Trinity St. Peter's

Church of England Primary School

where children shine

Online Safety Policy

Vision and Values

The school's vision and mission statement underpins the high standards of behaviour expected at all times at Trinity St. Peter's.

'Guided by Our Faith in Everything That We Do'

VALUES	VISION	INTENT
Serve with a kind heart Service	Follow Jesus' example	Act with integrity and honesty Have a strong sense of fairness, justice and respect for individuals, groups and communities Take responsibility for their own actions and the consequences that accompany them
HOPE with open eyes	Have a positive outlook on life	Believe in themselves Be optimistic Be resilient
Imagine with a curious mind Creation	Think critically and creatively	Ask questions and explore concepts, ideas and possibilities Create original and ingenious ideas, Form new solutions and techniques
Nurture with helping hands Kindness	Be kind to yourself and to others	Show empathy, compassion and respect towards themselves and the needs and feelings of others Have a personal commitment to make a positive difference to their own life, the lives of others and the environment Work well independently as well as effectively and willingly in collaboration with others
Enjoy with happy feet Joy	Enjoy and appreciate every step of the journey	Enjoy coming to school Have a love for learning and a thirst for knowledge Be thankful for their opportunities and experiences

Links To Our Mission Statement and Aims

Trinity St. Peter's recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is a vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Lessons on Online Safety are embedded into our school curriculum, particularly in Computing and PSHE lessons. Pupils are taught how to stay safe and behave appropriately online. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

We aim to tackle any Online Safety issues by trying to prevent it from occurring in the first place, and by tackling it consistently, fairly and effectively whenever it does. We are committed to promoting a safe environment online where children can learn and play, as well as communicate sensibly, while also being aware of the risks and dangers.

At Trinity St. Peter's, we take pride in the teachings of our unique school values that underpin all learning. We promote the British fundamental values where British law, democracy and a mutual respect and tolerance for those of other faiths, cultures and beliefs is embedded through all areas of the curriculum. Pupils are encouraged to be independent learners, constantly making choices, within a safe and supportive environment. Developing their self- esteem and self-confidence is very important. Pupils are encouraged to understand their personal freedoms and are taught how to use these rights to best effect.

Scope

The policy applies to all members of Trinity St Peter's Primary School community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school/ academy computer and communication systems, both in and out of Trinity St Peter's Primary School.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy should be read in conjunction with the Anti-Bullying Policy, Behaviour Policy, Anti-Radicalization and Extremism Policy, Safeguarding & Child Protection Policy, GDPR Emotional Health and Wellbeing Policy, PSHE Policy and RSE Policy.

External policies that have informed the creation and updating of this policy include: Keeping Children Safe in Education; RSE and Health Education; Inspecting Safeguarding and DfE Teaching Online Safety in Schools Guidance; DfE Mobile Phones in Schools Guidance.

Areas of Risk

In line with KCSiE 2025 (para 136), online safety risks are grouped into four categories:

- Content – exposure to harmful or inappropriate material, including extremist views, pornography, self-harm content, misinformation, and conspiracy theories.
- Contact – risks from interactions with others online, including grooming, exploitation, harassment, and unwanted contact.
- Conduct – risks arising from pupils' own online behaviour, including bullying, sexting, oversharing personal information, and managing digital reputation.
- Commerce – risks of financial harm, including scams, phishing, in-app purchases, advertising, and gambling.

The main areas of risk for our school community can be summarised as follows:

Content

For example:

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites and sites with radical / extremist views.
- Content validation: how to check authenticity and accuracy of online content.

Contact
For example:

- Grooming.
- Cyber-bullying in all forms.
- Identify theft (including hacking social media profiles) and sharing passwords.

Conduct
For example:
- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and wellbeing (amount of time spent online).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images).
- Copyright (little care or consideration for intellectual property and ownership - such as music and film)

Commerce
For example:
- Gambling
- Inappropriate advertising
- Phishing
- Financial scams

(KCSIE, 2025, para 136)

Role and Responsibilities

The school implements appropriate filtering and monitoring systems in line with DfE standards. These are reviewed regularly by senior leaders and governors, ensuring effectiveness and compliance. Governors receive termly updates on filtering/monitoring arrangements.

The headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety leads in this school are Mrs Molloy and Mr King. All breaches of this policy must be reported to Mrs Molloy and Mr King.

All breaches of this policy that may have put a child at risk must also be reported to the DSL, Mrs Martin.

