


Beavers Community Primary School Online Safety Policy - 2024/5

Introduction

Key people / dates

<p>Beavers Community Primary School</p> 	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Sarah Smith
	Deputy Designated Safeguarding Leads DSL Team Members	Lucinda Palmer-Dunn Christina Coulston Hannah Hunter Tracey Bunce
	Link governors for safeguarding (including web filtering)	Suresh Dhotre Michelle Davis
	Curriculum leads with relevance to online safeguarding and their role	ICT - Ghazala Dawe Computing - Saira Ahmed PSHE - Shanaj Miah Personal Development (including RSHE) - Lucy Thompson
	Network manager / other technical support	Click on it London
	Date this policy was reviewed and by whom	October 2024 by Headteacher
	Date of next review and by whom	September 2025 by Headteacher

Contents

Introduction	1
Key people / dates	1
Contents	2
Overview	3
Aims	3
Scope	4
Roles and responsibilities	4
Education and curriculum	4
Handling safeguarding concerns and incidents	6
Nudes – sharing nudes and semi-nudes	7
Priority Areas	9
Bullying	9
Child-on-child sexual violence and sexual harassment	9
Misuse of school technology (devices, systems, networks or platforms)	9
Social media incidents	10
Extremism	11
Data protection and cyber security	11
Appropriate filtering and monitoring	11
Messaging/commenting systems (incl. email, learning platforms & more)	13
Authorised systems	13
Behaviour/usage principles of messaging/commenting systems	14
Use of generative AI	14
Online storage or learning platforms	14
School website	14
Digital images and video	15
Social media	16
Our SM presence	16
Staff, pupils' and parents' SM presence	16
Device usage	18
Personal devices	18
Use of school devices	19
Searching and confiscation	19
Appendix 1 – Roles	21
All staff	21

Beavers Community Primary School

Online Safety Policy - 2024/5

Headteacher - Sarah Smith	22
Designated Safeguarding Lead – Sarah Smith	23
Governing Body, led by Online Safety / Safeguarding Link Governors - Suresh Dhotre and Michelle Davis	24
PSHE / RHSE Lead/s – Lucy Thompson and Shanaj Miah	25
Computing Lead – Saira Ahmed	26
Network Manager/other technical support roles – Click on it London	26
Data Protection Officer (DPO) – Gabrielle Hardy	27
Volunteers and contractors (including tutors)	28
Pupils	28
Parents/carers	28
External groups (e.g. those hiring the premises) including parent associations	28
Appendix 2 – Guidance for parents who want to film or photograph school events	29
Appendix 3 – Acceptable Use Policies	39
Appendix 4 – Curriculum information	43

Overview

Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Beavers Community Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:

Beavers Community Primary School

Online Safety Policy - 2024/5

- o for the protection and benefit of the children and young people in their care, and
- o for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
- o for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Scope

This policy applies to all members of the Beavers Community Primary School community (including teaching, supply and support staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Depending on their role, all members of the school community should read the relevant section in Annex A of this document that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions in the annex. All staff have a key role to play in feeding back on potential issues.

Education and curriculum

Despite the risks associated with being online, Beavers Community Primary School recognises the opportunities and benefits of children being online. Technology is a fundamental part of our adult lives and so developing the competencies to understand and use it, are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

Beavers Community Primary School

Online Safety Policy - 2024/5

It is important that schools establish a carefully sequenced curriculum for online safety that develops competencies (as well as knowledge about risks) and builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, [Teaching Online Safety in Schools](#) recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

RSHE guidance also recommends that schools assess teaching to “identify where pupils need extra support or intervention”.

The teaching of online safety features in these particular areas of curriculum delivery:

- Relationships education, relationships and sex education (RSE) and health (also known as RHSE or PSHE)
- Computing

However, as stated previously, it is the role of ALL staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise. Chromebooks are used for online learning platforms, for reading, research and assignments. This supports the children in developing the skills to navigate the digital world safely.

Whenever overseeing the use of technology (devices, the internet, generative AI tools, etc.) in school or setting as homework tasks, all staff should remind/encourage sensible use, monitor what pupils/students are doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation and fake news), access to age-appropriate materials and signposting, and legal issues such as copyright and data law. [saferesources.lgfl.net](#) has regularly updated theme-based resources, materials and signposting for teachers and parents. The use of devices used across the school is monitored (Senso) in order to identify any problematic use.

Beavers Community Primary School

Online Safety Policy - 2024/5

We aim to communicate with parents and carers about how we support pupils with their online safety learning, including what their children are being asked to do online and the sites they will be asked to access.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the safeguarding lead with any concerns (no matter how small these seem) to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom.

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Behaviour Policy (including school sanctions) including Anti-Bullying Policy
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Cyber Security

This school commits to take all reasonable precautions to safeguard pupils online but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding lead as soon as possible on the same day. The reporting member of staff will ensure that a record is made of the concern on CPOMS.

Any concern/allegation about staff misuse is always (similar to any safeguarding concern) referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

Beavers Community Primary School

Online Safety Policy - 2024/5

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service).

We will inform parents/carers of online safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

The school should ensure all online safety reporting procedures are sustainable for any unforeseen periods of closure.

For more information on reporting channels for online safety concerns, please visit reporting.lgfl.net.

The following sub-sections provide detail on managing particular types of concern.

