Online safety policy

Barn Croft Primary School

Approved by:	Full Governing Body	Date: December 2023
Last reviewed on:	December 2023	
Next review due by:	December 2024	

Contents

1. AIMS

Our school aims to:

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

> Identify and support groups of pupils that are potentially at greater risk of harm online than others

> 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 (which we refer to as 'mobile phones')

> 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 peer-to-peer 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 seminudes 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 (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

> Teaching online safety in schools

> Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

> Relationships and sex education – remove if not applicable, see section 4]

> Searching, screening and confiscation

It also refers to the DfE'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.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

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 appropriate staff to discuss online safety, requirements for 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 these standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;

- Reviewing filtering and monitoring provisions at least annually;

- Blocking harmful and inappropriate 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 Colin Whitehead.

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 3)

> Ensure that online safety is 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 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.

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 safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

> Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

> Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

> Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

- Working with the ICT Support provider (ROCIT Solutions) and LGfL to make sure the appropriate systems and processes are in place

- Working with the headteacher, ICT Support provider (ROCIT Solutions), LGfL and other staff, as necessary, to address any online safety issues or incidents

- Managing all online safety issues and incidents in line with the school's child protection policy, behaviour policy/online safety policy.

- Ensuring that any online safety incidents are logged (see appendix 5) 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/online safety policy.

- Updating and delivering staff training on online safety

- Liaising with other agencies and/or external services if necessary

- Providing regular reports on online safety in school to the headteacher and/or governing board

- Undertaking annual online safety risk assessments that consider and reflect the risks children face

- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

- Providing regular safeguarding and child protection updates, including online safety to parents and pointing parents to key information.

3.4 The ICT Support Provider (ROCIT Solutions alongside LGfL)

The Headteacher is responsible for ensuring that the ICT Support Provider implements the following:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept 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 fortnightly basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Ensuring that any online safety incidents are logged (see appendix 5) 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 and anti-bullying policy

- Reporting any concerns to the Headteacher/DSL in a timely fashion

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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

> Knowing that the DSL 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 DSL immediately and recording the incident on MyConcern. The ICT Provider will be informed and the incident logged. If appropriate the School Governor will be informed and actions drawn up to ensure that any breaches are dealt with.

> Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes, by requesting additional access to a specific URL by email to the Headteacher. The Headteacher will review the request and URL, and in conjunction with this policy, approve or deny the request.

> Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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 and anti-bullying 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.

3.6 Parents/carers

Parents/carers 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 (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites, as well as ParentMail notifications from school:

> What are the issues? – UK Safer Internet Centre

> Hot topics – Childnet International

> Parent resource sheet – Childnet International

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 3).

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

> [Relationships education and health education](#) in primary schools

In **Key Stage (KS) 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 (KS) 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.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. EDUCATING PARENTS/CARERS ABOUT ONLINE SAFETY

The school will raise parents/carers' awareness of internet safety via ParentMail and in information via our website. This policy will also be shared with parents/carers.

The school will let parents/carers know:

> What systems the school uses to filter and monitor online use

> What their children are being asked to do online through curriculum maps

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the Designated Safeguarding Lead (DSL) via email school@barncroft.waltham.sch.uk

Concerns or queries about this policy can be raised with 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the anti-bullying 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. Class teachers will discuss cyber-bullying with their class as part of the RHE and computing curriculum.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. 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).

The school also sends information/leaflets on cyber-bullying (via ParentMail) to parents/carers so they 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 as well as seek advice from the Safeguarding in education team (LBWF) and if applicable contact the Local Area Designated Officer (LADO). 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 DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (named DSLs), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

> Poses a risk to staff or pupils, and/or

>

> Is identified in the school rules as a banned item for which a search can be carried out, and/or

 Is evidence in relation to an offence

In all cases the Headteacher will follow DfE's searching, screening and confiscation advice for schools

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

> In all circumstances inform the Headteacher immediately and follow their advice

> Make an assessment of how urgent the search is, and consider the risk to other pupils and staff.

> Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it

> Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

> Cause harm, and/or

> Undermine the safe environment of the school or disrupt teaching, and/or

> Commit an offence

If inappropriate material is found on the device, it is up to the Headteacher/DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, the Headteacher/DSL will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

> They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

> The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or seminude image), they will:

> **Not** view the image

> Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

>

Any searching of pupils will be carried out in line with:

> The DfE's latest guidance on searching, screening and confiscation

> UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Our behaviour policy, anti-bullying policy, child protection policy and any other relevant polices

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

Barn Croft School recognises 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 form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Barn Croft School will treat any use of AI to bully pupils as bullying and deal with in line with our anti-bullying and behaviour policies.