Headteacher / Assistant Headteacher (Curriculum): Mrs Pringle / Mr King

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding;
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff;
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships ;
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information;
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information;
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles;
- Be responsible for ensuring that all staff receive suitable training online safety, including emerging risks such as AI, misinformation, radicalisation, and online scams;
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident;
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised;
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures;
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety;
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead / Online Safety Lead: Mrs Martin / Mrs Molloy

As part of their role, the Computing Subject Leader will take day to day responsibility for Online Safety issues and having a leading role in establishing and reviewing Online Safety policies/documents. In addition, the following points are from Keeping Children Safe in Education 2025, para. 136:

- The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety);
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- Liaise with the Local Authority and work with other agencies in line with Working Together to safeguard children;

- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns;
- Work with the headteacher and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety;
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees;
- Receive regular updates in online safety issues and legislation, be aware of local and school trends;
- Ensure that online safety education is embedded across the curriculum (e.g. by use of the UKCIS framework 'Education for a Connected World') and beyond, in wider school life;
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents;
- Liaise with school technical, pastoral, and support staff as appropriate;
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs on CPOMS and filtering/change control logs and discuss how filtering and monitoring;
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident;
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are aware;
- In line with Keeping Children Safe in Education 2025, staff adopt a zero-tolerance approach to sexual harassment and violence, including online incidents.;
- Facilitate training and advice for all staff.

Technical Support: Apex

It is the role of Apex to ensure that:

- reasonable systems are put in place to ensure that the network and related infrastructure is as secure as possible;
- the school's 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 Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant;
- equipment is protected adequately against threats such as hacking and viruses;
- the network infrastructure is monitored regularly and consistently.

Teaching and Support Staff

Teachers and support staff are responsible for ensuring that:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job;

- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL);
- Read all policies, including Keeping Children Safe in Education;
- Read and follow this policy in conjunction with the school's main safeguarding policy;
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures;
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself;
- Sign and follow the staff acceptable use policy and code of conduct/handbook.
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon;
- Online Safety lessons are taught explicitly through the Computing, PSHE and RSE curriculums;
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils) ;
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites;
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law;
- Prepare and check all online source and resources before using within the classroom;
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions;
- Notify the DSL/OSL of new trends and issues before they become a problem;
- Take a zero-tolerance approach to bullying and low-level sexual harassment, including 'up-skirting' and sharing of indecent videos images;
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom;
- They are aware of those students who may be targeted or exposed to harmful influences from violent extremists via the internet. Students and staff are warned of the risks of becoming involved in such groups and that accessing such websites is against school policies;
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues;
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this Online Reputation guidance for schools.
- E-mails sent to parents/guardians or any other agencies should be on a professional level and sent through individual class email accounts between the hours of 8:15am and 4:20pm.

Governors

To enable the Governing Body to carry out its duties in promoting high standards of education and achievement, governors need to be fully informed about the standards in Online Safety as well as priorities for development. Governors are kept informed in the following ways:

- The Headteacher reports to governors termly on progress towards objectives within the School Improvement Plan;
- The governors are given the opportunity to approve the Online Safety Policy and review the effectiveness of the policy.

Parents

Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and guardians do not fully understand the issues and are less experienced in the use of Computing than their children. The school will therefore take every opportunity to help parents understand these issues through the school website, parent evenings and newsletters.

Parents/Guardians will be responsible for:

- supporting the school in promoting Online Safety and endorsing the Parents' Acceptable Use Agreement (see Appendix 2) which includes the pupils' use of the Internet and the school's use of photographic and video images;
- reading, understanding and promoting the school Pupil Acceptable Use Agreement with their children;
- consulting with the school if they have concerns about their children's use of technology.

Pupils

It is important that all pupils at Trinity St Peter's Primary school:

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- (if age appropriate) will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying;
- should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website with hard copies available from school on request;
- Policy to be part of school induction pack for new staff;
- Acceptable Use Agreements discussed with pupils at the start of each year;
- Acceptable Use Agreements to be recorded by the office and kept in teacher files.

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 should be aware that email communications are monitored;
- Users must immediately report, to the nominated person – in accordance with the school / academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication;
- Any digital communication between staff and pupils (on iOS applications such as Tapestry / Google Classroom) must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications;
- Students / pupils should be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies;
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Approaches To Teaching and Learning

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHE;
- Relationships education, relationships and sex education (RSE) and Health;
- Computing.

However, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

SEN

At Trinity St Peter's we believe that all our children should be given the opportunity to achieve as well as they can in everything they do. However, we do recognise that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

Pupils who are identified as having additional learning needs will access PSHE learning through Quality First Teaching resources and additional strategies as outlined in the child's SEN Support Plan.

