St Peter's Brafferton
C of E (VA) Primary School

Small school, big heart

As a church school, our vision is for each child to have a love of learning, hope, confidence, wisdom and respect for all.

'Life in all its fullness'

John 10:10

Online Safety Policy

This policy document reflects the online safety guidance developed in partnership between Education and Skills (NYCC, Inclusion Education (NYC), the local Safeguarding board, North Yorkshire Police, NYES Digital and representatives from local schools. The document sets out the statutory requirements for schools and settings alongside the roles and responsibilities for different members of the school community, the range of issues that need to be considered and signposting to further resources.

Background information

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

Keeping Children Safe in Education (September 2022) clearly states that,

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

> **content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
>
> **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
>
> **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
>
> **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams

Our online safety policy has been written and will be followed in conjunction with other school policies; specifically anti-bullying, information (data protection) policy, behaviour, child protection / safeguarding, relationships and sex education, ICT and acceptable use policies. This policy to applies to all members of the school community (including staff, pupils, governors, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems, both in and out of school, as well as use of personal technology whilst on the school premises or engaged in school activities.

The school's ICT leader is Mrs Sarah Anderson who will also act as online safety co-ordinator.

The Online Safety Policy and its implementation will be reviewed every 2 years or as needed.

At St Peter's Brafferton CE (VA) Primary School, online safety education will be provided in the following ways:

• A planned online safety programme is provided as part of the PSHE and collective worship programme and is regularly revisited in Computing and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school.

• A range of safeguarding issues are considered as part of the online safety education: keeping their personal information private, healthy relationships on and off line, grooming, sending inappropriate images and the consequences of this, gaming, gambling, radicalisation and how to recognise the signs and keep themselves safe

- Pupils are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Pupils are helped to understand the need for the Pupil Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in school
- Staff act as good role models in their use of ICT, the Internet and mobile devices and follow the ICT Acceptable Use policy at all times.

<u>Roles and Responsibilites</u>

<u>Headteacher:</u>

• Supporting the Governors comply with the online safety aspects of the Keeping Children Safe in Education, September 2022 documentation

• The safety (including online safety) of all members of the school community.

• Effective and regular training about online safety is provided for the whole school community, including Governors, and a log is kept of the staff who complete the training

• Effective communication with parents/ carers about safe practices when using online technology's and support them in talking to their children about these issues

• Effective filtering, monitoring and security systems are set up (see Appendix 2 for arrangements for ensuring online safety)

• There are effective procedures in place the event of an online safety allegation which are known and understood by all members of staff

• Establishing and reviewing the school online safety policy and documents and making them available on the school website

• Ensuring that the school's Designated Safeguarding Lead (at St Peter's Brafferton, this is the Headteacher) should be trained in online safety issues and be aware of the potential for serious child protection issues that could arise through the use of ICT.

<u>Governors:</u>

- Responsibility for the approval of the online safety policy, ensuring it is disseminated to the wider school community and for reviewing the effectiveness of the policy.

- Ensuring that the statutory requirements of Keeping Children Safe in Education (Sep 2020) are complied with, including ensuring that staff undergo regularly updated safeguarding training which includes online safety.

- Ensuring children are taught about safeguarding through teaching and learning opportunities, as part of providing a broad and balanced curriculum. This may include covering relevant issues through the PSHE curriculum.

All staff:

In addition to the elements covered in the ICT and Acceptable Use appendix, all staff are responsible for ensuring that:

- They have an up to date awareness of and attend training on online safety matters and of the schools current online safety policy and practices

- Online safety issues are embedded in all aspects of the curriculum and other school activities.

All pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Rules for Online Safety and Acceptable Use (see Appendix 1), which they will be reminded of annually and children in Year 3 upwards required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature. This will be re-issued every 2 years.

- Should understand the importance of adopting good online safety practice and reporting abuse, misuse or access to inappropriate materials and know how to do so.

Parents/Carers:

- Are responsible for endorsing (by signature) the Pupil Rules for Online Safety and Acceptable Use.

- Are invited to engage with guidance and training provided by school in online safety and the health effects of children and young people having too much 'screen time'.

This policy is also linked with Child Protection Policy and the Remote Learning Policy.

Monitored by: FGB
Date adopted: June 23
Next review: June 2025
Date of next review: 2 years

Appendix 1 Online Safety rules for EYFS and Y1; Y2 and KS2 Acceptable Use Agreement

School Rules for Class 1 and Preschool

- ✓ I follow my teachers' and parents' instructions.
- ✓ I keep my passwords a secret.
- ✓ I am kind to others and I use kind words.
- ✓ I only upload and write what I want others to see.
- ✓ I can tell my teachers or parents if someone is unkind to me on the internet or mobile phone.
- ✓ I check with my teachers or parents before using a website.
- ✓ I tell my parents or teachers if something worries or upsets me when I am using the internet.

Technology/Internet User Responsibilities
Class 2 and Class 3

- ✓ I act responsibly by following my teachers' and my parents' instructions when using technology/the internet.
- ✓ I am responsible for keeping my passwords private.
- ✓ I am a responsible user of the internet and I use appropriate language when I add items or send messages.
- ✓ I only upload and write what I want others to see.
- ✓ I act responsibly by telling my teachers if I think that someone else has broken the rules.
- ✓ I check with my teachers or parents before using any website.
- ✓ I am responsible for telling my parents or teachers if I see or read inappropriate material on the internet.

Pupil Signed ………………………………………………………………………..

Date ……………………………………..

