



## *‘Improving the quality of family life’*

# Online Safety Policy

### Contents

Aims.....	3
2. Legislation and guidance .....	3
3. Roles and responsibilities.....	4
3.1 The board of trustees .....	4
3.2 The headteacher .....	4
3.3 The designated safeguarding lead (DSL) .....	4
3.4 The IT manager .....	5
3.5 All staff and volunteers.....	5
3.6 Parents/carers .....	6
3.7 Visitors and members of the community.....	6
4. Educating pupils about online safety .....	6
5. Educating parents/carers about online safety .....	7
6. Cyber-bullying .....	7
6.1 Definition.....	7
6.2 Preventing and addressing cyber-bullying .....	7
6.3 Examining electronic devices .....	7
6.4 Artificial intelligence (AI).....	8
7. Acceptable use of the internet in school .....	9
8. Pupils using mobile devices in school .....	9
9. Staff using work devices outside school.....	9
10. How the school will respond to issues of misuse .....	9
11. Training.....	10
12. Monitoring arrangements .....	10
13. Links with other policies.....	11
Appendix 1: KS1 acceptable use agreement (pupils and parents/carers) .....	12
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers).....	13
Appendix 3: acceptable use agreement (Trustees, staff, volunteers and visitors).....	14

Appendix 4: online safety training needs – self-audit for staff ..... 15  
Appendix 5: online safety incident report log..... 16  
Revision ..... 17

# Aims

Our school aims to:

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

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

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')

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

## The 4 key categories of risk

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

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

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

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

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

## 2. Legislation and guidance

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

[Teaching online safety in schools](#)

[Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)

[Relationships and sex education](#)

[Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#). It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. This policy complies with our funding agreement and articles of association.

## 3. Roles and responsibilities

### 3.1 The board of trustees

The board of trustees has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The board of trustees will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring. The board of trustees will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children. The board of trustees will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The board of trustees should ensure children are taught how to keep themselves and others safe, including keeping safe online. The board of trustees must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

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

All trustees will:

Ensure they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 3)

Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures

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

### 3.2 The headteacher

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

### 3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular:

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

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

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

Working with the IT manager to make sure the appropriate systems and processes are in place

Working with the headteacher, IT manager and other staff, as necessary, to address any online safety issues or incidents

Managing all online safety issues and incidents in line with the school's child protection policy

Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)

Liaising with other agencies and/or external services if necessary

Providing regular reports on online safety in school to the headteacher and/or board of trustees

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

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

This list is not intended to be exhaustive.

### 3.4 The IT manager

The IT manager is responsible for:

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

Ensuring that the school's IT 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 IT systems on a six-monthly basis

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

Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Ensuring that any filtering/monitoring alerts indicating potential harm are escalated to the DSL/DDSL and recorded as per the School's Child Protection and Safeguarding Policy.

This list is not intended to be exhaustive.

### 3.5 All staff and volunteers

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

Maintaining an understanding of this policy

Implementing this policy consistently

Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing.

If an internet-based resource required for educational purposes is blocked by the monitoring and filtering systems, staff will explain their need to a member of the SLG who will contact smoothwall to request access be enabled.

Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

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

This list is not intended to be exhaustive.

### 3.6 Parents/carers

Parents/carers are expected to:

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

Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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

What are the issues? – [UK Safer Internet Centre](#)

Hot topics – [Child net](#)

Parent resource sheet – [Child net](#)

### 3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

## 4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. **All** schools have to teach:

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

[Relationships and sex education and health education](#) in secondary schools

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

## 5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers. Online safety will also be covered during parents' evenings. The school will let parents/carers know:

What systems the school uses to filter and monitor online use

What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

### 6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class leads will discuss cyber-bullying with their tutor groups.

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

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

### 6.3 Examining electronic devices

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

Poses a risk to staff or pupils, and/or

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

Is evidence in relation to an offence

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

Assess how urgent the search is and consider the risk to other pupils and staff.