Nudes – sharing nudes and semi-nudes

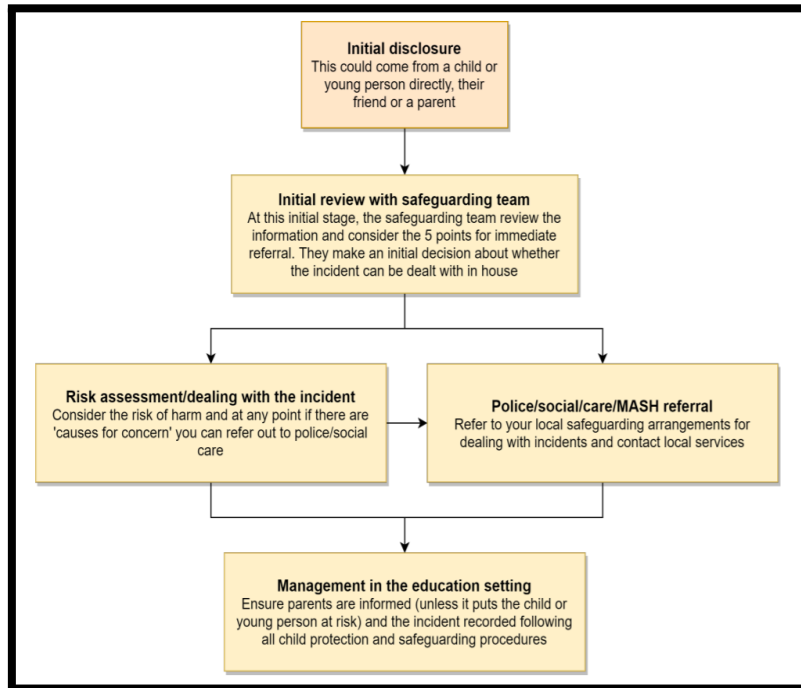
All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as [Sharing nudes and semi-nudes: advice for education settings](#).

There is a one-page overview called [Sharing nudes and semi-nudes: how to respond to an incident](#) for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

It is important that everyone understands that whilst the sharing of nudes involving children is illegal, students should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

The school DSL will use the full guidance document, [Sharing nudes and semi-nudes – advice for educational settings](#) to decide next steps and whether other agencies need to be involved (see flow chart below from the UKCIS guidance) and next steps regarding liaising with parents and supporting pupils.

Beavers Community Primary School Online Safety Policy - 2024/5



The following LGfL document (available at nudes.lgfl.net) may also be helpful for DSLs in making their decision about whether to refer a concern about sharing of nudes:



SAFEGUARDING QUESTION TIME

Q: WHEN SHOULD WE REFER NUDE SHARING?
A: IMMEDIATELY *IF* THE IMAGE/VIDEO:

- involves an adult
- is potentially coerced, blackmailed or groomed or concerns about capacity to consent
- might depict sexual acts unusual for their developmental stage or violent
- involves sexual acts / under 13s
- or the young person is at immediate risk of harm[...], suicidal or self-harming

Text simplified, taken from page 20 of 'Sharing Nudes and Semi-Nudes', UKCIS – search gov.uk

"We recommend DSLs read the entire UKCIS document; there is much more to know than this, and many helpful resources including training, scenarios and further guidance. Note also the one-pager for all staff!"

Beavers Community Primary School

Online Safety Policy - 2024/5

Priority Areas

Bullying

Online bullying (which may also be referred to as cyberbullying), including incidents that take place outside of school should be treated like any other form of bullying and the school bullying policy should be followed, . This includes issues arising from banter.

It is important to be aware that sometimes fights are being filmed, live streamed or shared online and fake profiles are used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Child-on-child sexual violence and sexual harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the guidance in KCSIE. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language. This will be discussed in staff training.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff disciplinary policy/code of conduct/handbook.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that the same applies for any home learning that may take place.

Beavers Community Primary School

Online Safety Policy - 2024/5

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology.

Social media incidents

Social media incidents involving pupils are often safeguarding concerns and should be treated as such and staff should follow the safeguarding policy. Other policies that govern these types of incidents are the school's Acceptable Use Policies/social media policy/online safety.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or disciplinary policy/code of conduct/handbook (for staff). See the social media section later in this document for rules and expectations of behaviour for children and adults in our school community.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community (e.g. parent or visitor), Beavers Community Primary School will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Beavers Community Primary School

Online Safety Policy - 2024/5

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Data protection and cyber security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cyber security policy. It is important to remember that there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cyber Security for Schools and Colleges.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools, 2023*, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2024, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring

The designated safeguarding lead (DSL) has lead responsibility for filtering and monitoring and works closely with Click on it London to implement the DfE filtering and monitoring standards, which require schools 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.

We look to provide 'appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times.

Beavers Community Primary School

Online Safety Policy - 2024/5

We ensure ALL STAFF are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking.

Technical and safeguarding colleagues work together closely to carry out annual reviews and checks, and also to ensure that the school responds to issues and integrates with the curriculum.

We carry out half-termly checks to ensure all systems are in operation, functioning as expected, etc and an annual review as part of an online safety audit of strategy, approach etc.

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

The safeguarding team checks filtering reports and notifications when alerted and takes any necessary action as a result.

According to the DfE standards, “a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and 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 Beavers Community Primary School, we use Senso for monitoring for key words and phrases entered onto a device.

Monitoring alerts are checked daily when alerted by the safeguarding team; teachers in Years 5 and 6 are also alerted to children in their own class so that swift action is taken.

Beavers Community Primary School

Online Safety Policy - 2024/5

Messaging/commenting systems (incl. email, learning platforms & more)

Authorised systems

- Our school does not have the chat or email function enabled for students. They are only able to message on the main Google Classroom dashboard or comment on shared documents. They are taught to do this appropriately.
- Staff at this school use the email system provided by Google for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. We have Class email addresses which can be used to communicate with parents so that our main email addresses are not given out. We use our individual work emails to communicate with external agencies.
- Staff at this school use Tapestry, Google Classroom, emails, text messages, medical tracker to communicate with parents and carers.

Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform or app with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from, or data being uploaded to the wrong account. If this private account is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Beavers Community Primary School

Online Safety Policy - 2024/5

Behaviour/usage principles of messaging/commenting systems

- More detail for all the points below are given in the Social media section of this policy as well as the school's Acceptable Use Policies, Behaviour Policy and Staff Code of Conduct.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.

Use of generative AI

- At Beavers Community Primary School, we acknowledge that generative AI platforms (e.g. ChatGPT or Bard for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread.
- We will talk about the use of these tools with pupils, staff and parents – their practical use as well as their ethical pros and cons
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, undressing apps).

Online storage or learning platforms

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc. At Beavers Community Primary School, this includes Tapestry, Google Classroom and Google drive.

For all these, it is important to consider data protection and cyber security before adopting such a platform or service and at all times when using it.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the

Beavers Community Primary School

Online Safety Policy - 2024/5

content of the website and ensuring compliance with DfE stipulations to the Office Manager.

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited, and material only used with permission. There are many open-access libraries of public-domain images/sounds etc that can be used.

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For social media
- For a specific high-profile image for display or publication
- Learning and management platforms (Tapestry, Edukey, Integris)

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Beavers Community Primary School, members of staff have access to school devices, but may *occasionally* use personal phones to capture photos or videos of pupils. These will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos). Photos are stored on Google drive and in the School and Photo zone in our local drive.

Staff and parents are reminded annually about the importance of not sharing images on social media or otherwise without permission, due to reasons of child protection (e.g.

Beavers Community Primary School

Online Safety Policy - 2024/5

children who are looked after by the local authority may have restrictions in place for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. Our letter is included in the Appendix.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social media

Our SM presence

We manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

The Senior Leadership Team is responsible for managing our Facebook account.

Staff, pupils' and parents' SM presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or

Beavers Community Primary School

Online Safety Policy - 2024/5

which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

The school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the [Digital Family Agreement](#) to help establish shared expectations and the [Top Tips for Parents](#) poster along with relevant items and support available from parentsafe.lgfl.net and introduce the [Children's Commission Digital 5 A Day](#).

Although the school has an official Facebook account, it asks parents/carers not to use these channels, especially not to communicate about their children.

Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

As outlined in the Acceptable Use Policies, pupils/students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs.. In the reverse situation, however, staff must not follow such public student accounts.

Beavers Community Primary School

Online Safety Policy - 2024/5

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital images and video and permission is sought before uploading photographs, videos or any other information about other people. Parents must not covertly film or make recordings of any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous (see nofilming.lgfl.net for more information). The school sometimes uses images/video of children for internal purposes such as recording attainment, but it will only do so publicly if parents have given consent on the relevant form.

Device usage

AUPs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUPs and the sections of this document which impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices

- Pupils/students in Years 5 and 6 are allowed to bring mobile phones in as they develop their independence in travelling to and from school. Phones are handed in to teachers at the start of the day and returned to children before they leave at the end of the day. Children may not use mobile phones during the school day.
- All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the 'Digital images and video' section of this document and the school data protection cyber security policies. Child/staff data should never be downloaded onto a private phone.

Beavers Community Primary School

Online Safety Policy - 2024/5

If a staff member is expecting an important personal call when teaching or otherwise on duty, they may seek permission from SLT to leave their phone on, and receive the call outside of the teaching area providing there is someone to cover.

- Volunteers, contractors, governors should leave their phones in their pockets and on silent. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- Parents are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. Please see the Digital images and video section of this document for more information about filming and photography at school events.

Use of school devices

Staff and pupils are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home. School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct.

Wi-Fi is accessible to staff via the wifi network, for school-related internet use and limited personal use within the framework of the acceptable use policy. All such use is monitored.

School devices for staff are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning and reasonable as well as appropriate personal use within the framework of the acceptable use policy.

All and any usage of devices and/or systems and platforms may be tracked.

Searching and confiscation

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools](#)', the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence

Beavers Community Primary School Online Safety Policy - 2024/5

or bullying. Full details of the school's search procedures are available in the school Behaviour Policy.

Beavers Community Primary School

Online Safety Policy - 2024/5

Appendix 1 – Roles

Please read the relevant roles & responsibilities section from the following pages.

All school staff must read the “All Staff” section as well as any other relevant to specialist roles.

Roles:

- All Staff
- Headteacher/Principal
- Designated Safeguarding Lead
- Governing Body, led by Online Safety / Safeguarding Link Governor
- PSHE / RSHE Lead/s
- Computing Lead
- Subject / aspect leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Pupils
- Parents/carers
- External groups including parent associations

All staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school’s main safeguarding policy, the code of conduct/handbook and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

They must report any concerns, no matter how small, to the designated safeguarding lead as named in the AUP, maintaining an awareness of current online safety issues (see the start of this document for issues in 2024) and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the DfE standards for filtering and monitoring and play their part in feeding back to the DSL about overblocking, gaps in provision or pupils bypassing protections. All staff are also responsible for the physical monitoring of pupils’ online devices during any session/class they are working within.

Beavers Community Primary School

Online Safety Policy - 2024/5

Headteacher - Sarah Smith

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee and support the activities of the designated safeguarding lead team and ensure they work with technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance.
- Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures.
- Ensure ALL governors undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the DfE standards—through regular liaison with technical colleagues and the DSL— in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
- Liaise with the designated safeguarding lead on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised.

Beavers Community Primary School

Online Safety Policy - 2024/5

Designated Safeguarding Lead – Sarah Smith

Key responsibilities (remember the DSL can delegate certain online safety duties but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

- The DSL should “take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).
- Ensure “An effective whole school approach to online safety” as per KCSIE.
- Ensure the school is complying with the DfE’s standards on Filtering and Monitoring.
- As part of this, DSLs will work with technical teams to carry out reviews and checks on filtering and monitoring, to compile the relevant documentation and ensure that safeguarding and technology work together.
- Where online safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible, but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication and that the DSL’s clear overarching responsibility for online safety is not compromised or messaging to pupils confused.
- Ensure ALL staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated.
 - This must include filtering and monitoring and help them to understand their roles.
 - All staff must read KCSIE Part 1 and all those working with children also Annex B – translations are available in 13 community languages at kcsietranslate.lgfl.net (the condensed Annex A can be provided instead to staff who do not directly work with children if this is better)
 - Cascade knowledge of risks and opportunities throughout the organisation.
- Ensure that ALL governors undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated.
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply.

Beavers Community Primary School

Online Safety Policy - 2024/5

- Work with the headteacher, DPO and governors to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding and “undertake Prevent awareness training.”
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others).
- Receive regular updates about online safety issues and legislation, be aware of local and school trends (Andrew Hall newsletter, LGFL newsletter).
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance and beyond, in wider school life.
- Promote an awareness of and commitment to online safety throughout the school community, including parents.
- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).

Governing Body, led by Online Safety / Safeguarding Link Governors - Suresh Dhotre and Michelle Davis

Key responsibilities (quotes are taken from Keeping Children Safe in Education)

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) [Online safety in schools and colleges: Questions from the Governing Board](#) .
- Undergo (and signpost all other governors to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated.
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated.

Beavers Community Primary School

Online Safety Policy - 2024/5

- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Hold strategic reviews with the online safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
- Work with the DPO, DSL and headteacher to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B.
- Ensure that all staff undergo safeguarding and child protection training, including online safety and now also reminders about filtering and monitoring.
- “Ensure that children are taught about safeguarding, including online safety [...] as part of providing a broad and balanced curriculum [...] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology.”

PSHE / RHSE Lead/s – Lucy Thompson and Shanaj Miah

Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from latest trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. “This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils’ lives.”
- Focus on the underpinning knowledge and behaviours outlined in [Teaching Online Safety in Schools](#) in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to “identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress” – [see

Beavers Community Primary School

Online Safety Policy - 2024/5

LGfL's SafeSkills Online Safety Quiz and diagnostic teaching tool at safeskillsinfo.lgfl.net] to complement the computing curriculum,.

- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

Computing Lead – Saira Ahmed

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

Network Manager/other technical support roles – Click on it London

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the safeguarding and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks
- Support the safeguarding and leadership team to carry out an online safety audit as recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the DfE standards.

Beavers Community Primary School

Online Safety Policy - 2024/5

- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact / RSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure filtering and monitoring systems work on new devices and services before releasing them to students and staff.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Work with the leadership team to ensure the school website meets statutory DfE requirements.

Data Protection Officer (DPO) – David Coy, Grow Education Partners Ltd

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cyber security policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools, 2023*, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."
- Note that retention schedules for safeguarding records may be required to be set as 'Very long-term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records. You should check the requirements in your area.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Beavers Community Primary School

Online Safety Policy - 2024/5

Volunteers and contractors (including tutors)

Key responsibilities:

- Read, understand, sign and adhere to an Acceptable Use Policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils

Key responsibilities:

Read, understand, sign and adhere to the pupil acceptable use policy.

Parents/carers

Key responsibilities:

- Read, sign and adhere to the school's parental acceptable use policy (AUP), read the pupil AUP and encourage their children to follow it.
- Read the monthly online safety newsletter; and engage with any workshops offered

External groups (e.g. those hiring the premises) including parent associations

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school.
- Support the school in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

Beavers Community Primary School

Online Safety Policy - 2024/5

Appendix 2 – Guidance for parents who want to film, photograph or stream school events

Dear Parents and Carers,

Guidance for parents who want to film, photograph or stream school events

Our [insert event/trip] is taking place on [insert date], and we would like to take this opportunity to remind you of our policy which applies to ALL video, image or audio capture of staff and pupils, both in and out of school.

This policy applies to sporting events, parents' evenings, plays, assemblies, school trips and any other school event or gathering, whether on school premises or beyond.

We appreciate that families will treasure photographic/video memories of these events, and the general rule is that parents and carers may take photos and videos of the children in their care, for personal use only. There may however, be rare exceptions to this, and we will let you know in advance of particular events where filming etc is not possible. The reason for this will always be for the safety and protection of people in our school community. Thank you for your understanding.

Live streaming, whether public or private, is not permitted and we request that you do not use any streaming platforms or 'live' features (e.g. Instagram/TikTok Live) to stream events/circumstances as they occur. You may be asked to leave the premises or event if this takes place.

When you capture footage or photos of your child, there is a strong possibility that other children will also be visible or audible. For this reason, no such content should be shared publicly (e.g. on any social media).

There are several important reasons for this, outlined below:

- Some children are deemed at risk by local authority safeguarding and child protection authorities; their image must not be put online for their own protection. You are very unlikely to know who these children are. There is the real possibility you could endanger a child by sharing their image in an identifiable context (e.g. where the school is easy to identify and locate).

Beavers Community Primary School

Online Safety Policy - 2024/5

- Explicit consent is needed from parents to comply with data protection legislation. Sharing could potentially incur fines for contravention of data protection rules.
- Some families may object for religious or cultural reasons, or simply for reasons of personal privacy.
- We encourage young people at our school to think about their online reputation and digital footprint: online photos and videos do not simply disappear when we delete them from our accounts. Help us be good adult role models by not oversharing (or providing embarrassment in later life).


