Kirkstall St Stephen's C of E Primary School

Online Safety and Acceptable Use Policy

April 2025

This school is committed to safeguarding and promoting the wellbeing of all children, and expects our staff and volunteers to share this commitment.

Kirkstall St Stephen's C of E Primary School

Rationale

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

Our Vision

We are cherished – we aim to create a caring environment where all children and staff feel welcome, valued, supported and respected.
We are challenged- through a stimulating and challenging learning environment, where achievements are recognised but it is also safe to fail, increasing our resilience.
We are children of God – we recognise the value of each and every individual, encouraging everyone's unique spiritual development and potential.

Aims:

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

1. ICT and internet use in School

Acceptable use of ICT and the internet in school

The internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our pupils with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school. Some of the benefits of using ICT and the internet in schools are:

For pupils:

• Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.

• Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.

• Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.

• An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen. • Access to learning whenever and wherever convenient.

• Freedom to be creative.

• Freedom to explore the world and its cultures from within a classroom.

• Social inclusion, in class and online.

• Access to case studies, videos and interactive media to enhance understanding.

• Individualised access to learning.

For staff:

• Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.

• Immediate professional and personal support through networks and associations.

• Improved access to technical support.

• Ability to provide immediate feedback to pupils and parents.

• Class management, attendance records, schedule, and assignment tracking.

Unacceptable use of ICT and the internet in school

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings. This applies to anyone in our school community.

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

E safety lessons

Pupils will be taught about online safety as part of the curriculum. In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- How to safely use social media platforms

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

The school uses the Google internet legends scheme of work as well as the Twinkl E safety lessons to ensure all the content is covered.

Monitoring systems

All teachers use CPOMS to record any behaviour and safeguarding issues related to online safety. These will all be sent to the designated safe guarding lead to be reviewed and actioned.
This policy will be reviewed annually by the Designated Safeguarding Lead and ICT Lead. At every review, the policy will be shared with the governing board.

The Headteacher and Deputy Headteacher receive automatic and immediate emails from the school's website support team if an internet safety breach has occurred, such as a search for a flagged keyword or website. They also receive a daily report on any inappropriate searches. In both instances, the source device can be identified.

Managing information systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will

be reviewed regularly by the IT technicians, Computing leader and virus protection software will be updated regularly.

Published content and school website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, pupils, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects. The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office only.

Under the Data Protection Act 1998 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign our photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to.

This consent form outlines the school's policy on the use of photographs of children, including:

• how and when the photographs will be used

• how long parents are consenting the use of the images for

• parents understand they can withdraw their consent at any time

The school follows general rules on the use of photographs of individual children:

• Parental consent must be obtained. Consent will cover the use of images in:

- all school publications
- on the school website o in newspapers as allowed by the school
- in videos made by the school or in class for school projects.

• Electronic and paper images will be stored securely.

• Names of stored photographic files will not identify the child.

• Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed.

• For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.

• Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.

• Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils.

For more information on safeguarding in school please refer to our school child protection and safeguarding policy.

Use of Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

KSS recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

KSS will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policy.
Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Equal Opportunities

All children are to be supported to understand how to stay safe on the internet.

Teachers are to ensure they are aware of children who may be vulnerable through inappropriate internet use. This vulnerability is not exclusive to children who are vulnerable in other ways and as such teachers must be vigilant with any concerns being formally written as a Cause for Concern form.

All children must have access to the full computing curriculum and must all be exposed to learning that encourages e-safety awareness.

2. Pupils and Parents/Carers

School devices and working from home

Children who are asked to work from home will be provided with a school laptop. These laptops are monitored and checked regularly for content and exposure. They all have the appropriate firewall to ensure children can use the internet safely. Pupils will not be able to access social media on these devices.

Mobile phones and personalised devices

Pupils in Year 6 may bring mobile devices into school with written permission by parents, but are not permitted to use them during:

- Lessons
- Playground - before and after school
- Clubs before or after school, or any other activities organised by the school

Year 6 children will hand in their devices to their classteacher at 8.55am and they will be securely kept until 3.25pm.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Any pupil who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.

Images or files should not be sent between mobile phones in school.

If staff wish to use pupil devices in class as part of a learning project, they must get permission from a member of the senior leadership team.

Pupils are not allowed to use social media on the school site

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules or relates to a criminal offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation

Unacceptable pupil use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute

- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Cyber bullying and peer on peer abuse

As with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the behaviour policy. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff. The school will not tolerate cyberbullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined.

If an allegation of bullying or peer on peer abuse does come up, the school will follow the school's behaviour policy and :

• Take it seriously

• Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully

• Record and report the incident

• Provide support and reassurance to the victim

• Speak to the parents of the children immediately

• Take appropriate action

Expectations of Parents/carers

Parents/carers do not have access to the school's ICT facilities as a matter of course.
However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.
Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, we expect parents/carers to:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure
- Not use private groups, KSS DOJO accounts or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way
- Not use private groups, KSS DOJO accounts or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. We expect that parents/carers contact the school and speak to the appropriate member of staff if they are aware of a specific behaviour issue or incident
- Not upload or share photos or videos on social media of any child in school

3. Staff/Visitors and Volunteers

Expectations of staff- emails and CLASS DOJO accounts

The school provides each member of staff with an email address and class DOJO account.

This email/DOJO account should be used for work purposes only and emails should be password protected.

All work-related business should be conducted using the email/DOJO address the school has provided.

Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account. This is unless permission has been given by the Headteacher.

Staff must take care with the content of all email/DOJO messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email/DOJO messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email/DOJO. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
If staff receive an email/DOJO in error, the sender should be informed and the email/DOJO deleted. If the email/DOJO contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email/DOJO in error that contains the personal information of another person, they must inform the Headteacher and SBM immediately and follow our data breach procedure.

Expectations of school staff, volunteers and visitors- personal devices

The school expects staff/volunteers/visitors to lead by example. Personal mobile phones should be on 'silent' during school hours and not accessed during learning time, unless permission has been given by the Headteacher.

Staff/volunteers/visitors are not permitted to take photos or videos of pupils using personal devices. If photos or videos are being taken as part of the school curriculum or for a professional capacity, school equipment will be used for this.

Members of staff or volunteers/visitors should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

If contacting parent using their own personal device (in the event of parent home calls) staff must have the caller ID on private.

Any breach of school policy may result in disciplinary action against that member of staff or subsequent action towards a volunteer/visitor, such as a ban. Any criminal action will be passed onto the police.

Roles and responsibilities

The Headteacher, Senior Leaders and ICT leader

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The ICT Lead will work with the Headteacher and the Designated Safeguarding Lead to have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate online contact with adults, potential or actual incidents of grooming and cyberbullying.
These staff take on lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Address any online safety issues or incidents
- Any online safety incidents are logged on CPOMS
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing boar

The governing body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL), Headteacher or Deputy Head.

All governors will:

- Ensure that they have read and understand this policy
- Delegate a governor to act as E-Safety link
- Work with the ICT Lead to carry out regular monitoring and report to Governors
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

Links with other policies

This online safety policy is linked to our:

- Child protection policy and Keeping Children Safe in Education
- Behaviour policy and Anti-bullying policy
- Data protection policy and privacy notices
- Complaints procedure