

BILLINGHAY CHURCH OF ENGLAND PRIMARY SCHOOL
E SAFETY POLICY
January 2024

Introduction

The requirement to ensure that children and young people are able to use the internet and related communication technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in our school. We must ensure that we keep children and young people safe and protected from harm both within and outside school.

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – pupils, all staff, governing body, parents.

Safeguarding is a serious matter; at Billingham Church of England Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to our pupils or liability to the school.

This policy is available for anybody to read on our school website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff e safety Policy. A copy of this policy and the Pupil Acceptable Use Policy will be sent home with pupils when they join the school and when the policy is amended with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet.

Headteacher Name: Mr R Allen

Signed:

Chair of Governors: Mr S Atkinson

Signed:

Review Date: Jan 24

Next Review: Jan 25

1. Roles & Responsibilities

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of e-safety at the school (Safeguarding Governor) who will:
 - Keep up to date with emerging risks and threats through technology use.
 - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
 - Receive half termly reports about e-safety incidents and monitoring.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to the e-Safety Officer (Mrs Pool) as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.
- Staff have read and understood the policy.

e-Safety Officer

The role of the e Safety Officer is combined with that of the ICT Subject Leader who works in conjunction with the Designated Safeguarding Lead who is the Headteacher.

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Ensure all members of staff have appropriate training on e-safety.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering and monitoring software, behaviour management software) are fit for purpose through liaison with the local authority and/or IT Technical Support.
- Use Smoothwall to monitor words and phrases on the internet and alert the Headteacher to any incidences when necessary.

IT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
 - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
 - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
 - Any e-safety technical solutions such as Internet filtering and monitoring are operating correctly.
 - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
 - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.
 - The IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made. See Appendix 1 for E Safety Incident Log), or in her absence to the Headteacher. If you are unsure the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision.
- They have an up to date awareness of e-safety matters and the policy.
- They have read, understood and signed the acceptable use policy.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils have a good understanding of the policy and acceptable use policy
- They monitor the use of digital technologies in lessons and other school activities and implement current policies with regard to these devices.
- In lessons where internet use is planned pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the Pupil Acceptable Use Policy (see appendix 1); any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Pupils are responsible for:

- Using technology in accordance with the Acceptable Use Policy for students (see appendix 1).
- Having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations appropriate to their age.
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- Knowing and understanding policies on the use of mobile devices and digital cameras, taking and the use of images and on cyber-bullying.
- Understanding the importance of adopting good online safety practice when using digital technologies inside and outside school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through communication via letters, newsletters and workshops the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs to have rules in place to ensure that their child/ren can be properly safeguarded. As such parents will sign the Pupil Acceptable Use Policy before any access can be granted to school ICT equipment or services.

2. Technology

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation, cyberbullying: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

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

- content: being exposed to illegal, inappropriate or harmful material;
- contact: being subjected to harmful online interaction with other users; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Filters and monitoring

As a school we recognise the importance of doing all that we reasonably can to limit children's exposure to the above risks from our IT system. As part of this process, governing bodies should ensure their school has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, governing bodies should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.

The appropriateness of any filters and monitoring systems are a matter for individual schools and will be informed in part by the risk assessment required by the Prevent Duty.

We recognise that whilst filtering and monitoring are an important part of the online safety picture for schools to consider, it is only one part. We need to consider a whole school approach to online safety which includes a Use of Mobile Technology Policy.

We also recognise that whilst it is essential to ensure that appropriate filters and monitoring systems are in place, we should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Billinghay Church of England Primary School uses a range of devices including PC's, laptops and ipads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Subject Leader, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Monitoring – School followed the buying advice guidance on e-security available from the National Education Network-NEN and purchased Future Digital for monitoring Internet usage.

Email Filtering – we use software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff passwords will change on a termly basis or if there has been a compromise, whichever is sooner. Pupil passwords will be changed if there has been a compromise. IT Support will be responsible for ensuring that passwords are changed.

Anti-Virus – All capable devices will have anti-virus software ESET endpoint. This software will be updated at least weekly for new virus definitions. F1 Group will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

3. Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety Policy and the staff e Safety Policy; pupils upon signing and returning their acceptance of the Acceptable Use Policy.

Internet activity will be monitored to ensure, as much as possible, that users are not exposed to illegal or inappropriate websites, including terrorist and extremist material and to ensure, as much as possible, that users do not actively seek access to illegal or inappropriate websites including terrorist and extremist material. These checks will be carried out by the e-Safety Officer or the Headteacher and records will be kept.

We must ensure that our pupils are safe from online terrorist and extremist material. This is typically by appropriate levels of filtering and monitoring.

What will happen in the event of a pupil being exposed to offensive or upsetting material?

If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will wish to respond to the situation quickly by following these steps:

- all pupils will be taught to switch off the monitor and report what they have seen to the teacher in charge;

- support will be given to the pupil/pupils involved, the Headteacher will inform parents/carers and they will be given an explanation of the course of action the school has taken;
- the ICT Subject Leader will be informed and report the URL (address) and content to our IT Support.
- Class teachers will give general guidance as a reminder of what to do in this event.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Students are permitted to use the school email system, and as such will be given their own email address.

How will e-mail be managed?

Pupils will learn how to use an e-mail application and be taught e-mail conventions. Staff and pupils will begin to use e-mail to communicate with others, to request information and to share information.

- Communications with persons and organisations will be managed to ensure appropriate educational use and the good name of the school is maintained.
- The forwarding of chain letters will be banned.
- Pupils may send e-mail as part of planned lessons using their e-mail addresses.
- E-mail sent out of school must be approved before sending.
- Pupils must not reveal details of themselves or others such as addresses or telephone numbers or arrange to meet anyone in e-mail communications.
- Pupils must ask an adult before they open an email so an adult can be present to read the received email.

