St Bede's Catholic Infant School
Internet Safety and Acceptable Use Policies

Agreed by Staff:	Spring 2023
Approved by Governors:	Spring 2023
Review Date:	Spring 2024

Signed by Chair of Governors: S. Howard Date: 30.2.2023

INTERNET SAFETY POLICY
Responsibilities
The member of school responsible for Internet Safety is Miss Parle. Miss Parle is the appointed Internet Safety coordinator and consults regularly with Miss Scragg as the Designated Safeguarding Lead. Mrs Lane is the designated Governor for Internet Safety.

Miss Parle is responsible for delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote Internet Safety within the school community. She also delivers/arranges workshops for parents.

Internet use and Acceptable Use Policies (AUPs)
All members of the school community agree to an Acceptable Use Policy that is appropriate to their age and role. (See Appendix 1)

A copy of the pupil AUP will be sent to parents. (See Appendix 2)

AUP's will be reviewed annually.

Children are made aware of the Acceptable Use Policies in school.

<u>The Prevent Duty</u>
The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's Computing curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent Duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

The Prevent Duty requires a schools monitoring and filtering systems to be fit for purpose.

Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents is gained if videos or photos of pupils are going to be used.

If photos/videos are to be used online then names of pupils should not be linked to pupils.

Staff must be fully aware of the consent form responses from parents when considering use of images. This is updated annually as part of the data collection exercise.

Staff should always use a school camera/ipad to capture images and should not use their personal devices.

Photos taken by the school are subject to the Data Protection Act.

Photos and videos taken by parents/carers

Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background, with

permission from associated parents.

Parents attending school based events will be reminded of their responsibilities in relation to social media verbally and through notices.

The parental letter concerning AUP's includes a paragraph concerning posting photos on social networking sites (see appendix 2)

Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

Mobile phones and other devices

St. Bede's Catholic Infant School recognises that staff may need to have access to mobile phones on site during the working day. However, there have been a number of queries raised within the local authority and nationally regarding the use of mobile phones and other devices in educational settings.

The concerns are mainly based around these issues:

- Staff being distracted from their work with children
- The use of mobile phones around children
- The inappropriate use of mobile phones

Ensuring the Safe and Appropriate Use of Mobile Phones

St. Bede's Catholic Infant School allows staff to bring in mobile phones for their own personal use. However, they must be kept securely at all times and are not allowed to be used in the toilets or in the play areas at any time. If staff fail to follow this guidance, disciplinary action will be taken in accordance to the school's staff code of conduct. If staff need to make an emergency call, they must do so out of sight/sound of the children. Staff must ensure that there is no inappropriate or illegal content on the device.

There are a number of children with medical needs whose critical medical data is analysed with the use of a mobile phone. These children have a designated mobile phone which is used continuously by trained school staff. These staff have permission to use the designated phones in the interest of Safeguarding.

Mobile phone technology may not be used to take photographs anywhere within the school grounds. There are digital cameras and tablets available within the school and only these should be used to record visual information within the consent criteria guidelines of the local authority and the school.

Pupils should not use mobile phones within the school grounds and should not bring in a mobile phone at any time – this includes use of smart devices (eg watches).

Use of Mobile Phones for Volunteers and Visitors

Upon their initial visit volunteers and visitors are given information informing them that they are not permitted to use mobile phones on the premises. If they wish to make or take an emergency call they may use either the main or the

Headteacher's office. Neither are volunteers or visitors permitted to take photographs or recordings of the children without the Headteacher's permission.

Important contact details of the children are kept on the school's mobile phone in case of an emergency.

All images are kept securely in compliance with the Data Protection Act.

If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated but staff should not 'search' the phone. The incident should be passed directly to SLT who will deal the matter in line with normal school procedures.

Use of e-mails
Pupils at St. Bede's Infants do not have access to the email system.

All staff have a school email address which should be used for all school correspondence.

Security and passwords
Passwords should be changed regularly. The system will inform users when the password is to be changed. Passwords must not be shared. Staff must always 'lock' the PC if they are going to leave it unattended. All users should be aware that the ICT system is filtered and monitored.

Data storage
Non-confidential data is stored on the school's private OneDrive account.

Staff use USB encrypted pen drives for storage of any confidential items and staff laptops are password protected with anti-virus software regularly updated.

Social networking
Pupils are not permitted to use social networking sites within school.

Internet Safety Education
Pupils
To equip pupils as confident and safe users of technology the school will undertake to provide:
a). A planned, broad and progressive Internet Safety education programme that is fully embedded for all children, in all aspects of the curriculum, in all years;
b). Regularly auditing, review and revision of the computing curriculum;
c). Internet Safety resources that are varied and appropriate and use new technologies to deliver Internet Safety messages in an engaging and relevant manner;
d). Opportunities for pupils to be involved in Internet Safety education e.g. through peer mentoring, Internet Safety committee, parent presentations etc.

