Online Safety Policy

Brixworth CEVC Primary School

Approved by:	Full Governing Board
Last reviewed on:	March 2024

Contents

.....

1. Aims

Our school aims to:

Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology including mobile and smart technology

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as child to child 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** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation and Relationships and sex Education. It also refers to the Department's guidance on protecting children from radicalisation..

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

All governors will:

- **Ensure that they have read and understand this policy**
- **Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)**

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings) as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children

The governing board will co-ordinate regular meetings with the appropriate staff to discuss online safety, requirements or training, and monitor online safety logs as provided by the designated safeguarding lead (DSL)

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manager filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and in appropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is **Jeannet Roberts**

All governors will:

- Ensure they have read and understand this policy

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2/3)
- Ensure that online safety if a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching and safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or diabilities (SEND). This is because of the importance of recognising that a "one size fits all" approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated online safeguarding lead

The designated online safeguarding lead is the headteacher

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The Online Safety Lead takes lead responsibility for online safety in school, in particular:

- **Supporting the DSL in ensuring that staff understand this policy and that it is being implemented consistently throughout the school**
- **Working with the DSL, ICT manager and other staff, as necessary, to address any online safety issues or incidents**
- **Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy**
- **Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy**
- **Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)**
- **Liaising with other agencies and/or external services if necessary**
- **Providing regular reports on online safety in school to the governing body**

3.4 Onsite technical support

The ICT consultant is responsible for:

- **Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material**
- **Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly**
- **Conducting a full security check and monitoring the school's ICT systems on a weekly basis**
- **Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files**

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- **Maintaining an understanding of this policy**

- **Implementing this policy consistently**
- **Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 4), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)**
- **Following the correct procedures of Brixworth CEVC Primary School if they need to bypass the filtering and monitoring systems for educational purposes**
- **Knowing that the DSL on-line safety lead is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing the on-line safety lead**
- **Working with the Online Safety Lead to ensure that any online safety incidents are logged (see appendix) and dealt with appropriately in line with this policy**
- **Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy**
- **Responding appropriately to all reports and concerns about sexual violence and/or harassment both online and offline and maintaining an attitude of "it could happen here"**

This list is not intended to be exhaustive

Staff responsibility

- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.6 Parents

Parents are expected to:

- **Notify a member of staff or the headteacher of any concerns or queries regarding this policy**
- **Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)**
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:

UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Online Safety, NSPCC: https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Helping parents keep their children safe online, Internet Matters https://www.internetmatters.org/

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. This will be taught at least once per half term

In **Early Years**, pupils will be taught to:

- **Ask permission before using technology, particularly the internet.**
- **Understand the term 'privacy'**

In **Key Stage 1**, pupils will be taught to:

- **Use technology safely and respectfully, keeping personal information private**
- **Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies**

Pupils in **Key Stage 2** will be taught to:

- **Use technology safely, respectfully and responsibly**
- **Recognise acceptable and unacceptable behaviour**
- **Identify a range of ways to report concerns about content and contact**

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

- The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home via ParentMail, and in information via our website, weekly newsletter called Primary Word. This policy will also be shared with parents.

Online safety may also be covered during parents' events.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the Online Safety Lead.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their class, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

There are links on the website on cyber-bullying so that parents are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The headteacher will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- **Cause harm, and/or**
- **Disrupt teaching, and/or**
- **Break any of the school rules**

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Online Safety Lead or other member of the senior leadership team to decide whether they should:

- **Delete that material, or**
- **Retain it as evidence (of a criminal offence or a breach of school discipline), and/or**
- **Report it to the police**

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the Brixworth CEVC Primary School complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Brixworth CEVC Primary School recognizes that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the for of "deepfakes" where AI is used to create images, audio or video hoaxes that look real. The includes deepfake pornography, pornographic content created using AI to include some's likeness

Brixworth CEVC Primary School will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the School

7. Acceptable use of the internet in school

All pupils, staff and any person from an organisation who accesses the school's internet are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

Unsuitable/inappropriate activities appendix 4

8. Pupils using mobile devices/ smartwatches/ fitness trackers in school

Children in Year 5 and 6 may bring mobile devices into school, but are not permitted to use them on the school premises. They **must** be turned off and handed into their class teacher at the start of the school day.