Planning and Organisation

Online Safety should be focused upon in all areas of the curriculum and staff should reinforce Online Safety messages during computing lessons. The Computing Subject Leaders have a clear, progressive and up-to-date Online Safety education programme as part of the Computing curriculum/Online Safety curriculum. This covers a range of skills and behaviours appropriate to their age and experience.

In the Foundation Stage, pupils are taught to not give out any personal information on the internet. They are told to tell a teacher or parent if anything they see on the internet makes them feel uncomfortable. At Trinity St Peter's Primary School, we do expect children of this age to be supervised whilst using the internet. Nursery and Reception pupils take part in the school "Safer Internet Week" using age appropriate CEOP resources.

In Key Stage One, pupils begin to understand what personal information is and who you can share it with. Children begin to recognise the difference between real and imaginary online experiences. They are taught to keep their passwords private and make sure that an adult knows what they are doing online. Teachers model appropriate online behaviour when communicating with others.

There are four key messages taught at Key Stage One:

- People you don't know are strangers. They're not always who they say they are.
- Be nice to others on the internet, like you would on the playground.
- Keep your personal information private.
- If you ever get that 'uh-oh' feeling, you should tell a grown-up you trust.

In Key Stage Two, themes taught in Key Stage One are built upon. In addition, pupils are made aware of online experiences which could cause potential danger, e.g. use of social networking, gaming sites and downloading or installing new applications. Links are made

between inappropriate sharing of personal information and the dangers this can pose in the real world. Relevant resources from CEOP, Childnet and SWGfL are used during “Internet Safety Week” and other resources can be accessed throughout the year on the school website. In Key Stage Two, children also develop their research skills, especially through use of their iPads. They are taught about plagerism and the need to upload copyright laws.

Resources

Online Safety resources are mainly Online Safety websites. Links are available on the school website and are differentiated for parents, children and teachers. Information about new resources/websites are communicated to staff via email.
The school also has access to Knowsley City Council scheme of work; this has guidance for each class about delivering a ‘My Online Life’ unit, which focuses on specifically on Online Safety.

The school also uses the Jigsaw scheme of work for PSHE, which includes aspects of Online Safety.

Cyber-Bullying / Abuse

Safer Internet Week is held annually in February with up to date Online Safety guidance. The school website has links to cyber-bullying advice. Incidents of cyber-bullying are dealt with by leadership team and communicated to parents where necessary.

Child on-Child abuse is when children abuse other children. This type of abuse can take place inside and outside of school as well as online.

Through our RSE curriculum, children are taught how to be safe online as well as how to report any inappropriate, upsetting or concerning online interactions. This is in line with the school's Child Protection and Safeguarding Policy where any reported incidents are dealt with swiftly to protect the child/ren involved.

Gaming

Online gaming is an activity that many children and adults get involved in. The school will raise awareness by:

- Talking to parents and carers about the games their children play and help them identify whether they are appropriate.
- Supporting parents in identifying the most effective way of safeguarding their children by using parental controls and safety mode.
- Talking to parents about setting boundaries and time limits when games are played.
- Highlighting relevant resources.
- Making our children aware of the dangers, including grooming and how to keep themselves safe.

- Making our children aware of how to report concerns.

Acceptable Use Policy (AUP)

The AUP is written and distributed to all pupils during the Autumn term of the school year and signed by parents/guardians. The AUP will be reviewed annually.

Acceptable Use of Personal Equipment - Children

Use of Facebook / Social networking sites

Children are not permitted to use social networking sites on school premises. Both on computers or mobile devices. Children are also reminded of minimum age guidelines for various social networking sites, as part of their Online Safety lessons.

Use of Mobile Phones

The school recognises both the opportunities and risks posed by mobile and smart technology. To manage these risks on our premises:
• Pupils may only bring mobile phones where essential (e.g. travel to/from school) and they must be switched off and stored safely during the school day.
• Smart watches and similar devices are strongly discouraged and, where permitted, must not be used for calls, messaging, or photography in school.
• Staff mobile phones and devices must not be used in teaching areas or when supervising pupils, except in emergencies or with senior leader permission.
• Misuse of devices will be dealt with in line with behaviour and safeguarding policies.
• Parents and carers will be made aware of this policy through the website, newsletters, and school communications.

Mobile devices must be switched off and remain in bags during the school day. Parents and pupils to sign a disclaimer form if they wish to bring a mobile device into school (see Appendix 3).

Mobile phones brought into school are entirely at the staff member/ visitors' own risk. Trinity St Peter's Primary School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.

The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

Where parents or students need to contact each other during the school day, they should do so only through the school's telephone.