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 in school.

7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. PUPILS USING MOBILE DEVICES IN SCHOOL

Pupils may bring mobile devices into school, in Years 5 and 6 (if they walk home alone) but these must be switched off and stored in the main office until collected at home time. Use of the phones during the school day and onsite before and after school is not permitted.

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 WORK DEVICES OUTSIDE SCHOOL

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

> Keeping the device password-protected – strong passwords with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

> School to ensure that hard drives are encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

Making sure the device locks if left inactive for a period of time

>

- > Not sharing the device among family or friends

- > School to ensure anti-virus and anti-spyware software is installed on devices

- > Keeping devices in a secure place

- > Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Headteacher or school ICT Provider (ROCIT Solutions).

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 our policies e.g. behaviour policy, anti-bullying policy and acceptable use etc. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. All incidents will be logged on My Concern.

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 and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that 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).

By way of this training, all staff will be made aware that:

- > Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

- > Children can abuse their peers online through:

   - o Abusive, harassing and misogynistic messages

   - o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

o   Sharing of abusive images and pornography, to those who don't want to receive such content

> Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse

- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks

- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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

Keeping Children Safe in Education has long asked schools to ensure "appropriate" web filtering and monitoring systems which keep children safe online but do not "overblock".

Since KCSIE 2023, in recognition of the importance of these systems to keeping children safe, the designated safeguarding lead now has lead responsibility for filtering and monitoring. *(See sections 3.1, 3.2 and 3.3 for information re roles and responsibilities of the Headteacher, DSL, and the named governor in respect of filtering and monitoring).*

Schools are asked to follow the new DfE filtering and monitoring standards, which require them to:
- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

As schools get to grips with these new standards, the challenge for DSLs and SLT is to better understand, review and drive the rationale behind decisions in this area. Tech teams and safeguarding teams will need to work much more closely together for this to be possible and technicians will be charged to carry out regular checks and feed back to DSL teams.

ALL STAFF will need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can

submit concerns at any point via the Headteacher, Designated Safeguarding Lead via email or the ICT Support Provider (ROCIT Solutions) via their online support portal. All emails will be reviewed by the Headteacher/DSL and a decision will be made based on all the information given, and any subsequent investigation.

Regular checks and subsequent reviews will take place once processes for monitoring are fine-tuned.

Staff will be reminded of the systems in place and their responsibilities at induction and at the start of the academic year in safeguarding training, as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

Staff will receive training to help them develop a clear understanding of the difference between filtering and monitoring, the meaning of overblocking and other terms, as well as how to get the best out of systems. Guidance videos and flyers to help with this at https://safefiltering.lgfl.net and training will be provided for all staff / safeguarding teams / technical teams as appropriate.

At Barn Croft Primary School:

- web filtering is provided by LGfL on school site and for school devices used in the home
- changes can be made by the Headteacher or DSL
- overall responsibility is held by the DSL - Emma-Jane Kelly
- technical support and advice, setup and configuration are provided by the ICT Support Provider (ROCIT solutions)
- Ongoing checks are made by LGfL to ensure filtering is still active and functioning everywhere. These are evidenced by emails sent directly to nominated the Headteacher, DSL and ICT Support Provider (ROCIT Solutions)
- an annual review is carried out as part of the online safety audit to ensure a whole school approach
- guidance on how the system is 'appropriate' is available at appropriate.lgfl.net
- According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and at may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

At Barn Croft Primary School, we use:

Ipads, chromebooks, laptops and PC devices that are filtered by LGfL webscreen filtering services/SOPHOS anti-virus software and CISCO MERAKI mobile device management, please see link to LGfL's Appropriate Filtering for Education Settings:

https://d1xsi6mgo67kia.cloudfront.net/uploads/2020/01/LGfL-Appropriate-Filtering-Provider-ResponseAugust-2023-LGfL.pdf

The DSL will log behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the DSL/Headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

> Child protection and safeguarding policy

> Behaviour policy

> Anti-bullying policy

> Staff code of conduct

> Staff disciplinary procedures

> Data protection policy and privacy notices

> Complaints procedure

And any other related policies and procedures that the school has.

