Sedgeberrow CE First School and Preschol

Approved by:	**The Full Governing Body**	**Date: 6/10/25**
Last reviewed on:	**6/10/25**	
Next review due by:	**6/10/26**	

Contents

Appendices

1. Aims

Our school is committed to ensuring the safety and wellbeing of all members of our community in their use of digital technologies. We aim to:

- Establish robust procedures to safeguard pupils, staff, volunteers, and governors in their online interactions.
- Identify and support pupils who may be at increased risk of online harm.
- Deliver a comprehensive and proactive approach to online safety that educates and empowers the entire school community, including the responsible use of mobile and smart technology (referred to as 'mobile phones').
- Implement clear and effective mechanisms for identifying, responding to, and escalating online safety incidents where appropriate.

The Four Key Categories of Online Risk

Our approach to online safety is structured around the following categories of risk:

- **Content** – Exposure to illegal, inappropriate, or harmful material, including pornography, misinformation, disinformation (e.g. fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism.
- **Contact** – Harmful interactions with others online, such as peer pressure, commercial advertising, and grooming or exploitation by adults posing as children or young people.
- **Conduct** – Risky or harmful personal online behaviour, including the creation, sharing, or receipt of explicit images (e.g. consensual and non-consensual sharing of nudes or pornography), and online bullying.
- **Commerce** – Exposure to financial risks such as online gambling, inappropriate advertising, phishing, and scams.

---

2. Legislation and Guidance

This policy is informed by statutory guidance and best practice, including:

- Department for Education (DfE) statutory guidance: *Keeping Children Safe in Education*
- DfE advice on:
    - *Teaching Online Safety in Schools*
    - *Preventing and Tackling Bullying* (including cyberbullying)

- *Searching, Screening and Confiscation*
- *Protecting Children from Radicalisation*

It reflects relevant legislation, including:

- Education Act 1996 (as amended)
- Education and Inspections Act 2006
- Equality Act 2010
- Education Act 2011 – which grants teachers powers to search for and delete inappropriate content from pupils' devices where there is a 'good reason' to do so.

For maintained schools and academies following the National Curriculum:

This policy also aligns with the computing programmes of study within the National Curriculum.

For academies and free schools:

This policy complies with our funding agreement and articles of association.

---

3. Roles and Responsibilities

3.1 Governing Board

The governing board holds overall responsibility for the implementation and monitoring of this policy and for holding the headteacher to account. Specifically, the board will:

- Ensure all staff receive online safety training as part of safeguarding and child protection induction and ongoing professional development.
- Ensure staff understand their responsibilities regarding filtering and monitoring of online activity.
- Provide regular updates to staff on online safety (e.g. via email, bulletins, and staff meetings), at least annually.
- Coordinate regular meetings with relevant staff to review online safety practices and training needs.
- Monitor online safety logs and reports provided by the Designated Safeguarding Lead (DSL).
- Ensure pupils are taught how to stay safe online and how to protect themselves and others.

- Ensure appropriate filtering and monitoring systems are in place on school devices and networks, and review their effectiveness regularly.

The board will also review the DfE's filtering and monitoring standards and work with IT staff and service providers to ensure compliance, including:

- Assigning clear roles and responsibilities for managing filtering and monitoring systems.
- Conducting annual reviews of filtering and monitoring provisions.
- Blocking harmful content without unduly affecting teaching and learning.
- Implementing effective monitoring strategies tailored to the school's safeguarding needs.

If applicable:

The governor with oversight of online safety is [insert role/title].

All governors will:

- Read and understand this policy.
- Agree to and follow the school's acceptable use policy (see Appendix 3).
- Ensure online safety is embedded across safeguarding policies and procedures.
- Support the adaptation of online safety education for vulnerable pupils, including those with SEND or who have experienced abuse, recognising that a personalised approach may be necessary.

3. Roles and Responsibilities (continued)

3.2 The Headteacher

The headteacher is responsible for ensuring that all staff understand and consistently implement this policy across the school. This includes:

- Promoting a whole-school approach to online safety.
- Supporting the DSL in delivering staff training and updates.
- Ensuring that online safety is embedded within the school's safeguarding culture and curriculum.
- Overseeing the response to any significant online safety incidents in collaboration with the DSL and other relevant staff.