Email

Children may have access to messaging systems on iOs applications such as Google Classroom with approval from parents (e.g. children adding a comment when submitting an assignment). Other messaging or e-mail solutions may be used when appropriate for a particular year group.

Acceptable Use of Personal Equipment - Staff

Use of Facebook / Social networking sites

Staff are not permitted to access Facebook or most other social networking sites from a school computer whilst on school premises. Staff are permitted to use Twitter on school computers for educational purposes and networking. Social networking sites can be accessed on a personal handheld device at break times only.

Use of Mobile Phones and other personal mobile devices

Mobile phones and other personal mobile devices can be accessed at break times only for personal communication. Mobile Phones and personally-owned devices will be switched off or switched to 'silent' during the school day. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team.

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. Staff will be issued with a school phone where contact with students, parents or carers is required.

If staff have a personal emergency they are free to use the school's phone or make a personal call from their mobile in the designated staff area of the school, e.g. staffroom, an office area.

If any staff member has a family emergency or similar and is required to keep their mobile phone to hand, prior permission must be sought from the a senior manager and the mobile phone should be stored in an agreed location.

Use of Cameras

Images of pupils and/ or staff must only be stored on computers/drivers owned by the school. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.

Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own

personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such image

Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website.

Email

Emailing is used as one of the many ways we communicate with each other at Trinity St Peter's Primary School and is invaluable in such a large school. However, the system should be used responsibly and staff should always act in a professional manner when using the email system. Members of staff should not feel obliged to reply to any emails sent to them in the evenings or at weekends and equally staff should not expect a reply from colleagues outside school hours. Staff are reminded of this at the start of the school year.

Review and Monitoring

The Online Safety policy is referenced from within other school policies:

- The school has Computing and PSHE subject leaders who will be responsible for document ownership, review and updates;
- The Online Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school;
- The Online Safety policy has been written by the school Computing and PSHE subject leaders and is current and appropriate for its intended audience and purpose;
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

The school has achieved the 360 Degree Safe – Online Safety Award. It continues to use the Online Safety Review Tool to review its provision.

Incident Management / Handling complaints

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview with teacher/ Computing Subject Leaders/ SLT / Headteacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including online homework];
- Referral to LA / Police.

Class teachers act as first point of contact for any complaint and can seek guidance from the Computing Subject Leader or SLT. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.
Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Computing Subject Leader, Apex or Leadership Team.

All security breaches, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Computing Subject Leader.

Appendices

Appendix 1:

Trinity St Peter's C.E Primary School

Staff ICT Acceptable use policy - September 2022

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Trinity St Peter's Primary School allows staff to bring in personal mobile telephones for their own use. Users bringing in personal mobile telephones must ensure there is no inappropriate or illegal content on the device.

- I understand that personal devices should be kept in bags/cupboards and not out on desks. Mobile phones can be used in the staffroom and classrooms when the children are not present, but should not be used when walking around school or in places where children are.
- I understand my smart device e.g watch must not distract me during the day and will be set to school mode each morning.
- I understand that personal mobile phone calls/messages may only be taken during staff breaks or in staff members' own time. If staff need to have their phones for emergency use, they should notify the Leadership Team.
- I will not access Facebook or other social networking sites from a school computer whilst on school premises. Facebook can be accessed on personal handheld devices at break times only.
- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role and use appropriate language.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware or software.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff must only be taken and stored on computers / drivers owned by the school. Images will not be distributed outside the school network (eg. Website / local press) without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.

- I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. It is the responsibility of staff to be vigilant and report any concerns.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

Photographs

Photographs are taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements and are an effective form of recording their progression in the Early Years Foundation Stage. They may also be used on our website and/or by the local press with permission from the parents. However, it is essential that photographs are taken and stored appropriately to safeguard the children in our care. Only school devices are to be used to take any photos within the setting or on outings. Images taken on this device must be deemed suitable without putting the child/children in any compromising positions that could cause embarrassment or distress.

Social Networking

Online conduct should not be different to offline conduct.

