Kirkstall St Stephen's C of E Primary School

Online Safety Policy

January 2022

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

Name of Policy

CONTENTS

Rationale

Aim

Legislation and guidance

Use of ICT in school

E safety lessons and social media

Monitoring arrangements

Managing information systems

Published content and school website

Cyber bullying and peer on peer abuse

Mobile phones and personal devices

Equal opportunities

Roles and responsibilities

Links to other policies

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.

KSS School Mission Statement

We are cherished, we are challenged, we are children of God

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.

Our Ethos Statement

Our school ethos is represented by the KSS Values Tree; showing children's growth as a tree planted firmly into God's sustaining love and rooted in our school values of: trust, justice, perseverance, respect, thankfulness and forgiveness.

This is based on Psalm 1:3.

They are like trees that grow beside a stream,
that bear fruit at the right time, and whose
leaves do not dry up. They succeed in
everything they do.

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 statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening

and confiscation. It also refers to the Department'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.

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.

E safety lessons

4Educating pupils about online safety 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.

Manging 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, ICT coordinator and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

• ensuring that all personal data sent over the internet or taken off site is encrypted

• making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this

• files held on the school network will be regularly checked for viruses

• the use of user logins and passwords to access the school network will be enforced

• portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team. For more information on data protection in school please refer to our data protection policy.

• Social media will not be used by pupils in school

• gaining parent consent before making contact and projects with other schools nationally and internationally

• in school, pupils should only use school-approved email accounts

• excessive social emailing will be restricted

• pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

• pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge. Pupils will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

• Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

• Staff should only use official school-provided email accounts to communicate with staff and parents. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.

• Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.

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.

E-safety policy (Year) 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.

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

Mobile phones and personalised devices

Pupils 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

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.

The school takes certain measures to ensure that mobile phones are used responsibly in school. Some of these are outlined below.

Pupils

• Pupils mobile phones must be handed in to the school office and switched off during the day

• 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 these devices in class as part of a learning project, they must get permission from a member of the senior leadership team.

• Pupils are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a pupil is found with a mobile phone in their possession it will be confiscated.

• 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

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

School staff

Staff will be discouraged from using their personal devices from school, however in the event they do need to use their personal device:

• Staff may only use their own personal devices to contact pupils or parents using the password protected dojo app.

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

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

• The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours and put in a locked cupboard with a passcode.

• Any breach of school policy may result in disciplinary action against that member of staff.

Mobile/smart technology

It is prohibited, whilst at school or college, for children or adults to sexually harass their peers via their mobile and smart technology, share indecent images: consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content. The school's 'Smoothwall' internet firewall is frequently monitored to ensure that this is adhered to.

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 smooth firewall to ensure children can use the internet safely. Pupils will not be able to access social media on these devices.

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.

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 and safeguarding policy
- Behaviour policy
- Data protection policy and privacy notices
- Complaints procedure

Updated: INSERT DATE HERE INSERT NAME OF REVIEWER