



# Online Safety Policy

Date	Reviewed by	Agreed by governors	Next due for review
September 2023	Helen Wallace	November 2023	October 2024

**BEDS-created**

**Statutory**

**1-year recommended review cycle**

**Believe to achieve! “Roots will grow down into God’s love and keep us strong.” Eph 3:17**

**Values: Friendship, Respect, Trust, Courage, Perseverance, Thankfulness**

Brinkworth Earl Danby’s is committed to providing a secure, happy and stimulating learning environment in which EVERYONE is valued, spiritual growth is nurtured and potential maximised. We believe as a community that each child can reach their vocational potential. We believe each child is of unique worth made in the image of God. We believe in each child being the best that they can be and finding their place in the world. We believe in: a child’s potential; being part of a community; being the best you can be.

In partnership with parents/carers, we aim to:

- create a happy, caring atmosphere in which each child feels secure and valued within an environment which is stimulating and attractive
- meet each child’s needs physically, creatively, intellectually, emotionally and socially
- educate children about a diverse society and world in order to promote understanding and positive attitudes
- help the child acquire a set of moral and spiritual values that reflect our designation as a Church of England Voluntary Controlled Primary School
- inspire each child to be an enthusiastic learner and develop capabilities and attributes that ‘build learning power’
- enable pupils to become confident and responsible citizens

Our ethos underpins our unique culture and behaviour in our Church of England School. Our children are at the centre of every decision made. We always ask ‘of what benefit will this be to our children? Will this help support them to be the best they can be?’ We go the extra mile. Whether it is staff, parents, children, governors or community members, we choose to make that extra effort for a better outcome for individuals and for our school community.

This policy is written with our vision, values, ethos and aims at its heart.

### Policy Statement

The internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning, such as phones. Computer skills are vital to access life-long learning and employment.

Young people have online access from many places - home, school, friends' homes, libraries and in some cases, mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help educate young people on online safety.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an online environment as possible and a need to teach them to be aware of, and respond responsibly to, the risks.

The DfE Keeping Children Safe in Education statutory guidance requires Local Authorities, Multi Academy Trusts, and schools in England to ensure learners are safe from harm:

*"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to **online safety** empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate"*

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of school. It also applies to the use of personal digital technology on the school site (where allowed).

Brinkworth Earl Danby's CE Primary School will deal with such incidents within this 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.

Its aims are to protect learners from potential harm, both on and off-site and to demonstrate a commitment to appropriate use of digital technologies.

### Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will mainly be carried out by the Safeguarding-link Governor receiving regular information about online safety incidents and monitoring reports, as part of termly safeguarding reviews with the Headteacher/Designated Safeguarding Lead.

The Headteacher/Designated Safeguarding Lead has a duty of care for ensuring the safety (including online safety) of members of the school community. They have undertaken training on online safety issues and are aware of the online child protection/safeguarding issues. They ensure that key online safety messages are reinforced through all stakeholder communications such as via newsletters, as part of a planned programme of assemblies etc.

The Business Manager liaises with those with technical responsibilities (Oakford Technology Ltd) to ensure:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority/MAT/other relevant body online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering system from Netsweeper is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is monitored termly with the Headteacher, in line with visits from the Safeguarding-link Governor, in order that any misuse/attempted misuse can be actioned
- that all users have clearly defined access rights to school technical systems and devices for example via the teacher or pupil profiles
- that all school networks and systems are password-protected

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they report any suspected misuse or problem to the Headteacher for investigation/action/sanction
- online safety issues are embedded in all aspects of the curriculum and other activities
- they teach pupils to understand and follow acceptable use policies
- they give pupils a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be 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

Pupils:

- are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement at [Appendix 2](#)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

## Online Safety at school

The DfE guidance "Keeping Children Safe in Education" states:

"All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."