Children in KS2 may wear smartwatches/fitness trackers but they must be set so the children cannot access notifications or the virtual assistant.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using devices inside and outside school

.9.1 School devices

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

9.2 Personal devices

Staff members wishing to use personal devices inside or outside of school to record school related activities must request permission. (appendix 3a)

Staff are permitted to wear fitness trackers and smartwatches in school but they must be set so that emails, phone calls and text messages are not received during teaching time.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.(*School Actions and Sanctions Appendix 5)*

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The Online Safety Lead logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

13. Links with other policies

This online safety policy is linked to our:

- **Child protection and safeguarding policy**
- **Behaviour policy**
- **Staff disciplinary procedures**
- **Data protection policy and privacy notices**
- **Complaints procedure**
- **Screening, confiscating and Searching Policy**

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school's ICT systems and accessing the internet in school, I will not: **Use them for a non-educational purpose** **Use them without a teacher being present, or without a teacher's permission** **Access any inappropriate websites** **Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)** **Use chat rooms** **Open any attachments in emails, or follow any links in emails, without first checking with a teacher** **Use any inappropriate language when communicating online, including in emails** **Share my password with others or log in to the school's network using someone else's details** **Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer** **Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision** If I bring a personal mobile phone or other personal electronic device into school: **I will not use it on the school premises** I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement for Adults

Acceptable use of the school's ICT systems and the internet: agreement for adults in school	
Name of adult:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: **Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature** **Use them in any way which could harm the school's reputation** **Access social networking sites or chat rooms** **Use any improper language when communicating online, including in emails or other messaging services** **Install any unauthorised software** **Share my password with others or log in to the school's network using someone else's details**	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and Online safety lead know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3 - Use of Devices

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*		*No*	*No*
Internet only	*Yes*	*Yes*	*Yes*		*Yes*	*Yes*

Communications Technologies	Staff and other adults				Pupils			
	Allowed	Allowed with permission	Allowed for selected staff	Not allowed	Allowed	Allowed with permission	Allowed for selected pupils	Not Allowed
Mobile phones may be brought into school	✓					✓		
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones/cameras		✓						✓
Use of other mobile devices e.g. tablets, gaming devices, smartwatches, fitness trackers	✓					✓		
Use of personal e-mail address in school, or on school network	✓							✓
Use of school e-mail for personal e-mail				✓	Na			
Use of messaging apps in social time	✓				Na			
Use of social media in school time	✓				Na			
Use of blogs	n/a				Na			

Appendix 3a – Use of personal devices

ONLINE SAFETY POLICY

SPECIFIC WRITTEN PERMISSION FORM

In line with the school's Online Safety Policy, I request permission to use my *personal digital recording equipment in school or on school related activities to assist/enhance teaching and learning.

**A personal device is personal digital recording equipment including cameras, phones, flip cams, iPads or other devices for taking/transferring images of pupils or staff.*

The school's policy assumes school equipment will be used at all times except in exceptional circumstances.

To be completed by the member of staff:

Reason for requesting to use own equipment e.g. superior image quality, shortage of school equipment:
Place and context of use e.g. educational visit, recording learning or outcomes, sports day, performance:
Device to be used: Date of use:

I agree to download images/or digitally recorded images that I wish to save to the school's intranet/or my school allocated laptop and delete all images and video from the equipment's own memory as soon as possible or within three days.

Staff name (print)……..
Signed…….

Head Teacher's permission agreed / permission refused

Signed (Head teacher)……
Date……

<u>This form when completed by the member of staff and signed by the Head Teacher constitutes the required written permission.</u>

Appendix 4 Report Log

Date:	Time:
Name of child/adult:	Class:
Setting:	
Other adults present:	
Description/nature of incident/concern	
Action taken at time of incident:	
Action taken following incident:	
Signed:	Name and position:

Appendix 5 Misuse Flowchart