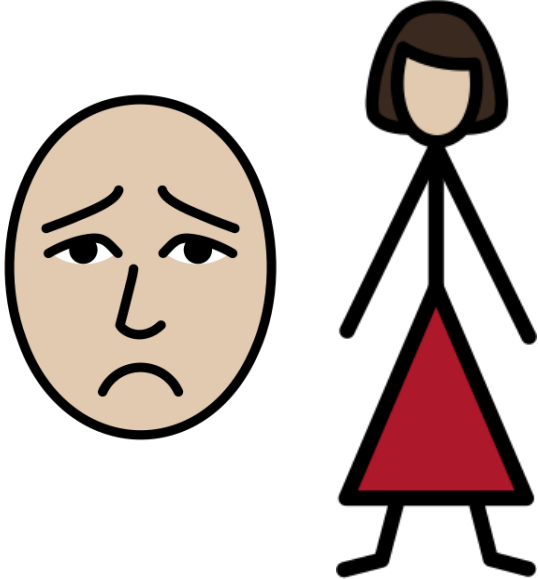
Take a look at the video here to understand about this issue further- nofilming.lgfl.net

Where possible, we will facilitate group shots of pupils whose parents/carers have given appropriate photographic permissions and make these available to you. Equally, and again wherever possible, we will ensure there is time for parents to take photographs of their own children for example by approaching the stage after a performance. The same provisos apply here as stated above.

We want you to enjoy school events and activities with your child, so why not just sit back, enjoy the memories and allow others to do so too? Remember, your child wants to see you looking at them, not at your phone.

Appendix 3 – Acceptable Use Policies



Acceptable Use Policy (AUP) for **EYFS Pupils** Staying safe whilst using technology

<p>I will only use computers or devices when an adult tells me that I can.</p>	
<p>I will tell an adult if I see something that makes me feel sad or scared.</p>	

Beavers Community Primary School Online Safety Policy - 2024/5

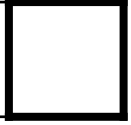
Acceptable Use Policy (AUP) for **KS1 PUPILS**

Class _____

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 or see 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, videos and photos.	

Beavers Community Primary School Online Safety Policy - 2024/5

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



Beavers Community Primary School

Online Safety Policy - 2024/5

Acceptable Use Policy (AUP) for **KS2 PUPILS**

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 devices, apps, sites and games if and when I am allowed to. If not sure, I will ask.
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 may be hurting someone else. I do not post, make or share unkind, hurtful or rude messages/comments, images or videos 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 add-ons 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 don't create artificial images, videos or deepfakes of others without consent. I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.

Beavers Community Primary School Online Safety Policy - 2024/5

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 can 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 say mean things, make fun of anyone or exclude them because they are different. 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, for example \_\_\_\_\_

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

I know I can also get in touch with [Childline](https://www.childline.gov.uk) 0800 1111 or use the worry box at school.

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

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

## Acceptable Use Policy (AUP) for PARENTS

# Beavers Community Primary School

## Online Safety Policy - 2024/5

### Background

The use of technology is an essential part of all of our lives. At Beavers Community Primary School, we take our responsibilities for supporting your child to develop skills in using technology very seriously, and their safety and wellbeing are our utmost priority to us.

We ask all children, young people and adults involved in the life of Beavers Community Primary School to read and sign an Acceptable Use\* Policy (AUP) to outline 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).

Your child has also signed an AUP which can be found in the appendix of the Online Safety Policy. .

We tell your children that they should not behave any differently when they are out of school or using their own device or on a home network. What we tell pupils about behaviour and respect applies to all members of the school community, whether they are at home or school. We seek the support of parents and carers to reinforce this message and help children to behave in a safe way when online:

“Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face.”

### Where can I find out more?

You can read Beavers Community Primary School’s full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding and Child Protection Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to a member of the safeguarding team.

### What am I agreeing to?

1. I understand that Beavers Community Primary School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including through behaviour policies and agreements, physical and technical monitoring, education and support and web filtering.

# Beavers Community Primary School

## Online Safety Policy - 2024/5

3. School network protections will be superior to most home filtering. However, please note that accessing the internet always involves an element of risk and the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies. Schools are asked not to overblock or provide an experience which is so locked down as to block educational content or not train pupils for life in an online world.
4. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school is subject to filtering and monitoring. More detail of this can be found in our online safety policy.
5. I understand and will help my child to use any devices at home in the same manner as when in school, including during any remote learning periods.
6. I understand that my child might be contacted online on Google Classroom by members of school staff and only about their learning, wellbeing or behaviour. If they are contacted by someone else or staff ask them to use a different app to chat, they will tell another teacher.
7. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
8. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age (for nearly every social media platform, this means under 13).
9. When I visit the school premises, I will keep any online technology in my pocket wherever possible.
10. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous (see [nofilming.lgfl.net](https://nofilming.lgfl.net) for more information). The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given consent.
11. I will not covertly film or make recordings of any interactions with pupils or adults in school.
12. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety and refer to [parentsafe.lgfl.net](https://parentsafe.lgfl.net) for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screentime and relevant topics from

# Beavers Community Primary School Online Safety Policy - 2024/5

bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc.