Staff
a). All staff will have CPD on the Prevent duty;

b). Internet Safety training is an integral part of Child Protection / Safeguarding training and vice versa;
c). All staff have an up to date awareness of Internet Safety matters, the current school Internet Safety policy and practices and child protection / safeguarding procedures;
d). All new staff receive Internet Safety training as part of their induction programme, ensuring that they fully understand the school Internet Safety policy and Acceptable Use Policy;
f). The culture of the school ensures that staff support each other in sharing knowledge and good practice about Internet Safety;
g). The school takes every opportunity to research and understand good practice that is taking place in other schools;
h). Governors are offered the opportunity to undertake training.
i). The school takes part in the annual Safer Internet Day during which our Digital Leaders deliver an assembly to the whole school.
j). External agencies are arranged to deliver Internet Safety sessions for all children and parents.

Parents and the wider community
There is a planned programme of Internet Safety sessions for parents, carers, etc. This is planned, monitored and reviewed by the Internet Safety co-ordinator.

Monitoring and reporting
a). The school network provides a level of filtering and monitoring that supports safeguarding. Any notifications (Smoothwall) are sent to the Headteacher and Computing Subject Leader for review.
b). The impact of the Internet Safety policy and practice is monitored through the review / audit of Internet Safety incident logs, behaviour / bullying logs, surveys of staff, students /pupils, parents / carers
c). The records are reviewed / audited and reported to:

- the school's senior leaders
- Governors
- Halton Local Authority (where necessary)
- Halton Safeguarding Children Board

d). The school action plan indicates any planned action based on the above.

Appendices
Appendix 1 – Acceptable Use Policies
Acceptable Use Policy for learners in KS1

I want to feel safe all the time.
I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher or another trusted adult if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- talk to my teacher before using anything on the internet in school
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else.
.

Acceptable Use Policy for any adult working with learners
The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- implement the school's policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- respect the copyright and intellectual property rights of others
- only use approved email accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- only give permission to pupils to communicate online with trusted users.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with pupils
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to school
- promote any supplied Internet Safety guidance appropriately.

I know that anything I share online may be monitored.
I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.
I agree that I will not:

- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - inappropriate images
  - promoting discrimination of any kind
  - promoting violence or bullying
  - promoting racial or religious hatred
  - promoting illegal acts
  - breach any Local Authority/School policies, e.g. gambling
- do anything which exposes others to danger
- post any other information which may be offensive to others
- forward chain letters that breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
- store images or other files off site without permission from the head teacher or their delegated representative.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.
I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed _____

Your name (in block capitals): ……

Date:……

AUP Guidance notes for schools and governors
The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an Internet Safety Coordinator and a named governor takes responsibility for Internet Safety
- an Internet Safety Policy has been written by the school
- the Internet Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology establish if the Internet Safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

Appendix 2 – Parent letter – internet/e-mail use

St. Bede's Catholic Infant School

Parent / guardian name:……..
Pupil name: ……
Pupil's registration class: ……
As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet and other Computing facilities at school. I know that my daughter or son is aware of the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed, if the rules have to be changed during the year.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching Internet Safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's Internet Safety or e-behaviour. I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's Internet Safety.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to Internet Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community

Parent / Guardians' signature:……

Your name (in block capitals): ……

Date:……

Appendix 3 – School audit
Audit
The self-audit in should be completed by the member of the Management Team responsible for the Internet Safety policy.

Is there a school Internet Safety Policy that complies with Halton guidance? Yes
Date of latest update (at least annual): March 2022
The Leadership team member responsible for Internet Safety is: Miss Parle
The governor responsible for Internet Safety is: Helen Lane
The designated safeguarding lead: Miss Scragg
The Internet Safety Coordinator is: Miss Parle
The Internet Safety Policy was approved by the Governors: March 2022
The policy is available for staff at: School website and policy file
The policy is available for parents/carers at: School website
Date of Prevent training: (Annually and on Induction)

Parental Permissions

As part of our school activities, we take photographs or recordings of the children's learning and progress. Photos maybe used in children's books and/or displayed around school. Additionally, we use these to assess, record achievement and to celebrate school events.

There are also occasions where we may wish to use these images in other ways:

- school publicity material
- school website/Twitter page
- parent communication app (School Spider)
- local or national media

Please sign and complete the form below. If you ever need to withdraw consent for any reason, please let us know.

PLEASE √ THE APPROPRIATE BOX	
I **AGREE** to photographs/videos being taken of my child for the purposes mentioned above.	
I **DISAGREE** to photographs/videos being taken for the purposes mentioned above.	
Parent/Carer Name:	
Signature:	Date:

Parent's Name: (Block capitals please) Signature: Date:

Commercial photographers normally visit schools once a year for class or group photographs. Parents will be advised when this is to take place. Copyright of these photographs is retained by the photographer.