Growing in Faith and Knowledge

E-Safety Policy -

The Acceptable Use of the Internet and related Technologies

Updated; September 2022

(Staff are notified of regular ISI updates)

Review Date: September 2023

Introduction

This policy has been developed as a result of a process of consultation. It has been agreed and approved by the Governors. It builds on guidance from NAACE and Child Exploitation and Online Protection (CEOP) and with regard to Preventing and tackling bullying, 2017.
It is a statement of the aims, principles and strategies for the safe use of Internet and related technologies at St Joseph's Prep school.

This Policy will be carried out with due regard to our School Mission Statement.

Philosophy

This Policy document is drawn up to protect all parties – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Aims

The philosophy of 'empowering children to stay safe' includes aims that children are:-

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from radicalisation
- safe from accidental injury and death
- safe from bullying and discrimination, including cyberbullying
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- An e-Safety education programme for pupils, staff and parents**.**

(Reference: Becta - E-safety Developing whole-school policies to support effective practice [1])

[1] http://schools.becta.org.uk/index.php?section=is

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and compliance with the Policy monitored.

The Headteacher has overall responsibility for e-Safety.

Our school **e-Safety Co-ordinator** is, Mr D Hood, ICT & Computing Coordinator

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through organisations such as NAACE and CEOP[2]. The school's e-Safety coordinator also ensures the Headteacher and Governors are updated as necessary.

Governors need to have an overview and understanding of e-Safety issues and strategies at St Joseph's. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging
- Blogs, Vlogs
- Podcasting
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile / Smart phones with camera, video, e-mail, and web functionality
- Fit bits & trackers

Accessing the Internet

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

All staff must read and sign the Staff Code of Conduct for Acceptable Internet Use before using the school ICT resources.

[2] http://www.ceop.gov.uk/

All staff and Governors also need to read and sign the Policy for Use of Social Networking and Internet Sites.

For younger children, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on –line materials.

Parents will be asked to sign a consent form for pupil access.

Parents will be informed that pupils will be provided with supervised Internet access.

The Internet and Learning

Effective practice in Internet use for teaching and learning is essential as the quantity of information can be over whelming.

Younger children should be offered selected sites rather than the open Internet to search. Older children benefit from the same use of suggested sites and must also be encouraged to evaluate everything they read and to refine their own publishing. Plagiarism will be discouraged at all times and children will be taught to acknowledge sources in their work.

The school internet access will be designed expressly for pupil use and includes filtering appropriate to primary school children.

Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use.

At present, these rules are based on Childnet's SMART rules for children:-
S – stay **safe**; do not give out personal information
M – Tell an adult if you are thinking of **meeting** someone.
A –**Accepting** e-mails or open attachments from people you do not know can lead to viruses and unwanted emails.
R – Information you find on the Internet may not be **reliable** and people may not be who they say they are.
T- **Tell** a parent, carer or trusted adult if someone or something makes you feel uncomfortable or worried, and if you or someone you know is being bullied online.

Other teaching tools include the use of e-safety websites including
Think U Know (www.thinkuknow.co.uk)
Grid Club (www.gridclub.com)
Kidsmart (www.kidsmart.org.uk)
Bizzikid (www.bizzikid.co.uk)

Pupils
The safe use of Technology is integral to the School's ICT curriculum. Pupils are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices Technology is included in the educational programmes followed in the EYFS in the following ways:
(a) children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;
(b) children are enabled to explore and play with a wide range of media and

materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and
(c) children are guided to recognise that a range of technology is used in places such as homes and Schools and encouraged to select and use technology for particular purposes.

The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies, PSHCE and teaching pupils:
(a) about the risks associated with using the Technology and how to protect themselves and their peers from potential risks;
(b) to be critically aware of content they access online and guided to validate accuracy of information;
(c) how to recognise suspicious, bullying, radicalisation and extremist behaviour;
(d) the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
(e) the consequences of negative online behaviour; and
(f) how to report cyberbullying and/or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly**.**

E-mail

E-mail is an essential means of communication for both staff and pupils. Directed e-mail has significant educational benefits when used in projects between schools and children in other countries. E-mail is safeguarded by the use of a filtering tool (Pure Message)
In addition –

- Pupils may only use approved school e-mail accounts.
- Pupils may not send or check e-mails in School without the teacher's permission.
- Whole-emails can be forwarded via the teacher's e-mail address.
- Pupils must immediately tell the teacher if they receive offensive e-mail.
- Pupils must not reveal personal details, send photographs of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to external organisations should be written carefully and using the school letterhead.
- The forwarding of chain letters is not permitted.

Website

Contact details on the website will include school address, e-mail and telephone number. Staff or pupils personal details must not be published.

No link should be made between an individual and any home address (including simply street names);

The Headteacher will take overall editorial responsibility to ensure that content is accurate and appropriate.

The school must respect intellectual property rights and copyright.

The publishing of pupils' full names with their images is not acceptable. Images should be carefully chosen to ensure that children who should not be included because of parental choice, do not appear on the website.