Photos and videos – Digital media such as photos and videos are covered in the schools' Use of Photographs Policy. All parents must sign a parental consent slip when their child joins school or when the policy is amended; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; Billingham Church of England Primary School is supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within our school and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school.
- Facebook – used by staff in school.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.

- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are “comment enabled”, comments are to be set to “moderated”.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

How will publishing on the Web be managed?

The school has a web site. A web site can celebrate good work, promote the school and publish resources for projects or homework. As the school’s web site can be accessed by anyone on the Internet, the security of the staff and pupils must be maintained.

- Class teachers are responsible for organising the information to be entered onto the web site.
- All material must be the author’s own work, credit other work included and state clearly the author’s identity or status.
- The point of contact on the web site will be the school’s address and telephone number. Home information or individual e-mail identities will not be published.
- Group photographs should not have a name list attached and any child featuring in a photograph must have parental permission allowing them to be published on the site.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in her absence to the Headteacher. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log (See Appendix 2).

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues.

e-Safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student’s learning.

Appendix 1
KS1 children

My name is _____

To stay **SAFE online and on my devices**, I follow the Digital 5 A Day and:

1. I only **USE** devices or apps, sites or games if a trusted adult says so
2. I **ASK** for help if I'm stuck or not sure
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I look out for my **FRIENDS** and tell someone if they need help
6. I **KNOW** people online aren't always who they say they are
7. Anything I do online can be shared and might stay online **FOREVER**
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to
9. I don't change **CLOTHES** in front of a camera
10. I always check before **SHARING** personal information
11. I am **KIND** and polite to everyone

✓

My trusted adults are:

_____ **at school**
_____ **at home**

For parents/carers

To find out more about online safety, you can read Billingham C of E Primary School's full Online Safety Policy for more detail on our approach to online safety.

You can find support and online safety resources for parents at parentsafe.lgfl.net

KS2 children

This agreement will help keep me safe and help me to be fair to others

1. **I learn online** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. **I ask permission** – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. **I am creative online** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things, and I remember my Digital 5 A Day.
I am a friend online – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
4. **I am a secure online learner** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
5. **I am careful what I click on** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes add-ons can cost money, so it is important I always check for these too.
6. **I ask for help if I am scared or worried** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
7. **I know it's not my fault if I see or someone sends me something bad** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
8. **I communicate and collaborate online** – with people I already know and have met in real life or that a trusted adult knows about.
9. **I know new online friends might not be who they say they are** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
10. **I check with an adult before I meet an online friend** face to face for the first time, and I never go alone.
11. **I don't do live videos (livestreams) on my own** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
12. **I keep my body to myself online** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
13. **I say no online if I need to** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
14. **I tell my parents/carers what I do online** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
15. **I am private online** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
16. **I am careful what I share and protect my online reputation** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
17. **I am a rule-follower online** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.

18. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
19. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
20. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
21. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

~~~~~

**I have read and understood this agreement.**

**If I have any questions, I will speak to a trusted adult: at school that includes an adult  
working in my classroom, Mrs. Pool or Mr. Allen.**

**Outside school, my trusted adults are**\_\_\_\_\_

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_

### **For parents/carers**

If your parents/carers want to find out more, they can read Billingham C of E Primary School's full Online Safety Policy for more detail on our approach to online safety. They will also have been asked to sign an AUP for parents.

## Appendix 2

### BILLINGHAY CHURCH OF ENGLAND PRIMARY SCHOOL

#### E Safety Incident Log

|                                                       |                                                                                                                                                                                                                                                                                                                    |                                            |                                                    |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|----------------------------------------------------|
| Details of incident                                   |                                                                                                                                                                                                                                                                                                                    |                                            |                                                    |
| Date                                                  |                                                                                                                                                                                                                                                                                                                    | Time                                       |                                                    |
| Where did the incident occur?                         |                                                                                                                                                                                                                                                                                                                    |                                            |                                                    |
| Name of person reporting incident                     |                                                                                                                                                                                                                                                                                                                    | Who was involved in incident (please tick) | Child:<br>Staff Member:<br>Other (please specify): |
| Names of those involved                               |                                                                                                                                                                                                                                                                                                                    |                                            |                                                    |
| Type of incident (please tick)                        | Bullying/harassment:<br>Online bullying or harassment (cyberbullying):<br>Sexting (self taken indecent imagery):<br>Deliberately bypassing security or access:<br>Hacking or virus propagation:<br>Racist, sexist, homophobic religious hate material, terrorist or extremist material:<br>Other (please specify): |                                            |                                                    |
| Description of incident                               |                                                                                                                                                                                                                                                                                                                    |                                            |                                                    |
| Nature of incident (please tick)                      | Deliberate access:<br>Accidental access:                                                                                                                                                                                                                                                                           |                                            |                                                    |
| Did the incident involve material being (please tick) | Created:<br>Viewed:<br>Printed:<br>Shown to other:<br>Transmitted to others:<br>Distributed:                                                                                                                                                                                                                       |                                            |                                                    |
| Could this incident be considered as (please tick)    | Harassment:<br>Grooming:<br>Cyberbullying:<br>Sexting:<br>Breach of AUP:<br>Other (please specify):                                                                                                                                                                                                                |                                            |                                                    |

|                                            |  |
|--------------------------------------------|--|
| Action Taken                               |  |
| Outcome of incident/investigation          |  |
| Learning from the case and recommendations |  |

Signed:

Print name:

Date: