# Online Safety Policy

# Online Safety Policy

Online Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their Online Safety experience.

The Schools' Online Safety Policy has been written to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole and relates to the internet activities detailed in Appendix 1. As a comprehensive guide, it also reflects school's policy on different areas, such as roles & responsibilities, IT security, BYOD(Bring You Own Device), social media, website requirements and monitoring.

The school's Online Safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Teaching and Learning, Data Protection and Security.

**Aims of the Policy**

- To set out the key principles expected of all members of the school community at St Teresa's Catholic Primary School with respect to the use of ICT-based technologies
- To safe guard and protect the children and staff of St Teresa's Catholic Primary School
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own practice
- To set out clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use

**End to End Online Safety**

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from EMPSN including the effective management of Capital Bytes Netsweeper Service.
- Linked closely with Anti-Bullying Policy

Our Online Safety Policy has been written by the school, building on government guidance. It has been agreed by senior management and approved by governors. The Online Safety Policy and its implementation will be reviewed annually.

- Online Safety Co-ordinator:
- Child Protection Co-ordinator:
- The Online Safety Policy was revised by:
- It was approved by the Governors on: … … ……..

## Roles and Responsibilities

We believe that Online Safety is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

### Responsibilities of the senior leadership team

- The Headteacher is ultimately responsible for Online Safety provision including Online Safety for all members of the school community and is our designated Online Safety co-ordinator.
- The Headteacher and senior leadership team are responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues when necessary.

### Responsibilities of the Online Safety Co-ordinator

- To promote an awareness and commitment to Online Safety throughout the school
- To be the first point of contact in school on all Online Safety matters
- To take day-to-day responsibility for Online Safety within school and to have a leading role in establishing and reviewing the school Online Safety policies and procedures
- To communicate regularly with school technical staff
- To communicate regularly with the designated Online Safety governor
- To create and maintain Online Safety policies and procedures
- To ensure that all members of staff receive an appropriate level of training in Online Safety issues
- To ensure that Online Safety education is embedded across the curriculum
- To ensure that Online Safety is promoted to parents and carers
- To liaise with the local authority, the Local Safety Children Board and other relevant agencies as appropriate
- To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident
- To ensure that an Online Safety incident log is kept up to date
- To ensure that the school Acceptable Use policies are current and pertinent.

### Responsibilities of teachers and support staff

- To read, understand and help promote the school's Online Safety policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any suspected misuse or problem to the Online Safety coordinator
- To develop and maintain an awareness of current Online Safety issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social media etc.
- To embed Online Safety messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To be aware of Online Safety issues related to the use of mobile phones, cameras and handheld devices

- To understand and be aware of incident-reporting mechanisms that exist within the school
- To maintain a professional level of conduct in personal use of technology at all times

**Responsibilities of ICT technician/technical staff**

- To read, understand, contribute to and help promote the school's Online Safety policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any Online Safety related issues that come to your attention to the Online Safety coordinator.
- To develop and maintain an awareness of current Online Safety issues, legislation and guidance relevant to their work
- To maintain a professional level of conduct in your personal use of technology at all times
- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure that access to the school network is only through an authorised, restricted mechanism
- To ensure that provision exists for misuse detection and malicious attack
- To take responsibility for the security of the school ICT system
- To liaise with the local authority and other appropriate people and organisations on technical issues
- To document all technical procedures and review them for accuracy at appropriate intervals
- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted

**Responsibilities of pupils**

- To read, understand and adhere to the school pupil Acceptable Use Policy
- To know and understand school policies on the use of mobile phones, digital cameras and handheld devices
- To know and understand school policies on the taking and use of mobile phones
- To know and understand school policies regarding cyber bullying
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school

**Responsibilities of parents and carers**

- To help and support the school in promoting Online Safety
- To read, understand and promote the school pupil Acceptable Use Policy with their children

- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home
- To discuss Online Safety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology
- To agree to and sign the school's permissions form which clearly sets out the use of photographic and video images outside of school
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites
- Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school
- Parents and carers are required to give written instruction if they do NOT wish for any images of their child to be used.

**Responsibilities of the governing body**

- To read, understand, contribute to and help promote the school's Online Safety policies and guidance
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils
- To develop an overview of how the school ICT infrastructure provides safe access to the internet
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school
- To support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school
- To ensure appropriate funding and resources are available for the school to implement its

**Responsibilities of the Child Protection Designated Person**

- To understand the issues surrounding the sharing of personal or sensitive information
- To understand the dangers regarding access to inappropriate Online Safety contact with adults and strangers
- To be aware of potential or actual incidents involving grooming of young children
- To be aware of and understand cyber bullying and the use of social media for this purpose

**<u>Teaching and learning</u>**

We believe that the key to developing safe and responsible behaviours Online Safety, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

**Internet use will enhance learning**

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- We will provide a series of specific e-Safeguarding-related lessons in specific year groups as part of the ICT curriculum / PSHE curriculum.
- We will celebrate and promote e-Safeguarding through whole-school activities, including promoting Safer Internet Day.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate Online Safety tools in a safe and effective way.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- All pupils will be taught in an age-appropriate way about copyright in relation to Online Safety resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyber bullying and know how to seek help if they are affected by any form of Online Safety bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse icon

**Manage IT security**

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- All users will sign an end-user Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.
- Pupils will access the internet using year group logins, which the teacher supervises. All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils

to access the internet through their id and password. They will abide by the school AUP at all times.

**E-mail**

- Pupils may only use approved e-mail accounts on the school system – Microsoft Office365.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

**School's website requirements and monitoring**

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Technical staff will be liaised with web hosting provider to ensure web content are monitored regularly.