When using communication technologies, Brinkworth Earl Danby's CE Primary School considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *Personal e-mail addresses, text messaging or social media must not be used for these communications.*
- personal devices will not be used for school work or taking images without prior approval
- staff will be aware of pupils whose images must not be taken/published
- pupils full names will not be used online, particularly in association with photographs
- any images will be stored in line with the school Retention Policy
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community

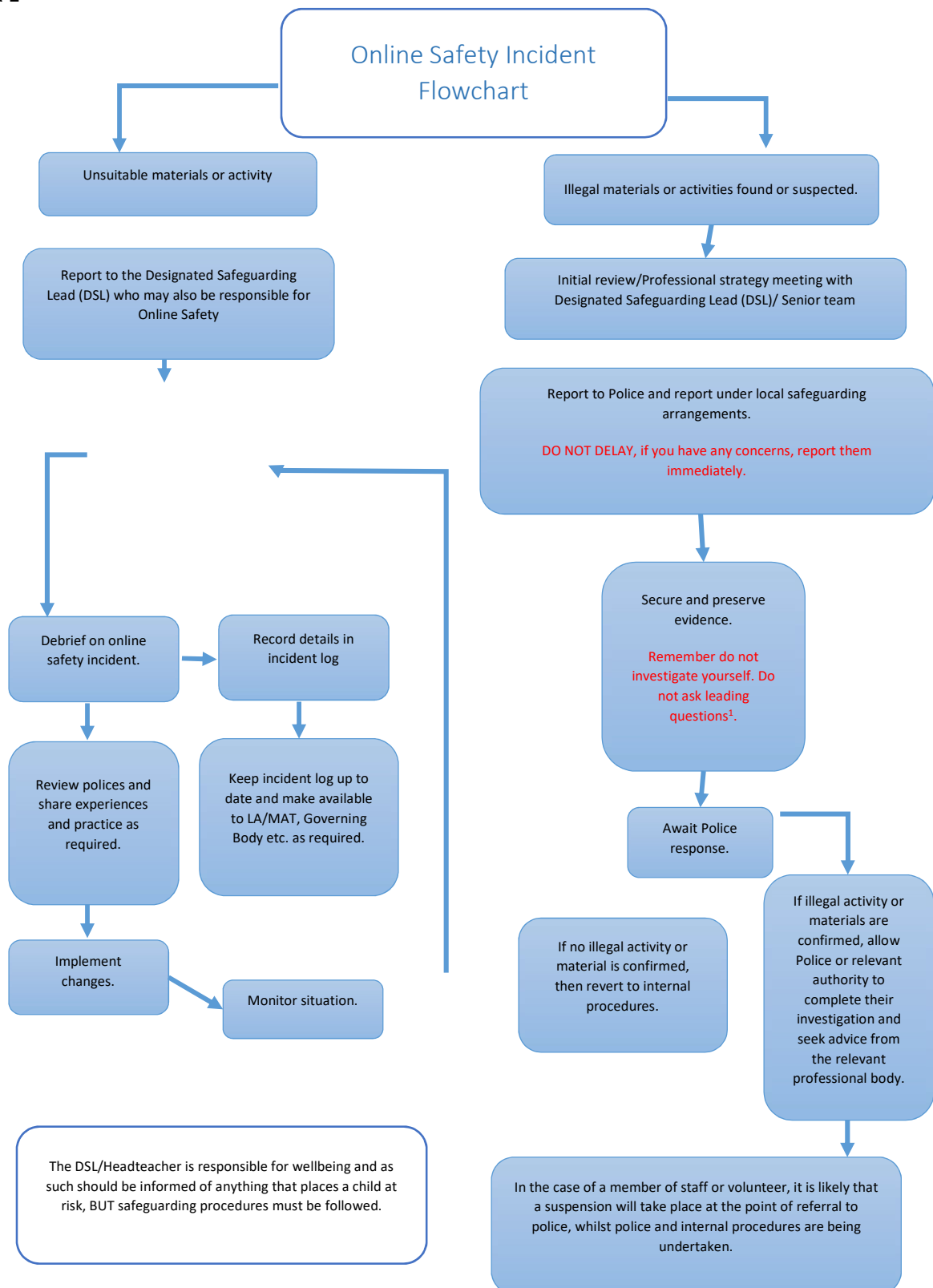
- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- the Designated Safeguarding Lead, Business Manager and other responsible staff have appropriate skills and training to deal with online safety risks.
- [Staff will sign and adhere to the acceptable use agreement at Appendix 3](#)