Parent / Carer Signed ………………………………………………………………….. Date………………………….

Appendix 2 Acceptable use agreement for Staff and Visitors

ICT in its many forms - email, the internet, web2 technologies and mobile devices- are now part of our daily lives. This agreement is designed to ensure that all members of staff and visitors on school business are aware of their professional responsibilities when using any form of ICT and the related technologies.

All staff, Governors and visitors on school business:

- Must only use the school's email, internet and intranet and other related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body. Individual employees' internet and other related technologies can be monitored and logged and can be made available, on request, to their line manager or Headteacher.
- Must only use approved, secure email systems for any school business.
- Must not browse, download or send material that could be considered offensive, and should report any accidental access of inappropriate materials to their line manager.
- Should not use school information systems or resources (e.g. cameras, laptops, memory devices) for personal purposes without specific permission from the Headteacher; they should only be used for professional purposes.
- Are not permitted to use personal portable media for storage of school related data/images (e.g. USB stick) without the express permission of the Headteacher.
- Should ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off school premises, or accessed remotely. Personal data can only be taken out of school when authorised by the Headteacher or Governing Body using an encrypted stick. School laptops should only be taken off site if they have 'bitlocker'.
- Are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, including when on external trips/visits. With the written consent of parents (on behalf of parents) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. Digital images are easy to capture, reproduce and publish and, therefore, be misused.
- Will make every effort to comply with copyright and intellectual property rights.
- Should ensure that their use of web 2 technologies, including social networking sites, such as Facebook, Twitter, Instagram, Snapchat and Myspace, does not question or bring their professional role into disrepute. Members of staff:
  - Are advised to consider, and set appropriately, their privacy settings on such sites.
  - Should consider the appropriateness of images and material posted. Once posted online, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.
  - Should not communicate with pupils, in relation to either school or non school business, via web 2 technologies. Members of staff should only communicate with pupils using the appropriate LA/school learning platforms or other systems approved by the Headteacher.
- Are not permitted to contact or communicate with pupils, parents or conduct school business using personal email addresses or telephones, without specific permission from the Headteacher.
- Should not give out their own personal details, such as telephone/mobile number or email address, to pupils.
- Must ensure that all electronic communication with pupils and staff is compatible with their professional role.
- Will report any incidents of concern regarding staff use of technology and / or children's safety to the Headteacher or Designated Deputy Lead professional in line with our school's Safeguarding Policy.

Appendix 3 Arrangements for Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly by NYCC Schools ICT.

Virus protection is updated regularly.

Advice on security strategies will be monitored on the NYCC Schools ICT web page and clarification sought as necessary.

E-mail

Pupils may only use approved Microsoft e-mail accounts on the school system and email usage should be supervised and monitored by a staff member or parent.

Pupils must immediately tell a teacher if they receive offensive e-mail.

E-mails are "locked" to within the school community. Pupils will not be able to communicate by e-mail an external organisation or individual.

The forwarding of chain letters is not permitted.

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Pupil's work can only be published with the permission of the pupil and parents.

Remote learning through Microsoft Teams

Online learning can present unique student safety challenges. We have employed these settings via NYCC Schools ICT to ensure a safe and productive environment for your pupils and staff using MS Teams for remote learning: (please see hyperlink for more information)

Policy area	Policy	Primary students	Staff
Teams policies	Create private channels	Off	On
Meetings policies	Allow Meet now in channels	Off	On
	Allow the Outlook add-in	Off	On
	Allow channel meeting scheduling	Off	On
	Allow scheduling private meetings	Off	On
	Allow Meet now in private meetings	Off	On
	Let anonymous people start a meeting	Off	On

Policy area	Policy	Primary students	Staff
	Roles that have presenter rights in meetings	Staff can enable	On
	Automatically admit people (per-organizer policy)	Off	Organizer only
	Video Filters Mode	BlurandDefaultBackgrounds	AllFilters
Live events policies	Allow scheduling	Off	On
Messaging policies	Owners can delete sent messages	Off	On
	Delete sent messages	Off	On
	Edit sent messages	Off	On
	Chat	Off	On
	Use Giphys in conversations	Off	On
	Send urgent messages using priority notifications	Off	On
	Remove users from a group chat	Off	On
Teams apps	Microsoft apps	Off	Allow all apps
Voice	Make private calls	Off	On
Audio Conferencing setting	Dial-out from meetings	Off	Off

Social networking and personal publishing

The school will block/filter access to social networking sites.

Pupils will be advised never to give out personal details of any kind that may identify them or their location.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

The school will work with the NYES Digital to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to a staff member and Online Safety Coordinator.

The Headteacher will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Any new technologies or apps introduced will be subject to a Data Protection Impact Assessment and approved by Veritau, eg Class Dojo, Microsoft Teams.

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. Pupils are not permitted to bring electronic devices into school except in exceptional circumstances where this should be discussed with the Headteacher.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 – see Information Policy.

Authorising Internet access

All staff must read and sign the ‘Acceptable ICT Use Agreement’ before using any school ICT resource.

For EYFS and Key Stage 1, access to the Internet will be by adult demonstration with occasional supervised access to specific, approved on-line materials.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor NYCC can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the online safety policy is adequate and that its implementation is effective at least every 2 years.

Handling e-safety complaints

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

Any complaint about staff misuse must be referred to the head teacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure.

Discussions will be held with the North Yorkshire Police Schools Liaison Officer and / or Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school should deal with such incidents within the procedures set out in the online policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that takes place out of school