3.3 The Designated Safeguarding Lead (DSL)

Details of the DSL and any deputies are outlined in the school's Child Protection and Safeguarding Policy and relevant job descriptions.

The DSL holds lead responsibility for online safety and will:

- Support the headteacher in ensuring consistent implementation of this policy.
- Collaborate with the headteacher and governing board to review and update the policy annually.
- Lead on understanding and overseeing the school's filtering and monitoring systems.
- Provide assurance to governors regarding the effectiveness of these systems.
- Work with the ICT manager to ensure appropriate technical safeguards are in place.
- Address online safety concerns and incidents in line with the school's safeguarding procedures.
- Respond to safeguarding issues identified through filtering and monitoring.
- Ensure all online safety incidents are logged and managed appropriately (see Appendix 5).
- Ensure incidents of cyber-bullying are addressed in accordance with the school's behaviour policy.
- Deliver and update staff training on online safety (see Appendix 4 for staff self-audit).
- Liaise with external agencies and services when necessary.
- Provide regular reports to the headteacher and governing board on online safety matters.
- Conduct annual risk assessments to identify and mitigate online risks faced by pupils.
- Provide safeguarding updates, including online safety, to staff at least annually.

Note: This list is not exhaustive.

3.4 The ICT Manager

The ICT manager is responsible for:

- Implementing and maintaining appropriate filtering and monitoring systems on school devices and networks, reviewed at least annually.

- Ensuring ICT systems are secure and protected against viruses, malware, and other threats.
- Conducting regular security checks and monitoring (e.g. weekly, fortnightly, or monthly as determined by the school).
- Blocking access to harmful websites and preventing downloads of dangerous files.
- Logging and managing online safety incidents (see Appendix 5) in line with this policy.
- Ensuring cyber-bullying incidents are addressed in accordance with the behaviour policy.

Note: This list is not exhaustive.

3.5 All Staff and Volunteers

All staff, contractors, agency staff, and volunteers are expected to:

- Maintain a clear understanding of this policy.
- Implement the policy consistently in their practice.
- Agree to and follow the acceptable use terms for ICT systems and internet (Appendix 3).
- Ensure pupils adhere to the acceptable use agreements (Appendices 1 and 2).
- Be aware that the DSL oversees filtering and monitoring systems, and report any failures via [insert school-specific reporting procedure].
- Follow the correct procedure via [insert school-specific bypass process] if filtering needs to be temporarily bypassed for educational purposes.
- Work with the DSL to log and manage online safety incidents appropriately (Appendix 5).
- Address cyber-bullying incidents in line with the behaviour policy.
- Respond appropriately to all concerns regarding sexual violence and/or harassment, both online and offline, maintaining an attitude of *“it could happen here.”*

Note: This list is not exhaustive.

3.6 Parents and Carers

Parents and carers are expected to:

- Raise any concerns or queries regarding this policy with a member of staff or the headteacher.
- Ensure their child has read, understood, and agreed to the acceptable use terms (Appendices 1 and 2).

Further guidance for parents/carers on keeping children safe online is available from:

- UK Safer Internet Centre – What are the issues?
- Childnet – Help and advice for parents/carers
- Childnet – Parents and carers resource sheet

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 and, where appropriate, asked to read and agree to the acceptable use terms (Appendix 3).

4. Educating Pupils About Online Safety

Online safety education is embedded within the school curriculum and delivered in an age-appropriate and progressive manner. Pupils are taught how to stay safe online through computing lessons, PSHE, RSE, and other relevant subjects.

This section reflects the National Curriculum computing programmes of study and the Department for Education's guidance on relationships education, relationships and sex education (RSE), and health education (valid until 31 August 2026). Academies not following the National Curriculum should adapt the Key Stage content to reflect their own curriculum.

Primary Education

In **Key Stage 1**, pupils are 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 online.

In **Key Stage 2**, pupils are 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.
- Be discerning in evaluating digital content.

