Stonebow

Online Safety and Acceptable Use Policy 2022-2023

Reviewed by:	Head Teacher, ICT Manager and DSLs
Approved by:	Full Governing Body
Signature of Chair of Governors:	
Status & review cycle	Statutory Annual
Date approved:	Autumn 2022
Review date:	Autumn 2025

Contents

1. Aims

At Stonebow Primary School we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

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

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

3. Roles and responsibilities

3.1 The Governing body

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

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

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incident
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged on My Concern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs which is completed annually by all staff.)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

  This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

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

This list is not intended to be exhaustive.

3.5 All staff, Governors and volunteers

All staff, Governors and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

3.7 Visitors and members of the community

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

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the computing and PSHE (SCARF) curriculum:

From September 2020 **all** schools will have to teach:

- Relationships education and health education in primary schools

This new requirement includes aspects about online safety.

Key Stage 1 pupils will be taught to:

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

Key Stage 2 pupils will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour

- Identify a range of ways to report concerns about content and contact

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

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

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

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

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

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL.

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

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

In our school, we deal very seriously with any kind of bullying. This is regardless of whether or not the incidents have happened in or outside of school, online or offline.

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

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

As appropriate, the school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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

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

6.3 Examining electronic devices

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

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

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

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

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police (staff may also confiscate the device for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element)

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

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

7. Acceptable use of the internet in school

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

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

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

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

8. Pupils using mobile devices in school

Pupils who walk to and from school by themselves, may bring mobile devices into school, but are not permitted to use them during:

- Lessons

- Break times
- Clubs before or after school, or any other activities organised by the school

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

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

9. Staff using work devices outside school

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

Staff must ensure that their work device is secure and password-protected (with a combination of upper and lower case letters, numbers and special characters), and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

Staff must ensure that they lock their computer when leaving it unattended.

Where personal data has to be sent by email, this must be done via a secure method.

Staff must not download or transfer any restricted or prohibited types of school data to their own personal devices for example via e-mail attachments, or store any such restricted or prohibited types of school data on the device.

USB devices/hard drives should not be used, other than to scan documents on the Riso when they are too large to email.

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

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

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

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

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

11. Training

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

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

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

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

- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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

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

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

All staff log behaviour and safeguarding issues related to online safety. A report can be submitted on My Concern.

This policy will be reviewed annually by the Head Teacher, DSLs and the ICT Manager. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- PSHE Policy
- Teaching online Safety in Schools
- National Curriculum Computing program of study.

Appendix 1: Acceptable Use Agreements

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:______________________

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher/lsa
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

Year 5 and 6 only: If I am in Y5 or Y6 and walk to school alone and I bring a personal mobile phone, I will switch it off when I arrive on site and hand it into the school office. I know that I am responsible for the phone and that if it is lost or broken, the school cannot take any responsibility.

I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school’s ICT systems and internet responsibly.

Parent/carer agreement: I agree that my child can use the school’s ICT systems and internet in line with this policy. I agree to the conditions set out above for pupils using the school’s ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Year 5 and 6 only: I understand that if my child brings a personal mobile phone because they are traveling to school unaccompanied, they must turn this off when entering the school site and hand it into the school office. I understand that mobile phones brought into school will be done at my own risk and that the school will not take any responsibility for any loss or damage.

Parent/Carer Signature____________________________________

Pupil Acceptable Use Agreement KS1

Teachers will show pupils how to use the computers safely.

All pupils must follow the rules of this agreement when using computers at home and in school.

Pupils that do not follow these rules may find:

- They are not allowed to use the computers
- They can only use the computers if they are more closely watched.

Computing Rules

- I will only use polite language when using the devices.
- I must not write anything that might: upset someone or give the school a bad name.
- I know that my teacher will regularly check what I have done on the school devices.
- I know that if my teacher thinks I may have been breaking the rules they will check on how I have used the devices before.
- I must not tell my username and passwords to anyone else but my parents.
- I must never use other people’s passwords or devices left logged in by them.
- If I think someone has learned my password, then I will tell the teacher.
- I must log off after I have finished with my device.
- I know that email is not guaranteed to be private. I must not send unnamed emails.

- I must not use the devices in any way that stops other people using them.
- I will report any websites that make me feel uncomfortable to my teacher or a member of staff.
- I will tell my teacher or another member of staff straight away if I am sent any messages that make me feel uncomfortable.
- If I find something that I think I should not be able to see, I must tell my teacher straight away and not show it to other pupils.

UNACCEPTABLE USE

Examples of unacceptable use include, but are not limited to:

- Using a computer with another person's username and password.
- Creating or sending on the internet any messages that might upset other people.
- Looking at, or changing work that belongs to other people.
- Wasting time or resources on school computers.

PUPIL AGREEMENT

I agree to follow the rules for staying safe online at home and at school.