**Social networking and personal publishing**

- The school will block/filter access to social networking sites.
- 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 or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

**Managing filtering**

- The school will work with the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

**Managing videoconferencing**

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

**Managing Email**

- Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils and staff will be reminded when using email about the need to send polite and responsible messages.
- Pupils and staff will be reminded about the dangers of revealing personal information within email conversations.

**Managing emerging technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school is allowed.
- Emerging technologies can incorporate software and/or hardware products.
- The acceptable use of any new or emerging technologies in use within school will be reflected within the school e-Safeguarding and Acceptable Use policies.
- Prior to deploying any new technologies within school, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks

**Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to the EU General Data Protection Regulation(GDPR).

**Managing Digital Content**

**Using images, video, sound and examples of work**

- Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published. This will be done via the permissions form included in the welcome pack for new starters.
    1. On the school website or blog
    2. In the school prospectus and other printed promotional material, e.g. newsletters
    3. In display material that may be used around the school
    4. In display material that may be used off site
    5. Recorded or transmitted on a video or via webcam in an educational conference
    6. On Twitter and other websites
- Parents and carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site 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 Web site.
- Pupil's work can only be published with the permission of the pupil and parents.
- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their Online Safety activities both at school and at home.
- Pupils and staff will only use school equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the headteacher provided that any media is transferred solely to a school device and deleted from any personal devices. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text Online Safety; such resources will not be published Online Safety without the permission of the staff and pupils involved.
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.

**Storage of images**

- Any images, videos or sound clips of pupils must be stored on the school network or school owned cloud storage and never transferred to personally-owned equipment.
- The school may store images of pupils that have left the school following their departure for use in school activities and promotional resources.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.
- Our ICT technician and office staff have the responsibility of deleting the images when they are no longer required.

## Policy Decisions

**Authorising Internet access**

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all breaches of the Online Safety rules and will restrict or withdraw pupil's access to the internet where necessary.
- At Key Stage 1, 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 and return a consent form.

**Assessing risks**

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school can not accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

**Recording and Reporting Online Safety Concerns and Handling Online Safety complaints**

- All incidents involving any Online Safety concerns will be reported to the Online Safety Co-Ordinator and recording.
- If necessary, they will be reported to the Child Protection Co-Ordinator and further action will be taken
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police School Liaison Officer to establish procedures for handling potentially illegal issues.

**Community use of the Internet**

- The school will liaise with local organisations to establish a common approach to Online Safety.

## Bring You Own Device(BYOD)

The school recognises BYOD (bring your own device) is the increasing trend toward employee-owned devices within an organization. Smartphones are the most common example but employees also take their own tablets, laptops and USB drives into the workplace. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, St Tereasa's Primary School aims to provide a safe and secure environment to protects all people on and off the premises during school terms.

**User responsibility**

- Mobile phones and personally owned devices will not be used in any way during lessons or formal school time.
- Mobile phones and personally owned mobile devices brought in to school by staff are the responsibility of the device owner. Owners need to do what is necessary to ensure the adequate physical security of the Device. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
- The owner is responsible for setting up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device.
- Not hold any information that is sensitive, personal or confidential from school on personally owned devices.
- All USB devices used at school must be encrypted and stored in secured place when not in use.
- If the device is lost or stolen, or if it is believed to have been compromised in some way, the incident must be reported immediately to senior management team.
- Pupils are not permitted to bring mobile phones or other personal own devices to school

**Pupils' use of personal devices**

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones or devices will be released to parents or carers in accordance with the school policy.

**Staff use of personal devices**

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Mobile Phones and personally owned devices will be switched off or switched to 'silent' mode during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then they may use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.

**Appendix 1: Internet use - Possible teaching and learning activities**

| Activities | Key Online Safety issues | Relevant websites |
|---|---|---|
| Creating web directories to provide easy access to suitable websites. | Parental consent should be sought.<br>Pupils should be supervised.<br>Pupils should be directed to specific, approved on-line materials. | Web directories e.g.<br>Ikeep bookmarks<br>Kent Grid for Learning (Tunbridge Wells Network)<br>Espresso |
| Using search engines to access information from a range of websites. | Parental consent should be sought.<br>Pupils should be supervised.<br>Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with. | Web quests e.g.<br>- Ask Jeeves for kids<br>- Yahooligans<br>- CBBC Search<br>- Kidsclick<br>- Living Library |
| Exchanging information with other pupils and asking questions of experts via e-mail. | Pupils should only use approved e-mail accounts.<br>Pupils should never give out personal information.<br>Consider using systems that provide Online Safety moderation e.g. SuperClubs. | SuperClubs PLUS<br>School Net Global<br>Open Hive<br>Skype |
| Publishing pupils' work on school and other websites. | Pupil and parental consent should be sought prior to publication.<br>Pupils' full names and other personal information should be omitted. | Making the News<br>SuperClubs<br>Headline History<br>Focus on Film |
| Publishing images including photographs of pupils. | Parental consent for publication of photographs should be sought.<br>Photographs should not enable individual pupils to be identified.<br>File names should not refer to the pupil by name. | Making the News<br>SuperClubs<br>Learninggrids<br>Museum sites, etc.<br>Digital Storytelling<br>BBC – Primary Art |
| Communicating ideas within chat rooms or Online Safety forums. | Only chat rooms dedicated to educational use and that are moderated should be used.<br>Access to other social networking sites should be blocked.<br>Pupils should never give out personal information. | SuperClubs |
| Audio and video conferencing to gather information and share pupils' work. | Pupils should be supervised.<br>Only sites that are secure and need to be accessed using an e-mail address or protected password should be used. | Skype<br>National Archives "On-Line"<br>Global Leap<br>National History Museum |