St Joseph's Catholic Primary School

Internet and E-Safety Policy

Revision	Date	Author	Summary of Amendments	Reviewed	Date	Approved (Date of FGB meeting)	Next Review	Responsible Committee
1	01/04/2022	E. Broyd	New draft	C&SI	24/09/22	26/01/2023	September 2024	C & SI

Internet and E-Safety Policy

Vision

St Joseph's Catholic Primary School
Together we love ~ Together we hope ~ Together we learn

Together we love - Together we hope - Together we learn

Mission

St Joseph's Catholic Primary School is an inclusive, vibrant, Catholic community where we enable and encourage everyone to share and nurture a love of learning and the love of Christ.

Together, we hope to inspire ourselves and each other to be the best we can and to embrace our future with confidence.

Rationale

New technologies have become integral to the lives of children in today's society, both within schools and in their lives at home. The internet and other digital information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access. The requirement to ensure that children are able to use the internet and communication technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

Scope

This policy applies to all who have access to and are users of school ICT systems, both in and out of school. Where appropriate, it may also cover internet or e-safety incidents that take place out of school, but which are linked to a member of the school community (including staff, pupils, volunteers, parents and carers, visitors.

Role and responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

Governors

The Governors are responsible for the approval of e-safety policy and for reviewing the effectiveness of the policy. A member of the Governing Body will take on the role of E-Safety Governor and will be supported by the Safeguarding Governor. The role of E-Safety Governor will include meeting with the member of staff who is the designated E-Safety Coordinator and reporting to the relevant Governing Body Committee.

Headteacher and Senior Leadership Team (SLT)

The Headteacher and SLT are responsible for ensuring the safety (including e-safety) of members of the school community. They will ensure that the E-Safety Coordinator and other members of staff receive relevant CPD in order for them to carry out their roles. The Headteacher and SLT will ensure that there is a system in place to allow for the monitoring of e-safety (such as a filtering system), as well as supporting those who carry out this monitoring process.

E-Safety Coordinator

This should be a member of staff. Their role will include the day to day responsibility for e-safety issues and taking a role in reviewing the School's e-safety policy. They should ensure that all staff are aware of the procedure to follow should an e-safety incident take place. They should work with the Local Authority and other agencies, providing relevant training or opportunities for training to staff. The E-Safety Coordinator should meet with the E-Safety Governor and the SLT to discuss any incidents that have occurred.

Teaching and support staff

The teachers and support staff at the School are responsible for:

- making sure they have an up to date awareness of e-safety matters and of the current school e-safety policy and procedures.
- reading and understanding the Staff Acceptable Use Policy (AUP).
- reporting any incidents or suspected misuse via the school's Child Protection Online Management System (CPOMS).
- making sure pupils know and understand the pupil's Rules for Responsible Internet Use.
- monitor ICT activity in lessons, clubs and extra-curricular activities.

Pupils

Pupils at the School are responsible for:

- using school ICT systems in accordance with the Pupil's Rules for Responsible Internet Use, which they will be expected to read and understand at the start of each year.
- knowing and understanding the School's expectations on the use of mobile phones, as well as the School's policies on the taking and use of images and on cyber-bullying.
- understanding the importance of adopting good e-safety practices when using digital technologies both in and out of school, knowing that the School's E-Safety Policy also covers their actions out of school.

Parents and carers

Parents and carers play a crucial role in ensuring the children in their care understand the need to use the internet and mobile devices in an appropriate way. The School will take every opportunity to help parents and carers understand these issues through parents' evenings, newsletters and the school website. Parents and carers will be responsible for:

- helping the children in their care to know and understand the Pupil's Rules for Responsible Internet Use.
- knowing and understanding the Parents' Acceptable Use Policy.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread.

Training

It is essential that all staff and Governors receive e-safety training and understand their responsibilities as outlined in this policy. Formal e-safety training will be made available to staff and an audit of training needs should be carried out annually. All new staff should receive relevant training as part of their induction process. This E-Safety Policy and any updates should be discussed during a staff meeting or INSET days and the E-Safety Coordinator will provide training to individuals as required.

Governors should take part in e-safety training and awareness sessions, with particular importance for those who are members of any sub-committee involved in ICT, e-safety, health and safety or safeguarding. This may be through attending training provided by the

Local Authority or other relevant organisation, or participating in school training and information sessions for staff or parents and carers.

Curriculum

E-Safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across these areas. In lessons where internet use is planned, it is best practice that pupils should be guided to sites checked and deemed suitable for their use. Where pupils are allowed to freely search the internet (e.g. using search engines), staff should be vigilant in monitoring the content of the websites pupils visit. Pupils should be taught to be critically aware of the materials and content that they access online and should be guided to validate the accuracy of that.

Managing filtering

The School will work with its service provider (Bristol ICT) to ensure that systems to protect pupils and staff are regularly reviewed. If someone using the School's internet discovers an unsuitable site, it must be reported to the E-Safety Coordinator or a member of the SLT.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes unless agreed with the head teacher.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website, social media or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. This will normally be carried out at the beginning of each academic year.

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 must report to the Heateacher or E-Safety Coordinator the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or personal social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Approved by the C&SI committee:

Date: 24th September 2022

Approved by Governing Body: 26th January 2023

Review Date: September 2024

Policy Monitoring And Review (To Include Sub-Committee)

This policy will be reviewed bi-annually by the Curriculum & School Improvement Committee

Authorisation

Signed by (Chair of Governing Board)

Approved by Governing Body:

Review Date: September 2024