Written permission will be sought from parents each academic year with respect to publication of any images or work on the web site or newsletter.

Social Networking

Examples of social networking sites include- Facebook, wikis, blogs, MySpace, MSN space, Instagram, Snapchat, bulletin boards, chat rooms, instant messaging and many others. As children can access these at home, advice to children will be supplemented by similar advice to their parents.

Children should adhere to age restrictions on social media sites
School will block access to these sites and others.
Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them and / or their location
Pupils will be advised not to place personal photos on any social network space.

Staff are also encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

Although these networks are used by staff in their own time, staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks.

It is recognised that some such services may have an appropriate application in school, however, where such activities are planned a separate account should be set up for the purpose and there should be no connection made between personal and school accounts used for educational purposes. Any such accounts and activities should be approved by a member of the SMT prior to use.

It is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors.
Further advice is found in the Policy on 'Staff/Governor Use of Social Networking and Internet Sites'.

Managing Filtering

At present, St Joseph's Preparatory School uses Draytek 'Global View', a dynamic service which filters Internet sites and we also endeavour to block unsuitable sites as reported.

To this end we will:-

Work with our Internet Service Provider (netcentral) to ensure that systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites, the URL must be reported immediately to the e-Safety Coordinator.

Any material that the school believes is illegal must be reported to appropriate agencies such as IWF, CEOP or the police.

Mobile Phones and Hand-Held Devices.

The use of Mobile phones is set out in the Mobile Phone Policy. Pupils are not permitted to bring mobile devices into School.

Use of Portable Equipment

The school provides portable ICT equipment such as laptop computers, colour printers, I-pads and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

Exactly the same principles of acceptable use apply as in other sections of this policy

- Equipment may be in the care of a specific individual, but it is expected that all staff may wish to benefit from the use of a laptop computer and access should be negotiated with the individual concerned. Any difficulties should be referred to the ICT co-ordinator;

- Certain equipment will remain in the care of the ICT co-ordinator, and may be booked out for use according to staff requirements. Once equipment has been used, it should be returned to the appropriate classroom (Mr Hood);

- Equipment such as laptop computers can be taken offsite for use by staff if permission is given by the Head teacher and in accordance with the E-Safety Policy and the equipment is fully insured from the moment it leaves the school premises. The cover excludes theft or attempted theft from an unattended vehicle unless the vehicle is locked, there are signs of forced entry and the property is out of sight in a locked compartment or boot within the vehicle.

- Any costs generated by the user at home, such as phone bills, printer cartridge etc. are the responsibility of the user;

- Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc.) or maternity leave, arrangements must be made for any portable equipment in their care to be returned to school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it.

- If an individual leaves the employment of the school, any equipment must be returned;

- The use of USB flashdrives, re-writeable CDs, etc. must be regulated. Where information has been downloaded from the internet, or copied from another computer, wherever possible, it must be emailed to school to ensure that it undergoes anti-virus scanning. If this proves to be impossible, (due to file size, technical difficulty etc.) express permission must be sought from the ICT co-ordinator prior to the data being transferred;

- No other software, whether licensed or not, may be installed on laptops in the care of teachers as the school does not own or control the licences for such software;

Roles and Responsibilities

Responding to an incident of concern

Our e-Safety Coordinator acts as first point of contact for any complaint.

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

In the event of children being unintentionally exposed to undesirable materials the following steps will be taken:

1. Pupils should notify a teacher immediately
2. The e-Safety Coordinator should be notified and the incident reported to the Headteacher.
3. The incident should be recorded in a central log by which the school may reliably report the frequency and nature of incidents to any appropriate party
4. The child's parents and/or the School Governors should be notified at the discretion of the Headteacher according to the degree of seriousness of the incident.

Children must never intentionally seek offensive material on the Internet. Any transgression should be reported and recorded as outlined above. Any incident will be treated as a disciplinary matter and the parents of the children will normally be informed. If deliberate access to undesirable materials is found to be repeated, flagrant or habitual the matter will be treated as a serious disciplinary issue. The child or children's parents will be informed and the Governing body advised.

Staff and pupils are given information about infringements in use and possible sanctions.

Sanctions available include:

- Interview/counselling with Headteacher / e-Safety Coordinator
- Informing parents or carers;
- Removal of Internet or computer access for a period, which could ultimately prevent access to files, held on the system.
- Referral to the police.

Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school Safeguarding procedures.

Staff

All staff will be given the School e-Safety Policy and its application and importance explained.

Staff are required to read and sign a 'Code of Conduct' regarding Acceptable Use of the school's information system. (See Appendix 1)

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

The ICT Coordinator, who at present manages the filtering systems, will be supervised by the Headteacher and have clear procedures for reporting issues.

Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided and updated at least annually.

Any complaint about staff misuse must be referred to the Headteacher.

Parents

Parents' attention will be drawn to the school's e-Safety Policy in newsletters, and on the school website.