Appendix 1:

EYFS AND KS1 ACCEPTABLE USE AGREEMENT

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 I am allowed to

2. I **ASK** for help if I'm stuck or not sure; I **TELL** a trusted adult if I'm upset, worried, scared or confused

3. I look out for my **FRIENDS** and tell someone if they need help

4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult

5. I **KNOW** that online people aren't always who they say they are and things I read are not always **TRUE**

6. Anything I do online can be shared and might stay online **FOREVER**

7. I don't keep **SECRETS** 🚫 unless they are a present or nice surprise

8. I don't have to do **DARES OR CHALLENGES** ❌ , even if someone tells me I must.

9. I don't change **CLOTHES** or get undressed in front of a camera

10. I always check before **SHARING** my personal information or other people's stories and photos

11. I am **KIND** and polite to everyone

My trusted adults are:

_____ **at school**

_____ **at home**

_____ **at** _____

FOR PARENTS/CARERS

To find out more about online safety, you can read Barn Croft's full Online Safety Policy (available at www.barncroftprimary.org/policies) You can find support and online safety resources for parents at parentsafe.lgfl.net

KS2 acceptable use agreement

THESE STATEMENTS CAN KEEP ME AND OTHERS SAFE & HAPPY AT SCHOOL AND HOME

1. *I learn online* – I use school internet, devices and logins for school and homework, to learn and have fun. School can see what I am doing to keep me safe, even when at home.

2. *I behave the same way on devices as face to face in the classroom, and so do my teachers* – If I get asked to do anything that I would find strange in school, I will tell another teacher.

3. *I ask permission* – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.

4. *I am creative online* – I don't just use apps, sites and games to look at things other people made or posted; I also get creative to learn or make things, remembering my 'Digital 5 A Day'.

5. *I am a good friend online* – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.

6. *I am not a bully* – I know just calling something fun or banter doesn't stop it maybe hurting someone else. 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.

7. *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!

8. *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 app addons can cost money, so it is important I always check.

9. *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.

10. *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.

11. *If I make a mistake I don't try to hide it but ask for help.*

12. *I communicate and collaborate online* – with people I already know and have met in real life or that a trusted adult knows about.

13. *I know 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.

14. *I never pretend to be someone else online* – it can be upsetting or even dangerous.

15. *I check with a parent/carer before I meet an online friend* the first time; I never go alone.

16. *I don't go live (videos anyone can see) 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.

17. *I don't take photos or videos or people without them knowing or agreeing to it* – and I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.

18. *I keep my body to myself online* – I never get changed or show what's under my clothes when using a device with 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.

19. *I say no online if I need to* – I don't have to do something just because someone 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.

20. *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.

21. *I follow age rules* – 13+ games, apps and films aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.

22. *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.

23. *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).

24. *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, at home and at school.

25. *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 and/or report it.

26. *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.

27. *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, and I know which sites to trust, and how to double check information I come across. If I am not sure I ask a trusted adult.

~~~~~~~~~~~~~~~~~~~~~

I have read and understood this agreement. If I have any questions, I will speak to a trusted

adult: at school that might mean _____

Outside school, my trusted adults are_____

I know I can also get in touch with Childline

Signed: _____

Date: _____

Acceptable Use Policy (AUP) for
STAFF, GOVERNORS, VOLUNTEERS

BACKGROUND

We ask everyone involved in the life of Barn Croft Primary School to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and staff, governors and volunteers are asked to sign it when starting at the school and whenever changes are made. All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy. If you have any questions about this AUP or our approach to online safety, please speak to the Headteacher or DSL.

WHAT AM I AGREEING TO?

1. **(This point for staff and governors):**
   I have read and understood Barn Croft's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay as outlined in the Online Safety Policy.

2. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area.

3. I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher and make them aware of new trends and patterns that I might identify.

4. I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media)

5. I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom.

6. I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment – know that 'it could happen here'!

7. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language

8. I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

9. When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).

10. I will follow policy and best-practice pedagogy for online-safety education, avoiding scaring and other unhelpful prevention methods.

11. I will prepare and check all online sources and classroom resources before using for accuracy and appropriateness. I will flag any concerns about overblocking to the DSL.

12. I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.

13. During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main child protection and safeguarding policy when it comes to behaviour, ways to contact and the relevant systems and bahaviours.

14. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

15. I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE 2023, now led by the DSL. If I discover pupils may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the school to inform regular checks and annual review of these systems.

16. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

17. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the Headteacher.

18. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the code of conduct. If I am ever not sure, I will ask first.

19. I agree to adhere to all provisions of the school's Safeguarding and child Protection policies and Data Protection Policies at all times, whether or not I am on site or using a school device, platform or network.

20. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.

21. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.

22. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.

23. I understand that breach of this AUP and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

To be completed by Emma-Jane Kelly

I approve this user to be allocated credentials for school systems as relevant to their role.

Systems: _____

Additional permissions (e.g. admin) _____

Signature: _____

Name: _____

Role: _____

Date: _____

ONLINE SAFETY TRAINING NEEDS AUDIT

Name of staff member/volunteer:	Date:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

APPENDIX 5: ONLINE SAFETY INCIDENT REPORT LOG

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident