ONLINE SAFETY POLICY

Approved by Gledhow Primary School Governing Body – May 2026

To be reviewed – May 2027

GLEDHOW PRIMARY SCHOOL

1. Aims

Our school aims to:

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

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

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

2. The 4 key categories of risk

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

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

3. Roles and responsibilities

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will ensure Online Safety is discussed and monitored regularly

All governors will:

* Ensure that they have read and understand this policy

* 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

The Headteacher will:

* Ensure that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (DSL) and deputies will:

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

* Work with the headteacher, Online Safety Co-Ordinator (Louise Evans) and other staff, as necessary, to address any online safety issues or incidents

* Manage all online safety issues and incidents in line with the school Safeguarding and Child Protection policy

* Update and deliver staff training on online safety

* Liaise with other agencies and/or external services if necessary

* Provide regular reports on online safety in school to the headteacher and/or governing board.

This list is not intended to be exhaustive.

The IT Manager will:

*Liaise with internet provider(s) who provide our firewall to ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

* Ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly through liaison with our Schools ICT IT Technician.

* Ensure the school network is kept secure through only the appropriate people having access to it.

This list is not intended to be exhaustive.

The Computing lead will:

* Lead teaching and learning of a robust Computing Curriculum, which educates children on being safe online.

All staff and volunteers will:

* Confirm they have read and understood this policy and will implement this policy consistently

* Ensure that any online safety incidents are logged and dealt with appropriately in line with this policy

* Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintain an attitude of 'it could happen here'

* Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use below:

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

• Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
• 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, or connect unauthorised hardware or devices to the school's network
• Share my password with others or log in to the school's network using someone else's details
• Take photographs of pupils without checking with teachers first
• Share confidential information about the school, its pupils or staff, or other members of the community
• Access, modify or share data I'm not authorised to access, modify or share
• Promote private businesses, unless that business is directly related to the school
• Use a personal mobile phone in areas which children access

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 and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

This list is not intended to be exhaustive.

Parents/Carers are expected to:

* Notify a member of staff or the headteacher of any concerns or queries regarding this policy

* Support school in ensuring their child has understood and agreed to acceptable use of the school's ICT systems and internet.

Pupils are expected to:

***** Adhere to the below acceptable use agreements

EYFS and KS1
• Only use websites that a teacher or adult has told me or allowed me to use • Tell my teacher immediately if: o I click on a website by mistake o I receive messages from people I don't know o I find anything that may upset or harm me or my friends • Use school computers and devices for school work only • Be kind to others and not upset or be rude to them • Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly • Only use the username and password I have been given • Try my hardest to remember my username and password • Never share my password with anyone, including my friends. • Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer • Save my work on the school network • Check with my teacher before I print anything • Log off or shut down a computer when I have finished using it
KS2
• Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it I will not: • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate

• Log in to the school's network using someone else's details
• Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:
• I will hand it into the teacher at the start of the day
• I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

4. Online Safety Curriculum

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

In Key Stage 1, pupils will be taught to:

* Use technology safely and respectfully, keeping personal information private

* Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

* Use technology safely, respectfully and responsibly

* Recognise acceptable and unacceptable behaviour

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

By the end of primary school, pupils will know:

* That people sometimes behave differently online, including by pretending to be someone they are not

* That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

* The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

* How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

* How information and data is shared and used online

* What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

* How to respond safely and appropriately to adults they may encounter (in all contexts, including online)

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

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

5. Support for parents on Online Safety

The school will raise parents' awareness of internet safety in letters, online posts and on the school website. If parents have any queries or concerns in relation to online safety, these should be raised to Class Teachers or Designated Safeguarding Leads. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-Bullying

Cyber-bullying is bullying that takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

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. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. The school also sends information 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 Positive Behaviour and Anti-Bullying policies. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police and or Children's Social Work Services as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to adhere to acceptable use of the school's ICT systems and the internet. 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 filter the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. Pupil's use of the internet is monitored through SENSO internet safety management software.

8. Pupils and Parents Mobile Devices in school

Pupils in Year 5 and 6 who travel to or from school independently are allowed to bring mobile devices/Smart Watches into school. Pupils are not permitted to use them during the school day. All mobile devices and technology with photo or messaging functions must be handed to an adult at the beginning of the day to be stored in a locked drawer or cupboard until the end of the school day, when they will be returned. Pupils are not allowed to use phone cameras/apps in school. Children in Pre-school – Year 4 are not permitted to bring or wear Smart Watches to school. Children who do not adhere to this will be dealt with appropriately in line with the school behaviour policy.

Parents are requested not to use mobile devices whilst on site, including playgrounds.

9. Staff using work devices

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

* Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

* Not using external storage devices like USB drives in the device.

* Enabling 2 factor authentication on emails when using the device outside of school premises.

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

* Not sharing the device among family or friends.

* Ensuring any anti-virus and anti-spyware software installed by the technician is not altered and is kept up to date.

* Keeping operating systems up to date by always installing the latest updates; handing the device back to the technician for annual updates when requested; seeking advice from the technician if prompted to install anything that appears suspicious.

*Not installing any new applications or software themselves; asking the technician to support with this.

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

* Work devices must be used solely for work activities. This is monitored using SENSO online safety management software.

*Staff members all follow the principles shared in the annual NCSC cyber security training when using work devices.

10. 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. Annual cyber security training using NCSC materials will be delivered.

All staff will access refresher Child Protection training every three years. In addition to this, staff will receive regular refreshing training (for example through emails, e-bulletins and staff CPD and briefings).

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

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable.

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

11. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety, including any alerts raised by SENSO internet safety management software. An incident report can be found on CPOMs. These logs contain the following information:

- Where the incident took place
- Description of the incident
- Action taken

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

12. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1

EYFS and Key Stage One Acceptable Use Agreement

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
o I click on a website by mistake
o I receive messages from people I don't know
o I find anything that may upset or harm me or my friends

• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Appendix 2

Key Stage 2 Acceptable Use Agreement

I will read and follow the rules in the acceptable use agreement policy. When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it I will not: • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision If I bring a personal mobile phone or other personal electronic device into school: • I will hand it into the teacher at the start of the day • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

Appendix 3

Acceptable use agreement (staff, governors, volunteers and visitors)

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • 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, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school • Use a personal mobile phone in areas which children access
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 and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Appendix 4

Online safety training needs – self-audit for staff

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