When joining the school, parents are required to read and agree to the school's Statement of Acceptable Use for ICT.

A partnership approach with parents will be encouraged.

The School works closely with parents and guardians in promoting a culture of Digital-Safety. The School will always contact parents if there are any concerns about a pupil's behaviour in this area, and parents are encouraged to share any concerns with the School. It is recognised that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents. (see list of e-safety sites above) Discussion evenings for parents are arranged to offer advise about the potential hazards of technology, and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity. Parents have the legal responsibility to ensure that they and their child/children understand how to use technology safely.

Specific Learning Needs

Provision for children with specific learning needs in relation to e-Safety is made after discussion between class /subject teacher, support staff and the SEND Co-ordinator.

Some groups of children are potentially more vulnerable and more at risk than others when using ICT. These can include children with emotional or behavioural difficulties, learning difficulties, and other complex needs, as well as those whose English is an additional language, and looked after children.

Children with Specific Learning Needs can use the internet in educational, creative, empowering and fun ways, just like their peers. However, they may be particularly vulnerable to e-safety risks. For example:

- Children and young people with Autistic Spectrum Disorder may make literal interpretations of content, which will affect how they respond.

- Some children may not understand much of the terminology due to language delays or disorders.
- Some children with complex needs do not understand the concept of friendship, and therefore trust everyone implicitly. They do not know how to make judgments about what is safe information to share. This leads to confusion about why you should not trust others on the internet.
- There is also growing concern around cyber bullying. We need to remember that some children with Specific Learning Needs or disabilities may be vulnerable to being bullied through the internet, or not recognise that they are being bullied.
- Some children may not appreciate how their own online behaviour may be seen by someone else as bullying.
- Where appropriate, special adaptations, such as video presentations with signing and the use of Widget cards for poorer readers, of Child net International's SMART resources can be accessed.
- Teachers should tackle these sensitive issues sympathetically.
- The SEND co-ordinator should ensure that strategies for safe internet use are part of individual children's learning plan.

Equal Opportunities

- All teaching and non-teaching staff at St Joseph's Preparatory School are responsible for ensuring that all children, irrespective of grounds of race, religion, culture, sex, gender, homophobia, special educational needs and disability, or because a child is adopted or is a carer, have access to the whole curriculum and make the greatest possible progress. Equal access needs to be planned and monitored very carefully and this must be reflected in teacher's pairs and groupings. General monitoring is the responsibility of the Headteacher and the Assistant Head teacher.
- Where use of a school computer proves difficult for a child because of a disability, the school will provide specialist equipment and software, so that the pupil may have access. (i.e. lower case lettering on keyboards, concept keyboards, roller ball mouse, filter screens.) Pupils with learning difficulties can also be given greater access to the issues of e-Safety through the use of ICT.

Procedures for dealing with incidents of misuse
Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and behaviour policies and procedures.

Misuse by pupils
Anyone who has any concern about the misuse of Technology by pupils should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying.

Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's safeguarding

Misuse by staff
Anyone who has any concern about the misuse of Technology by staff should report it

in accordance with the School's Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures.
If anyone has a safeguarding-related concern, they should report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's Safeguarding Policy.

Misuse by any user
Anyone who has a concern about the misuse of Technology by any other user should report it immediately to the Headteacher.
The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.
If the School considers that any person is vulnerable to radicalisation the School will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police

Review

- The speed and nature of development is such that a review of the e-Safety Policy should take place on an annual basis or sooner is circumstances arise which require immediate amendments to the policy. The ICT Co-ordinator then makes any changes or adaptations of policy. Throughout the year, all staff are encouraged to feedback information about the effectiveness of this policy and ideas to the co-ordinator.

Appendix 1

St. Joseph's Preparatory School

Staff Code of Conduct for Computing

To ensure that you as members of staff are fully aware of your professional responsibilities when using information systems and when communicating with pupils, you are asked to sign this code of conduct. Members of staff should also consult the school's e-safety policy for further information and clarification.

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The Internet facility will be available during term time only. The school reserves the right to examine or delete files where it believes unauthorised use of the information system may be taking place or to monitor any Internet sites visited.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDA's, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I will not access the system without the use of an authorised account and password, which should not be made available to anyone other than an authorised system manager;
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I will not install any software or hardware without permission
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- I will respect copyright and intellectual property rights;
- I will ensure that electronic communications with pupils including email, and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- No e-mail attachments must be opened unless you are absolutely sure they are from known associates. If you are unsure, always delete it straight away without opening it as this is the major route for computer viruses;
- Posting anonymous messages and the forwarding of chain letters is forbidden, as is the use of public chat lines;
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will report any incident of concern regarding children's safety to the e-Safety Coordinator, the Designated Safeguarding Lead or Headteacher.
- I understand that access to undesirable materials by adults is unacceptable and will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual the matter will be treated as a very serious disciplinary issue and the Governors will be advised

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed : …… Capitals: …… Date: ……..

Accepted for School: …… Capitals: ……