### **Online Safety out of school**

Brinkworth Earl Danby's CE Primary School will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- that information is provided to parents and carers to promote online safety
- that the school community is aware of reporting routes, consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm ([see flowchart and user actions chart in Appendix 1](#)), the incident must be escalated through the agreed school safeguarding procedures

## Appendix 1



## Appendix 2

### Acceptable Use Agreement – for younger learners

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or teaching assistant if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child): .....

Signed (parent): .....

## Appendix 3

### Acceptable Use Agreement – for staff

#### **Laptop/device policy for Brinkworth Earl Danby's school staff**

1. The laptop/device remains the property of Brinkworth Earl Danby's School.
2. The device is allocated to a named member of staff and is their responsibility. Only Brinkworth Earl Danby's School Staff should use the laptop/device.
3. On the teacher leaving the school's employment, the laptop is returned to Brinkworth Earl Danby's School. Staff on extended leave of 4 weeks and over should return their laptops to the school (other than by prior agreement with the Headteacher).
4. When in school and not being used, the laptop or other device such as digital camera must be kept in an office, locked room or drawer. It must not be left in an unlocked, unattended classroom.
5. Whenever possible, the laptop must not be left in an unattended car. If there is a need to do so, it should be locked in the boot.
6. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the Headteacher with evidence of adequate insurance.
7. Staff may load their own software onto the laptop but it must be fully licensed and not corrupt any software or systems already installed on the laptop. Any software loaded must not affect the integrity of the school network.
8. If any removable media is used then it must be checked to ensure it is free from any viruses. Digital camera SD cards must be uploaded to the shared media drive and then images erased and cards kept in cameras.
9. It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the laptop is kept up to date.
10. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
11. Students must never use the laptop.
12. If any fault occurs with the laptop, it should be referred immediately to the IT subject leader.
13. The laptop would be covered by normal household insurance. If not it should be kept in school and locked up overnight.

#### **Online Safety: Staff, Governors and Volunteers Responsible Use Agreement**

This Responsible Use Agreement is part of the school's Online Safety Policy and must therefore be adhered to at all times. The agreement is intended to ensure that:

- All staff, governors and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.
- The school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff, governors and volunteers are protected from potential risk in their use of IT in their everyday work.

#### **For my professional and personal safety:**

- I understand that the school will monitor the use of the IT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school IT systems (e.g. laptops, email etc.) out of school.
- I understand that the school IT systems are primarily intended for educational use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Headteacher.
- I will only use the email address given to me by school for any school communication

#### **I will be professional in my communications and actions when using school IT systems:**

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will not delete any resources produced for whole department use unless they have been updated.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language.



- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use social networking sites in school.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner. I will not give students my personal email address.
- I will only give students my personal mobile phone number if authorised (for example on a school trip) and will tell students to delete any staff numbers once they are no longer needed.
- I will not contact any students via a social networking site and will ensure that there is nothing inappropriate on the public profile of my social networking site.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos) and will ensure I have permission for the use of others' original work.

**The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:**

- When I use my personal hand held/external devices (tablets/laptops/mobile phones/USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on any machine, or store programs on a computer, nor will I try to alter computer settings without the permission of the Headteacher.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will encrypt any data that is determined to be personal or sensitive in nature if transporting it (e.g. on a USB stick).
- I will not store any data which includes details of students on any personal devices.

**I understand that I am responsible for my actions in and out of school:**

I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

*To be shared with all and signed by permanent staff members*

**Name:**..... **Signature:** ..... **Date:** .....