By the end of primary school, pupils will understand:

- The risks of online abuse, trolling, bullying, and harassment, and their impact on mental health.
- That people may behave differently online, including pretending to be someone else.
- That respectful behaviour applies both online and offline, including when anonymous.
- Rules and principles for staying safe online, recognising harmful content and contact, and how to report concerns.
- How to critically evaluate online friendships and sources of information.
- How data is shared and used online.
- How to be a discerning consumer of online information, including understanding search engine algorithms.
- Appropriate boundaries in digital friendships.
- How to respond safely to unfamiliar adults online.
- The importance of limiting screen time and understanding the impact of online content on wellbeing.
- Age restrictions on social media and gaming, and how to manage online challenges.
- The impact of online actions on others and the importance of privacy.
- Where and how to report concerns and seek support.

Secondary Education

In **Key Stage 3**, pupils are taught to:

- Use technology safely, respectfully, responsibly, and securely.
- Protect their online identity and privacy.
- Recognise and report inappropriate content, contact, and conduct.

In **Key Stage 4**, pupils are taught to:

- Understand how technological changes affect online safety.
- Learn new ways to protect their privacy and identity.
- Report a range of online concerns.

By the end of secondary school, pupils will understand:

- Their rights, responsibilities, and opportunities online.
- That online behaviour is subject to the same expectations as offline behaviour.
- The risks of sharing material online and the difficulty of removing it.
- The importance of not sharing personal or compromising material.
- How to report and manage online issues.
- The impact of harmful content, including sexually explicit material.
- That sharing indecent images of children is a criminal offence.
- How data is generated, collected, and used online.
- How to identify and respond to harmful behaviours online.
- How to recognise and communicate consent, including online.
- The similarities and differences between online and offline worlds, including the risks of comparison, curated online personas, online gambling, and targeted advertising.

Whole-School Approach

Online safety is also addressed across other subjects where relevant. Teaching is adapted to meet the needs of vulnerable pupils, including those with SEND or who have experienced abuse, ensuring a personalised and contextualised approach where necessary.

---

5. Educating Parents and Carers About Online Safety

The school is committed to working in partnership with parents and carers to promote online safety. Awareness will be raised through:

- Letters and communications sent home.
- Information shared via the school website or virtual learning environment (VLE).
- Inclusion of online safety topics during parents' evenings.
- Sharing this policy with parents/carers.

Parents/carers will be informed about:

- The school's filtering and monitoring systems.
- The nature of online activities pupils are asked to engage in, including websites accessed and any staff interaction online.

Parents/carers are encouraged to raise any concerns or queries regarding online safety with the headteacher or DSL. General concerns about this policy may be directed to any member of staff or the headteacher.

6. Cyber-Bullying

6.1 Definition

Cyber-bullying is a form of bullying that occurs online, including through social networking sites, messaging apps, and gaming platforms. As with other forms of bullying, it involves the repetitive, intentional harming of an individual or group by another, where there is an imbalance of power. For further guidance, refer to the school's Behaviour Policy.

6.2 Preventing and Addressing Cyber-Bullying

To prevent cyber-bullying, the school will:

- Ensure pupils understand what cyber-bullying is, how it manifests, and what to do if they experience or witness it.
- Encourage pupils to report incidents, whether they are victims or bystanders.
- Discuss cyber-bullying regularly with pupils, exploring its causes, forms, and consequences. These discussions will be led by class teachers or form tutors.
- Integrate cyber-bullying education into the curriculum, particularly through PSHE and other relevant subjects.

All staff, governors, and volunteers (where appropriate) will receive training on cyber-bullying, its impact, and how to support affected pupils, as part of safeguarding training (see Section 11).

The school will also provide parents/carers with information and resources (e.g. leaflets) to help them recognise signs of cyber-bullying, understand how to report it, and support their children.

In the event of a specific cyber-bullying incident, the school will follow procedures outlined in the Behaviour Policy. Where harmful or illegal content has been shared among pupils, the school will take all reasonable steps to contain the incident.

If the DSL has reasonable grounds to believe that material involved in an incident is illegal, they will report it to the police and provide the relevant evidence as soon as reasonably practicable. The DSL will also liaise with external agencies where appropriate.

