Reviewed May 2023

St Berteline's Church of England Primary School

E-Safety Policy & Acceptable Use Policy

Responsibilities

The member of school responsible for e-safety is Mr Charlie Hall. He is supported in his role by Mrs Kate Burton.

He 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 e-safety within the school community. He may also be required to deliver workshops for parents.

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

Examples of the AUPs used can be found in appendix 1.

Parents are made aware of the E-Safety Policy & Acceptable Use Policy which can be found on the school website.

The AUP will form part of the first lesson of ICT for each year group.

The Prevent Duty

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 ICT 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 need to be aware of the risks posed by online activity.

The Prevent Duty requires school 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 is encouraged. Parents give consent by signing the Home School Agreement.

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

Staff must always use a school camera 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.

Parents attending school-based events are reminded of their responsibilities in relation to social media both verbally and through the weekly newsletter.

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 Berteline's C of E Primary 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, changing rooms 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 either in the main office or The Den. Staff must ensure that there is no inappropriate or illegal content on the device.

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 school.

Pupils and adults must adhere to the school policy regarding the use of Mobile Phones, Smart Watches, Tablets and Cameras for Employees and Adults as well as the Social Media Policy. See school website for policy on Volunteer Helpers.

Use of Mobile Phones for Volunteers and Visitors

Upon their initial visit volunteers and visitors are given information informing them 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 office or The Den. Neither are volunteers or visitors permitted to take photographs or recordings of the children without the Headteacher's permission. See school website for policy regarding the use of Mobile Phones, Smart Watches, Tablets and Cameras.
Any misuse of a mobile phone will be dealt with initially by a member of the Senior Management Team.

Security and passwords

All computer devices are password protected. All users should be aware that the ICT system is filtered and monitored.

Reporting

All breaches of the e-safety policy will be referred to our Data Protection Officer and reported to the relevant supervisory authority if needed.

Incidents that are of a concern under the Prevent Duty should be referred to the Headteacher immediately who should decide on the necessary actions regarding safeguarding and the Channel Panel.

Incidents, which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to Headteacher.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse, then it should be handled according to the DFE document titled 'Dealing with

allegations of abuse against teachers and other staff'. If necessary, the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. CEOP button, trusted adult, ChildLine).

Infringements and sanctions

Whenever a student infringes the E-Safety & Acceptable Use Policy, the final decision on the level of sanction will be at the discretion of the school management.

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

Schools may involve external support agencies if needed eg Police.

Social networking

Pupils are not permitted to use social networking sites within school. Staff are reminded to adhere to the use of social media.

E-Safety Education Pupils

To equip pupils as confident and safe users of ICT the school will undertake to provide: a) A planned, broad and progressive e-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) E-safety resources that are varied and appropriate and use new technologies to deliver e-safety messages in an engaging and relevant manner

d) Opportunities for pupils to be involved in e-safety education e.g. appointment of e-safety officers, PCSO presentations, parent presentations etc

Additionally,

a) Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information

b) There are many opportunities for pupils to develop a good understanding of research skills

c) The school actively provides systematic opportunities for pupils / students to develop the skills of safe and discriminating on-line behaviour

Staff

a) A planned programme of formal e-safety training is made available to all staff. Additionally, all staff will have CPD on the Prevent duty.
b) E-safety training is an integral part of Child Protection / Safeguarding training and vice versa
c) All staff have an up-to-date awareness of e-safety matters, the current school e-safety policy and practices and child protection / safeguarding procedures
d) All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-safety Policy & Acceptable Use Policy
e) The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety
f) The school takes every opportunity to research and understand good practice that is taking place in other schools
g) Governors are offered the opportunity to undertake training.

Monitoring and reporting

The school network provides a level of filtering and monitoring that supports safeguarding.

The impact of the e-safety policy and practice is monitored through ongoing review.

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 if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else. If I am worried about anything, I will tell my teacher.

Acceptable Use Policy for learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.
I agree that I will:

- always keep my passwords a secret
- only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved and will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my own mobile device in school unless I am given permission
- only give my mobile phone number to friends I know in real life and trust
- only email people I know or approved by my school
- only use email which has been provided by school
- obtain permission from a teacher before I order online
- discuss and agree my use of a social networking site with a responsible adult before joining
- always follow the terms and conditions when using a site
- always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult that I know with me

Anything I do on the computer may be seen by someone else. If I am worried about anything, I will tell my teacher.
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.

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.
- respect the copyright and intellectual property rights of others
- 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 the named E-Safety officer
- promote any supplied E-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 letter 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 headteacher 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:…….

Acceptable Use Policy 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 E-Safety Coordinator and a named governor takes responsibility for E-Safety
- an E-Safety Policy & Acceptable Use Policy has been written by the school
- the E-Safety Policy & Acceptable Use Policy and its implementation will be reviewed regularly
- 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 E-Safety Policy & 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 the use of technology to establish if the E-Safety Policy & Acceptable Use Policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed regularly
- complaints of internet misuse will be dealt with by a senior member of staff