I will use the internet in a sensible way and follow the rules explained by my teacher.

I will tell an adult if anyone is not using the computers sensibly or safely.

I also agree to tell my teacher or another member of staff if I see anything online that make me feel unhappy or uncomfortable.

If I do not follow the rules, I understand that this may mean I might not be able to use the computers.

Pupil Name__________________________

Stonebow

Pupil Acceptable Use Agreement KS2

Teachers will show pupils how to use the computers safely.

All pupils must follow the rules of this agreement when using computers at home and in school.

Pupils that do not follow these rules may find:

- They are not allowed to use the computers
- They can only use the computers if they are more closely watched.

Computing Rules

- I will only use polite language when using the devices.
- I must not write anything that might: upset someone or give the school a bad name.
- I know that my teachers will regularly check what I have done on the school devices.
- I know that if my teacher thinks I may have been breaking the rules they will check on how I have used the devices before.
- I must not tell my username and passwords to anyone else but my teacher or parents.
- I must never use other people's passwords or devices left logged in by them.
- If I think someone has learned my password, then I will tell the teacher.
- I must log off after I have finished with my device.
- I know that email is not guaranteed to be private. I must not send unnamed emails.
- I must not use the devices in any way that stops other people using them.
- I will report any websites that make me feel uncomfortable to my teacher or a member of staff.

- I will tell my teacher or another member of staff straight away if I am sent any messages that make me feel uncomfortable.
- If I find something that I think I should not be able to see, I must tell my teacher straight away and not show it to other pupils.

UNACCEPTABLE USE

Examples of unacceptable use include, but are not limited to:

- Using a device with another person's username and password.
- Creating or sending on the internet any messages that might upset other people.
- Looking at, or changing work that belongs to other people.
- Wasting time or resources on school devices.

PUPIL AGREEMENT

I agree to follow the rules when using the school devices. I will use the network in a sensible way and follow the rules explained by my teacher.

I agree to report anyone not using the devices sensibly to my teacher.

I also agree to tell my teacher or another member of staff if I see any websites that make me feel unhappy or uncomfortable.

If I do not follow the rules, I understand that this may mean I might not be able to use the school device.

Pupil Name_________________________

Appendix 2: Acceptable Use Agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature

Use them in any way which could harm the school's reputation

Access social networking sites or chat rooms

Use any improper language when communicating online, including in emails or other messaging services

Install any unauthorised software

Share my password with others or log in to the school's network using someone else's details

Use any USB devices

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are stored securely at all times.

I will ensure that work devices are shut down when in transit and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will not leave a laptop or any personal data in a car at any time.

I will use a unique, strong password to protect my email account.

I will use my school email account exclusively for school business.

I will manage my email account in accordance with the school Information Management Policy. I will not use my email account for storage.

I will not send personal data via email.

I will not download or transfer any restricted or prohibited types of school data to my own personal device for example via e-mail attachments, or store any such restricted or prohibited types of school data on the device.

I will manage the data I am responsible for in accordance with the school Data Protection Policy and GDPR rules.

I will not send unsecured personal data by email.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will record this on My Concern.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I will ensure professional boundaries are maintained with pupils at all times.

I will not invite any pupils onto social media sites, or accept requests from them to join sites.

Appendix 3 Google Classroom

Key Stage 2 Acceptable use of the Google Classroom Stream information, protocols and guidance.

1) The Google Classroom is an online platform for learning, maintained by Stonebow Primary school and contributed to by students and teachers, including support staff.
2) The Google Classroom Stream is a live social platform for the sharing of educational ideas directly related to the curriculum.
3) It is monitored by Google and our Internet filtering system for foul language and inappropriate links, photographic or video content, but no system is infallible. So constant vigilance is the order of the day. This is well monitored in the classroom environment; however, the stream is accessible from home.
4) Personal, social communication is not allowed or the posting of photos or content unrelated to the curriculum.
5) Examples of appropriate content: Photographs including selfies of pupil sharing homework they are proud of; Photographs or videos of pupils engaging in reading aloud, recital of poetry, sporting activity, educational games, musical performances, D&T construction/manufacture or similar.
6) Examples of inappropriate content: Photographs of: Family gatherings or celebrations, family holidays or friend sleepovers, gifts received for birthdays or celebrations and any other photograph or video unrelated to the learning curriculum at Stonebow Primary School.
7) The school's behaviour policy applies to the Google Classroom world as well as the offline world: Words designed deliberately to make someone feel bad about themselves or foul language will attract a consequence in line with the behaviour policy.
8) Electronic communication and Internet learning is revolutionising how children learn and grow and is here to stay, however we need to be vigilant to ensure that it is a power for good and not a place for negative and hurtful communication to get a foothold so early in our children's development