6.3 Examining Electronic Devices

The headteacher, and any staff member authorised by the headteacher (as specified in the Behaviour Policy), may search and confiscate electronic devices if they have reasonable grounds to suspect that the device:

- Poses a risk to staff or pupils;
- Is listed in the school rules as a banned item subject to search;
- Contains evidence related to an offence.

Before conducting a search, authorised staff will:

- Assess the urgency of the search and consider risks to others. If not urgent, they will seek advice from the headteacher, DSL, or another appropriate staff member.
- Explain the reason for the search to the pupil and how it will be conducted.
- Seek the pupil's cooperation.

Authorised staff may examine, and in exceptional cases erase, data or files on a confiscated device if they believe there is a 'good reason' to do so. A 'good reason' may include suspicion that the device has been used to:

- Cause harm;
- Undermine the safe environment of the school or disrupt teaching;
- Commit an offence.

If inappropriate material is found, the response will be determined by the staff member in consultation with the DSL, headteacher, or another member of the senior leadership team. If the material is suspected to pose a safeguarding risk, the appropriate safeguarding response will be prioritised.

Staff will not delete material that may constitute evidence of a suspected offence. In such cases, the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence of an offence, staff may delete it if:

- Its continued existence is likely to cause harm; and/or
- The pupil or parent/carer refuses to delete it themselves.

If a staff member suspects that a device contains an indecent image of a child (e.g. a nude or semi-nude image), they will:

- Not view the image.
- Confiscate the device and report the incident immediately to the DSL.
- The DSL will follow the DfE's latest guidance on *Searching, Screening 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.

All searches will be conducted in accordance with:

- DfE guidance on *Searching, Screening and Confiscation*;
- UKCIS guidance on *Sharing Nudes and Semi-Nudes*;
- The school's Behaviour Policy and/or Searches and Confiscation Policy.

Complaints regarding the searching or deletion of inappropriate material on pupils' devices will be handled through the school's Complaints Procedure.

6.4 Artificial Intelligence (AI)

Generative AI tools are increasingly accessible and widely used. Staff, pupils, and parents/carers may be familiar with platforms such as ChatGPT, Google Gemini, and other generative chatbots.

[School Name] recognises the educational potential of AI to enhance learning and engagement. However, we also acknowledge the risks associated with its misuse, particularly in the context of bullying. One such risk includes the creation of *deepfakes*—AI-generated images, audio, or video hoaxes that appear real. This includes deepfake pornography, where AI is used to fabricate explicit content featuring someone's likeness.

Any use of AI to bully, harass, or harm others will be treated with the utmost seriousness and addressed in accordance with the school's **Behaviour Policy** and **Anti-Bullying Policy**.

Staff must remain vigilant when using AI tools, especially those still in development. A **risk assessment** must be conducted before introducing new AI tools or using existing ones in ways that may pose risks to pupils, staff, or other individuals.

All use of AI must comply with the school's **AI Usage Policy** [if applicable].

---

7. Acceptable Use of the Internet in School

All pupils, parents/carers, staff, volunteers, and governors are required to sign an **Acceptable Use Agreement** regarding the use of the school's ICT systems and internet (see Appendices 1–3). Visitors may also be asked to read and agree to these terms where relevant.

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

The school will monitor internet usage across all users and apply appropriate filtering systems to restrict access to harmful or inappropriate content.

Further details are provided in the Acceptable Use Agreements in Appendices 1–3.

---

8. Pupils Using Mobile Devices in School

Pupils may bring mobile devices to school; however, they are not permitted to use them during:

- Lessons
- Tutor group time
- Before or after school clubs or any other school-organised activities

All use of mobile devices must comply with the Acceptable Use Agreement (Appendices 1 and 2). Breaches may result in disciplinary action in line with the **Behaviour Policy**, including confiscation of the device.

---

9. Staff Using Work Devices Outside School

Staff must take appropriate measures to ensure the security of work devices used outside school. This includes:

- Using strong passwords (e.g. three random words with numbers/symbols or password manager-generated)
- Ensuring hard drive encryption
- Activating automatic locking after periods of inactivity
- Not sharing devices with family or friends
- Installing and maintaining anti-virus and anti-spyware software
- Keeping operating systems and software up to date

Work devices must be used solely for professional purposes and in accordance with the Acceptable Use Agreement (Appendix 3).

