policy for more information

**Misuse and Infringements**

Staff or pupils who misuse the internet or detract from the core principles in this policy, including actions that seriously compromise the safety of the children, will be subject to disciplinary procedures including exclusion or the termination of employment.

**Complaints**

• Complaints of internet misuse will be dealt with by a senior member of staff

• Any complaint about staff misuse must be referred to the Head Teacher

• These will be logged and dealt with as deemed appropriate by the Head Teacher

• Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures

• Pupils and parents will be informed of the complaints procedure (See Making A Complaint – a guide for parents)

**Inappropriate material**

All users are aware of the procedures for reporting accidental access to inappropriate materials.  The breach must be immediately reported to the e-safety co-ordinator / Head Teacher.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-safety co-ordinator, depending on the seriousness of the offence; investigation by the Head Teacher/ Police.  Staff are aware that misuse or misconduct could lead to disciplinary action.

**Equal Opportunities**

**Pupils with additional needs**

The school endeavours to deliver a consistent message to parents and pupils with regard to the schools’ e-safety rules.

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety.

Internet activities are planned and well-managed for these children and young people.

**Communication Of E safety And Internet Usage Policy**

 **Pupils**

• Pupils will sign an Acceptable Use Agreement

• Rules for internet access will be posted in all classrooms

• Pupils will be informed that internet use will be monitored

* Pupils will be reminded of E safety rules regularly – especially when using the internet

**Staff**

• All staff will be given the E safety Policy and its importance explained

• Staff will sign an Acceptable Use Agreement

• Staff should be aware that internet traffic can be monitored and traced to the individual user.

• Discretion and professional conduct is essential.

**Parents**

• Parents’ attention will be drawn to the E-safety Policy in newsletters, communication home and the school website

 • Parents will be aware of their child’s Acceptable Use Agreement

**The school will monitor the impact of the policy using:**

• Logs of reported incidents

 • Broadband monitoring logs of internet activity (including sites visited)

• Internal monitoring data for network activity

• E safety co-ordinator in school and the E-safety Trustee will meet regularly to review monitoring