13. I understand that my child needs a safe and appropriate place to do home learning, whether for homework or during times of school closure. When on any video calls with school, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
14. If my child has online tuition, I will refer to the [Online Tutors – Keeping children Safe poster](#) and undertake necessary checks where I have arranged this privately, ensuring they are registered/safe and reliable, and for any tuition to remain in the room where possible, ensuring my child knows that tutors should not arrange new sessions or online chats directly with them.
15. I understand that whilst home networks are much less secure than school ones, I can apply safety settings to my home internet and to various devices, operating systems, consoles, apps and games. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content. Find out more at [parentsafe.lgfl.net](https://parentsafe.lgfl.net)
16. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my child, and refer to the principles of the Digital 5 A Day: [childrenscommissioner.gov.uk/our-work/digital/5-a-day/](https://childrenscommissioner.gov.uk/our-work/digital/5-a-day/)
17. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
18. I can find out more about online safety at Beavers Community Primary School by reading the full Online Safety Policy. I can talk to the class teacher if I have any concerns about my child/ren’s use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

~~~~~

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of:

Date: _____

Beavers Community Primary School

Online Safety Policy - 2024/5

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

Background

We ask everyone involved in the life of Beavers Community 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 will be 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 a member of the Safeguarding team.

What am I agreeing to?

1. I have read and understood Beavers Community Primary School'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. I have noted the section in our online safety policy which describes trends over the past year at a national level and in this school.
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/Principal (if by an adult) and make them aware of new trends and patterns that I 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.

Beavers Community Primary School

Online Safety Policy - 2024/5

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 with pupils 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 check with the Safeguarding team if I want to use any new platform or app that has not already been approved by the school, to ensure this is quality assured.
11. I will follow best-practice pedagogy for online safety education, avoiding scaring and other unhelpful prevention methods.
12. I will prepare and check all online sources and classroom resources before using them, for accuracy and appropriateness. I will flag any concerns about “overblocking” to the DSL.
13. 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.
14. I will physically monitor pupils using online devices in the classroom to ensure appropriate and safe use.
15. 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 behaviours.
16. 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.
17. 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. If I discover pupils or adults 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.

Beavers Community Primary School

Online Safety Policy - 2024/5

18. 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.
19. 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.
20. If I already have a personal relationship to a pupil or their family, I will inform the DSL/Headteacher of this as soon as possible.
21. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am ever not sure, I will ask first.
22. I will not use any new technology or download any apps without agreement from the Safeguarding team/Network manager.
23. I will not use a mobile hotspot to provide internet to any device I use in school.
24. I agree to adhere to all provisions of the school's Cybersecurity and Data Protection Policies at all times, whether or not I am on site or using a school device, platform or network.
25. 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.
26. 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. I understand that any breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.
27. I will only use gen AI platforms that have been authorised for use, and I will ensure that any use of these platforms is transparent, appropriate, legal and ethical. I will also ensure that I abide by all data protection legislation in relation to using these platforms.

Beavers Community Primary School Online Safety Policy - 2024/5

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: _____

Beavers Community Primary School

Online Safety Policy - 2024/5

Appendix 4 - Curriculum information

Year group	SCARF PSHE unit	Learning outcomes	DfE Relationships Education and Health Education statutory requirements (see below)	NC links Teach Computing
R	Keeping safe online	Share ideas about activities that are safe to do on electronic devices. What to do and who to talk to if they feel unsafe online.	Online relationships - 3 Being safe - 2, 5, 6	The technology strand has been removed from the revised EYFS Framework. However, discussions around computing and understanding e-safety are on-going. Smartie the penguin - to be added
1	Sharing pictures	Link to <i>Thinkuknow</i> (NCA-CEOP) resources, Jessie and Friends Episode 2: Sharing Pictures	Respectful relationships - 8 Online relationships - 1, 2, 3, 4, 5 Being safe - 1, 2, 6 Internet safety and harms - 1, 3, 5, 7	Computing KS1 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. Computing Systems Technology around us
2	Playing games	Link to <i>Thinkuknow</i> (NCA-CEOP) resources, Jessie and Friends Episode 3: Playing Games	Online relationships - 1, 2, 3, 4, 5 Being safe - 1, 2, 6 Internet safety and harms - 1, 2, 3, 5, 7	Computing KS1 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. Computing Systems Technology around us

Beavers Community Primary School

Online Safety Policy - 2024/5

3	Super Searcher	Evaluate the validity of statements relating to online safety; Recognise potential risks associated with browsing online; Give examples of strategies for safe browsing online.	Online relationships - 3, 4, 5 Internet safety and harms - 1, 3, 6	Starters All year groups begin their computing lesson with a true or false statement or a 'What would you do if...?' relating to online safety.
3	None of your business!	Know that our body can often give us a sign when something doesn't feel right; to trust these signs and talk to a trusted adult if this happens; Recognise and describe appropriate behaviour online as well as offline; Identify what constitutes personal information and when it is not appropriate or safe to share this; Understand and explain how to get help in a situation where requests for images or information of themselves or others occurs	Respectful relationships - 8 Online relationships - 1, 2, 3, 4, 5 Being safe - 1, 4, 5 Mental wellbeing - 3, 4 Internet safety and harms - 3, 5, 7	Computing KS2 Use technology safely, respectfully and responsibly. Recognise acceptable/unacceptable behaviour. Identify a range of ways to report concerns about content and contact. Digital Media Stop Frame Animation