Employees using social networking sites in a personal capacity must ensure that they do not conduct themselves in a way that is detrimental to the School. To do otherwise may lead to formal disciplinary action under the School's Disciplinary Procedure. They should not:

- Post offensive, defamatory or inappropriate comments about the School, its students, suppliers or any of its employees.
- Allow interaction on websites to damage or compromise working relationships with colleagues
- Make discriminatory or offensive comments about work colleagues or students.
- Post photographs/videos of themselves, colleagues or students taken in school or which is work related unless agreed by the Headteacher.
- Post or send abusive or defamatory messages.
- Record any confidential information about the School on any social networking sites
- Post information which would lead to the identification of a student.
- Accept requests of any pupil of the School or former pupils under the age of eighteen to become 'friends' on Facebook or any other social networking site.
- It is advisable not to accept requests from the parents or guardians of any pupil of the School or former pupils under the age of eighteen to become 'friends' on Facebook or any other social networking site. Should you wish to accept such a request you must seek advice from your Headteacher before doing so.
- Make a request to become 'friends' with any pupil of the School or former pupils under the age of eighteen as friends on Facebook or any other social networking site.
- Make a request to the parents or guardians of any pupil of the School or former pupils under the age of eighteen to become 'friends' on Facebook or any other social networking sites.
- It may be is necessary to create closed 'blogs' and social networking areas for curriculum purposes. Any such activity should be agreed in advance with the Headteacher.
- On occasions when it is appropriate for staff and students to share a closed 'blog' or social network area for curriculum purposes and permission has been given to do so, appropriate measures must be put in place to ensure the safety of the staff and pupils.
- Profiles on social media should not be traceable to a person's place of work.

User Signature

I agree to follow this code of conduct and to support the safe and appropriate use of ICT throughout the school and in my online activity.

Signature …….…… Date ……

Full Name ……..... (printed)

Appendix 2:

Dear Parent/Guardian,

At Trinity St Peter's Primary School, ICT, including the Internet, email, i-pads and mobile technologies; play an important role across the curriculum. We expect all children to be safe and responsible when using any form of ICT.

Please read and discuss these Online Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like further information please contact your class teacher, Mrs Molloy or Mr King.

Pupil Acceptable Use Policy

All pupils must follow the rules set out in this policy when using school computers, hand held devices and websites recommended by the school.

- I must not write anything that might upset someone or give the school a bad name.
- I know that the adults supervising me will regularly check what I have done on the school computers/I-pads. If I have not followed the school rules, I know this will be dealt with using the school's behaviour policy.
- I must not tell anyone my name, where I live, or my telephone number when using the Internet.
- I must log off after I have finished with my computer.
- I must not use the computers in any way that stops other people using them.
- I will only access websites that have been recommended by my teacher.
- I will report any websites that make me feel uncomfortable to my teacher, Mrs Molloy or Mr King.
- I will tell my parents, teacher, Mrs Molloy or Mr King straight away if I am sent any messages that make me feel uncomfortable at home or at school.
- I will not try to harm any equipment or the work of another person on a computer.
- If I find something that I think I should not be able to see, I must tell the adult supervising me straight away and not show it to other pupils.
- If I have a mobile phone in school, I must turn it off and hand it to my teacher who will keep it in the school office until the end of the day when it will be returned.

UNACCEPTABLE USE

Examples of unacceptable use include, but are not limited to:

- Creating or sending any messages that might upset other people.

- Accessing websites that have not been checked by an appropriate adult first.

This agreement is what we expect of the children whilst in school, we are sure you will help support us by following these guidelines at home also.

Please Return to Class Teacher

……..... (Child's name) has discussed and agreed to follow the Online Safety rules, to support the safe use of ICT at Trinity St Peter's Primary School.

Parent/Guardian Signature …….……..…….

Child's Signature ……. Class …… Date ……

Appendix 3:

Mobile Phone Permission Form

The use of mobile phones in school is strongly discouraged, as is the use of any other devices that allow for private communication, such as Smartphone watches. **The school cannot take responsibility for loss or damage to such devices.**

It is recognised that some pupils do require mobile phones for their journeys to and from school. Under these circumstances mobile phones may be switched on and used outside normal school hours. During school hours, mobile devices must be switched off and stored away in your child's school bag.

If a phone is activated during school hours, without the permission of a member of staff, it will be confiscated for the rest of that school day. If the mobile phone is used inappropriately, i.e. taking photographs or videos without permission, this privilege will be removed.

Parent/Guardian Permission

If you give permission for your child to bring their phone into school, please email the class teacher via their class account to give your approval and provide the name and mobile phone number of your child.

By sending this email, you agree that:

- You have read and understand the above information about appropriate use of mobile phones at Trinity St Peter's;
- You understand that your email will be saved and that the details may be used (and shared with a third party) to assist in the identification of a phone should the need arise (e.g. if lost, or if the phone is being used inappropriately);
- You give your child permission to carry a mobile phone to school and understand that your child will be responsible for ensuring that the mobile phone is used appropriately and correctly;
- You understand that the school accepts no responsibility for pupils who lose or have their mobile phones stolen.

Reviewed October 2025
Next review October 2026