Any concerns regarding device security must be reported to the **ICT Manager** [or relevant role].

---

10. How the School Will Respond to Issues of Misuse

Pupils

Misuse of the school's ICT systems or internet by pupils will be addressed in accordance with the **Behaviour Policy** and **ICT and Internet Acceptable Use**

Policy. Responses will be proportionate to the nature and seriousness of the incident.

Staff

Misuse by staff, including inappropriate use of personal devices where it constitutes misconduct, will be dealt with under the **Staff Disciplinary Procedures** or **Staff Code of Conduct**, as appropriate.

Serious Incidents

Where incidents involve illegal activity or content, or are otherwise serious, the school will consider reporting the matter to the police.

---

11. Training

11.1 Staff, Governors and Volunteers

All new staff will receive induction training on safe internet use and online safeguarding, including cyber-bullying and online radicalisation.

All staff will receive annual refresher training and ongoing updates via emails, bulletins, and staff meetings.

Training will ensure staff understand:

- The role of technology in safeguarding and wellbeing issues.
- How children may abuse peers online through:
    - Abusive or misogynistic messages
    - Non-consensual sharing of indecent images/videos
    - Sharing of unwanted explicit content
- That physical, sexual, and initiation/hazing abuse may have online elements.

Training will also support staff to:

- Recognise signs of online abuse.
- Help pupils identify and assess online risks.
- Guide pupils in making safe and healthy choices online.

The **DSL and any deputies** will undertake safeguarding training, including online safety, at least every two years, with annual updates to maintain current knowledge.

Governors will receive online safety training as part of their safeguarding responsibilities.

Volunteers will receive appropriate training and updates where applicable.

Further details are available in the **Child Protection and Safeguarding Policy**.

11.2 Pupils

All pupils will receive age-appropriate training on safe internet use. This will include:

- Understanding methods used by hackers to trick individuals into disclosing personal information.
- The importance of password security and how to create strong passwords.
- Awareness of social engineering tactics.
- Risks associated with removable storage devices (e.g. USB drives).
- The role and benefits of multi-factor authentication.
- How to report a cyber incident or attack.
- How to report a personal data breach.

In addition, pupils will be taught about safeguarding issues such as cyber-bullying and the risks of online radicalisation, in a manner appropriate to their age and developmental stage.

---

12. Monitoring Arrangements

The Designated Safeguarding Lead (DSL) maintains logs of behaviour and safeguarding issues related to online safety. An incident report log template is provided in **Appendix 5**.

This policy will be reviewed annually by the **[Insert Job Title, e.g. Headteacher or DSL]**. Each review will be shared with the governing board and supported by an **annual risk assessment** that reflects the evolving risks pupils face online. This is essential due to the rapid development of technology and associated risks.

---

13. Links with Other Policies

This Online Safety Policy is closely linked to the following school policies and procedures:

- **Child Protection and Safeguarding Policy**
- **Behaviour Policy**
- **Staff Disciplinary Procedures**
- **Data Protection Policy and Privacy Notices**
- **Complaints Procedure**

- **ICT and Internet Acceptable Use Policy**

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

Adapt this agreement to reflect your school's approach, in line with any changes you made to this policy.

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

Acceptable use of the school's ICT systems and internet:

agreement for pupils and parents/carers

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:
    - 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 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 or other device 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:**

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Parent/carer agreement: I agree that my child can use the school's ICT 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 ICT 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)

Adapt this agreement to reflect your school's approach, in line with any changes you made to this policy.

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 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 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, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
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 ICT 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 ICT 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 (staff, governors, volunteers and visitors)

Adapt this agreement to reflect your school's approach, in line with any changes you made to this policy.

Acceptable use of the school's ICT systems and 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 (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

Acceptable use of the school's ICT systems and internet: agreement for staff, governors, volunteers and visitors	
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) and ICT 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 ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self-audit for staff

Adapt this form to suit your needs.

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?	

online safety training needs audit	
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**