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

Seek the pupil's co-operation

The DSL has lead responsibility for decisions about viewing content and safeguarding responses involving digital material. They may authorise staff to examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the DSL should reasonably suspect that the device has, or could be used to:

Cause harm, and/or

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

Commit an offence

If inappropriate material is found on the device, it is up to the DSL / headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response. When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if authorised to do so by the DSL/headteacher because:

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

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

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

**Not** view the image

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

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

The DfE's latest guidance on [searching, screening and confiscation](#)

UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Our Behaviour Policy

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

## 6.4 Artificial intelligence (AI)

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

many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. Snowflake School will treat any use of AI to bully pupils in line with our Anti-Bullying/Behaviour Policy. Any suspected AI-generated sexual imagery will be treated as a safeguarding concern, reported to the DSL or DDSL and managed under the nudes and semi-nudes guidance. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the Snowflake School.

## 7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, trustees and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate. More information is set out in the acceptable use agreements in appendices 1 to 3.

## 8. Pupils using mobile devices in school

The school operates a mobile-phone-free environment in line with the Mobile Phones and Smart Devices Policy. Pupils may bring devices to school but must hand them in on arrival unless an approved exception is in place.

## 9. Staff using work devices outside school

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

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

Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

Making sure the device locks if left inactive for a period

Not sharing the device among family or friends

Installing anti-virus and anti-spyware software

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

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3. Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from Senior Leadership.

## 10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies on 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 IT 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 / staff code of conduct. The action taken will depend on the individual circumstances, nature

and seriousness of the specific incident. The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## 11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). By way of this training, all staff will be made aware that:

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

Children can abuse their peers online through:

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

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Trustees 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 student access to the internet in school is supervised at a level appropriate to need and risk, usually 1:1, by staff who support the students to make good decisions and to use the internet safely. Any concerns about types of access the student attempts or requests are reported to the DSL or DDSL and logged according to the school's Child protection and Safeguarding Policy.

Any electronic monitoring of online access is carried out in accordance with the UK GDPR and Data Protection Act 2018. Logs are stored securely, accessed only by authorised staff, and retained in line with the school's data retention schedule. The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5. This policy will be reviewed every year by the Head Teacher. At every review, the policy will be shared with the board of trustees. The review (such as the one available [here](#)) will be supported by an annual risk

assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

## 13. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

This policy incorporates the ICT and internet acceptable use policy

# Appendix 1: KS1 acceptable use agreement (pupils and parents/carers)

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

**Name of pupil:**

**When I use the school's IT 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:

- I select a website by mistake
- I receive messages from people I don't know
- I find anything that may upset or harm me or my friends

Use school computers for schoolwork only

Be kind to others and not upset or be rude to them

Look after the school IT 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.**

**Signed (pupil):**

**Date:**

**Parent/carer agreement:** I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet and will make sure my child understands these.

**Signed (parent/carer):**

**Date:**

## Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

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

**Name of pupil:**

**I will read and follow the rules in the acceptable use agreement policy.**

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

- Always use the school's IT 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 that 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 not use it during lessons, tutor group time, clubs or other activities organised by the school, unless an approved exception is in place and I am supervised by staff.
- 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.**

**Signed (pupil):**

**Date:**

**Parent/carer's agreement:** I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

**Signed (parent/carer):**

**Date:**

## Appendix 3: acceptable use agreement (Trustees, staff, volunteers and visitors)

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

**Name of trustee/staff member/volunteer/visitor:**

**When using the school's IT 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 that 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

I will only use the school's IT 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 IT 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) and IT manager know if a pupil informs me they have found any material that 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 IT systems and internet responsibly and ensure that pupils in my care do so too.

**Signed (Trustee/staff member/volunteer/visitor):**

**Date:**

## 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, trustees and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

## Appendix 5: online safety incident report log

online safety incident log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

## Revision

Version Update	March 2026
Review due	March 2027
Reviewed By	Sumen Starr
Approved by Board of Trustees on	March 2026