4	Traffic lights (OPTIONAL)	Identify strategies for keeping personal information safe online; Describe safe behaviours when using communication technology.	Online relationships - 3, 5 Internet safety and harms - 3	Computing KS2 Use technology safely, respectfully and responsibly. Recognise acceptable/unacceptable behaviour. Identify a range of ways to report concerns about content and contact. Digital Media Audio Production
4	Picture wise	Identify images that are safe/unsafe to share online; Know and explain strategies for safe online sharing; Understand and explain the implications of sharing images online without consent.	Online relationships - 3, 5 Internet safety and harms - 3, 5,	Computing KS2 Use technology safely, respectfully and responsibly. Recognise acceptable/unacceptable behaviour. Identify a range of ways to report concerns about content and contact.

Beavers Community Primary School

Online Safety Policy - 2024/5

5	Spot bullying	<p>Demonstrate strategies to deal with both face-to-face and online bullying</p> <p>Demonstrate strategies and skills for supporting others who are bullied;</p> <p>Describe the difference between online and face-to-face bullying.</p>	<p>Being safe - 1. 4. 5</p> <p>Mental wellbeing - 3. 4</p> <p>Respectful relationships - 8</p>	<p>Computing KS2</p> <p>Understand computer networks, including the internet; how they can provide multiple services, such as the World Wide Web, and the opportunities they offer for communication and collaboration</p> <p>Digital Media Video Production</p>
5	Communication (OPTIO NAL)	<p>Understand that online communication can be misinterpreted;</p> <p>Accept that responsible and respectful behaviour is necessary when interacting with others online as well as face-to-face.</p>	<p>Being safe - 1. 4. 5</p> <p>Mental wellbeing - 3. 4</p>	<p>Computing KS2</p> <p>Understand computer networks, including the internet; how they can provide multiple services, such as the World Wide Web, and the opportunities they offer for communication and collaboration</p>
5	Play, like, share	<p>Consider what information is safe/unsafe to share offline and online, and reflect on the consequences of not keeping personal information private;</p> <p>Recognise that people aren't always who they appear to be online and explain risks of being friends online with a person they have not met face-to-face;</p> <p>Know how to protect personal information online;</p> <p>Recognise disrespectful behaviour online and know how to respond to it.</p>	<p>Online relationships - 1. 2. 3. 4. 5</p> <p>Being safe - 1. 4. 5</p> <p>Mental wellbeing - 3. 4</p> <p>Internet safety and harms - 3. 5. 7</p>	<p>Computing KS2</p> <p>Use technology safely, respectfully and responsibly. Recognise acceptable/unacceptable behaviour. Identify a range of ways to report concerns about content and contact.</p>
5	Is it true?	<p>Understand that the information we see online, either text or images, is not always true or accurate;</p> <p>Recognise that some people post things online about themselves that aren't true, sometimes this is so that people will like them;</p> <p>Understand and explain the difference between sex, gender identity, gender expression and</p>	<p>Being safe - 1. 4. 5</p> <p>Internet safety and harms - 3. 5. 7</p>	<p>Computing KS2</p> <p>Use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs</p>

Beavers Community Primary School

Online Safety Policy - 2024/5

		sexual orientation.		
6	To share or not to share?	Know that it is illegal to create and share sexual images of children under 18 years old; Explore the risks of sharing photos and films of themselves with other people directly or online; Know how to keep their information private online.	Being safe - 1, 4, 5 Online relationships - 3, 5 Internet safety and harms - 3 Mental wellbeing - 3, 4	<u>Computing KS2</u> Use technology safely, respectfully and responsibly. Recognise acceptable/unacceptable behaviour. Identify a range of ways to report concerns about content and contact. Digital Media Web Creation
6	Pressure online	Understand the risks of sharing images online and how these are hard to control, once shared; Understand that people can feel pressured to behave in a certain way because of the influence of the peer group; Understand the norms of risk-taking behaviour and that these are usually lower than people believe them to be.	Online relationships - 3, 5 Internet safety and harms - 3 Mental wellbeing - 3, 4 Respectful relationships - 8	<u>Computing KS2</u> Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
6	Fakebook friends	Know the legal age (and reason behind these) for having a social media account; Understand why people don't tell the truth and often post only the good bits about themselves, online; Recognise that people's lives are much more balanced in real life, with positives and negatives.	Internet safety and harms - 3 Being safe - 1, 4, 5 Mental wellbeing - 3, 4 Respectful relationships - 8 Caring friendships - 2	<u>Computing KS2</u> Understand computer networks, including the internet; how they can provide multiple services, such as the World Wide Web, and the opportunities they offer for communication and collaboration
6	It's a puzzle (OPTIONAL)	Identify strategies for keeping personal information safe online; Describe safe and respectful behaviours when using communication technology.	Internet safety and harms - 3	<u>Computing KS2</u>
6	Think before you click	Accept that responsible and respectful behaviour is necessary when interacting with others online and face-to-face; Understand and describe the ease with which something posted online can spread.	Internet safety and harms - 3 Mental wellbeing - 3, 4 Respectful relationships - 8	<u>Computing KS2</u> Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content

Beavers Community Primary School

Online Safety Policy - 2024/5

DfE Statutory Guidance Categories: Relationships Education (Primary)

By the end of primary school pupils should know:

<p>Families and people who care for me (FPC)</p>	<ol style="list-style-type: none"> 1. that families are important for children growing up because they can give love, security and stability. 2. the characteristics of healthy family life, commitment to each other, including in times of difficulty, protection and care for children and other family members, the importance of spending time together and sharing each other's lives. 3. that others' families, either in school or in the wider world, sometimes look different from their family, but that they should respect those differences and know that other children's families are also characterised by love and care. 4. that stable, caring relationships, which may be of different types, are at the heart of happy families, and are important for children's security as they grow up. 5. that marriage represents a formal and legally recognised commitment of two people to each other which is intended to be lifelong. 6. how to recognise if family relationships are making them feel unhappy or unsafe, and how to seek help or advice from others if needed.
<p>Caring friendships (CF)</p>	<ol style="list-style-type: none"> 1. how important friendships are in making us feel happy and secure, and how people choose and make friends. 2. the characteristics of friendships, including mutual respect, truthfulness, trustworthiness, loyalty, kindness, generosity, trust, sharing interests and experiences and support with problems and difficulties. 3. that healthy friendships are positive and welcoming towards others, and do not make others feel lonely or excluded. 4. that most friendships have ups and downs, and that these can often be worked through so that the friendship is repaired or even strengthened, and that resorting to violence is never right. 5. how to recognise who to trust and who not to trust, how to judge when a friendship is making them feel unhappy or uncomfortable, managing conflict, how to manage these situations and how to seek help or advice from others, if needed.
<p>Respectful relationships (RR)</p>	<ol style="list-style-type: none"> 1. importance of respecting others, even when they are very different from them (for example, physically, in character, personality or backgrounds), or make different choices or have different preferences or beliefs. 2. practical steps they can take in a range of different contexts to improve or support respectful relationships. 3. the conventions of courtesy and manners. 4. the importance of self-respect and how this links to their own happiness. 5. that in school and in wider society they can expect to be treated with respect by others, and that in turn they should show due respect to others, including those in positions of authority. 6. about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help. 7. what a stereotype is, and how stereotypes can be unfair, negative or destructive. 8. the importance of permission-seeking and giving in relationships with friends, peers and adults.
<p>Online relationships (OR)</p>	<ol style="list-style-type: none"> 1. that people sometimes behave differently online, including by pretending to be someone they are not. 2. 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. 3. the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them. 4. how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met. 5. how information and data is shared and used online.
<p>Being safe (BS)</p>	<ol style="list-style-type: none"> 1. what sorts of boundaries are appropriate in friendships with peers and others (including in a digital context). 2. about the concept of privacy and the implications of it for both children and adults; including that it is not always right to keep secrets if they relate to being safe. 3. that each person's body belongs to them, and the differences between appropriate and inappropriate or unsafe physical, and other, contact. 4. how to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Beavers Community Primary School

Online Safety Policy - 2024/5

	<ol style="list-style-type: none"> 5. how to recognise and report feelings of being unsafe or feeling bad about any adult. 6. how to ask for advice or help for themselves or others, and to keep trying until they are heard, 7. how to report concerns or abuse, and the vocabulary and confidence needed to do so. 8. where to get advice e.g. family, school and/or other sources.
Mental wellbeing (MW)	<ol style="list-style-type: none"> 1. that mental wellbeing is a normal part of daily life, in the same way as physical health. 2. that there is a normal range of emotions (e.g. happiness, sadness, anger, fear, surprise, nervousness) and scale of emotions that all humans experience in relation to different experiences and situations. 3. how to recognise and talk about their emotions, including having a varied vocabulary of words to use when talking about their own and others' feelings. 4. how to judge whether what they are feeling and how they are behaving is appropriate and proportionate. 5. the benefits of physical exercise, time outdoors, community participation, voluntary and service-based activity on mental wellbeing and happiness. 6. simple self-care techniques, including the importance of rest, time spent with friends and family and the benefits of hobbies and interests. 7. isolation and loneliness can affect children and that it is very important for children to discuss their feelings with an adult and seek support. 8. that bullying (including cyberbullying) has a negative and often lasting impact on mental wellbeing. 9. where and how to seek support (including recognising the triggers for seeking support), including whom in school they should speak to if they are worried about their own or someone else's mental wellbeing or ability to control their emotions (including issues arising online). 10. it is common for people to experience mental ill health. For many people who do, the problems can be resolved if the right support is made available, especially if accessed early enough.
Internet safety and harms (ISH)	<ol style="list-style-type: none"> 1. that for most people the internet is an integral part of life and has many benefits. 2. about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing. 3. how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private. 4. why social media, some computer games and online gaming, for example, are age restricted. 5. that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health. 6. how to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted. 7. where and how to report concerns and get support with issues online.
Physical health and fitness (PHF)	<ol style="list-style-type: none"> 1. the characteristics and mental and physical benefits of an active lifestyle. 2. the importance of building regular exercise into daily and weekly routines and how to achieve this; for example walking or cycling to school, a daily active mile or other forms of regular, vigorous exercise. 3. the risks associated with an inactive lifestyle (including obesity). 4. how and when to seek support including which adults to speak to in school if they are worried about their health.
Healthy eating (HE)	<ol style="list-style-type: none"> 1. what constitutes a healthy diet (including understanding calories and other nutritional content). 2. the principles of planning and preparing a range of healthy meals. 3. the characteristics of a poor diet and risks associated with unhealthy eating (including, for example, obesity and tooth decay) and other behaviours (e.g. the impact of alcohol on diet or health).
Drugs, alcohol and tobacco (DAT)	<ol style="list-style-type: none"> 1. the facts about legal and illegal harmful substances and associated risks, including smoking, alcohol use and drug-taking.
Health and prevention (HP)	<ol style="list-style-type: none"> 1. how to recognise early signs of physical illness, such as weight loss, or unexplained changes to the body. 2. about safe and unsafe exposure to the sun, and how to reduce the risk of sun damage, including skin cancer. 3. the importance of sufficient good quality sleep for good health and that a lack of sleep can affect weight, mood and ability to learn. 4. about dental health and the benefits of good oral hygiene and dental flossing, including regular check-ups at the dentist. 5. about personal hygiene and germs including bacteria, viruses, how they are spread and treated, and the importance of hand washing. 6. the facts and science relating to allergies, immunisation and vaccination.

Beavers Community Primary School Online Safety Policy - 2024/5

Basic first aid (BFA)	<ol style="list-style-type: none">1. how to make a clear and efficient call to emergency services if necessary.2. concepts of basic first-aid, for example dealing with common injuries, including head injuries.
Changing adolescent body (CAB)	<ol style="list-style-type: none">1. key facts about puberty and the changing adolescent body, particularly from age 9 through to age 11, including physical and emotional changes.2. about menstrual wellbeing including the key facts about the menstrual cycle.