The LETTA Trust

Online Safety Policy (Inc. Acceptable use)

Approved & adopted on:	Spring 2026	**To be reviewed:**	Spring 2027
Reviewed by:	Trust Board	**Signed:**	

Contents

1. Aims and approach:

- To educate the whole school community in its safe use of technology
- To ensure the online safety of pupils, staff, visitors, and those in governance roles
- To establish clear mechanisms to identify, intervene, and manage online safety concerns if they occur

The 4 key categories of risk
Our approach to online safety is based on addressing the following categories of risk:

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

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

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

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

2. Legislation and guidance

This policy is based on the DfE's statutory safeguarding guidance KCSiE non-statutory advice to schools:

- Teaching online safety in schools
- Preventing and tackling bullying
- Cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Protecting children from radicalisation
- Education Act 1996
- Education Act 2011
- Education and Inspections Act 2006
- Equality Act 2010
- DfE Filtering and Monitoring Standards for Schools 2024
- DfE 'Keeping children safe in education' 2025

The policy also takes into account the National Curriculum computing programmes of study and complies with our funding agreement and articles of association.

3. Current Online Safeguarding Trends

Self-generative artificial intelligence (AI) has become rapidly more accessible, and many pupils have unrestricted access to tools that generate text, images, and video both at home and in school. While these tools can offer creative and educational opportunities, they present significant safeguarding challenges. AI-generated content can be inaccurate, misleading, or harmful, and there is an increased risk of plagiarism in school work. Mainstream AI tools generally lack end-user safety settings, have minimum age requirements of 13 or 18, and, while filtering basic offensive language, can produce inappropriate material.

AI also makes it easier than ever to create sexualised images and deepfake videos. Even when content is not real, it can have a severe impact on pupils' emotional well-being and physical safety, and may be used to intimidate, humiliate, or abuse. Reports from the Internet Watch Foundation indicate that AI-generated imagery of child sexual abuse is increasing at a concerning rate.

Social media use remains widespread among pupils. According to Ofcom's *Children and Parents: Media Use and Attitudes Report 2024*, YouTube is the most used platform for under-18s, while WhatsApp, TikTok, and Snapchat continue to grow in reach. Children aged 3–17 spend an average of 3 hours and 5 minutes online daily, and many parents report difficulty managing screen time. Despite age restrictions, 51% of children under 13 use social media, and four in ten admit to giving a false age online.

Within the Trust, we recognise that many pupils engage with apps and AI tools regardless of age restrictions. Our approach is therefore to educate pupils on safe and responsible use, support parents in managing their child's digital activity, and ensure that safeguarding measures are in place both at school and at home. Primary-aged children are particularly vulnerable, with over 90% having access to their own devices by the end of primary school, often without safety controls or limitations. Young children are increasingly targeted by harmful content online, including AI-generated sexualised material.

The Trust is committed to ongoing digital safety education, clear guidance for pupils and families, and robust monitoring to address emerging risks and trends in online safeguarding.

3.1 Content Risks

The LETTA recognises that certain online content can be harmful to pupils' wellbeing and safety. This includes **misinformation, disinformation, and conspiracy theories**. Staff must be aware that exposure to these types of content can affect mental health or contribute to radicalisation.

4. Roles and responsibilities

4.1 Trustees and members of the local governing board

The Trust Board has overall responsibility for monitoring this policy and holding the CEO to account for ensuring that headteachers implement it in LETTA Trust schools. Members of the LGB will meet regularly with school DSLs and will check online safety logs during these meetings.

All those in governance will:

- ensure that 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 2)
- ensure that online safety is included in safeguarding and related policies and procedures
- ensure that, where necessary, teaching about online safety is adapted for some pupils with special educational needs and/or disabilities (SEND)
- ensure that effective cybersecurity checks and measures are in place

4.2 The headteacher

The headteacher is responsible for ensuring that school staff understand this policy and that it is being implemented consistently throughout the school. The headteacher will monitor online safety logs as provided by the designated safeguarding lead (DSL).

4.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

The LETTA Trust treats poor attendance as a potential safeguarding concern. Online safety incidents, including bullying, will be considered if they may contribute to absence. DSLs will ensure all attendance concerns are monitored and investigated in line with statutory guidance.

The DSL will also work closely with the IT leader and takes lead responsibility for online safety, including filtering and monitoring systems:

- supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- understanding the filtering and monitoring systems and processes in place, as explained in KCSIE
- working with the headteacher, ICT manager, and other staff, as necessary, to address any online safety issues or incidents
- ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- ensuring that any incidents of cyberbullying, including sexual harassment online, are logged and dealt with appropriately in line with the school behaviour policy
- updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)that helps staff understand their expectations, roles, and responsibilities around filtering and monitoring. This is explained in paragraph 124 of KCSIE 2023
- liaising with external services if necessary
- providing regular reports on online safety in school to the headteacher

This list is not intended to be exhaustive.

4.4 The IT leader

The IT leader is responsible for:

- putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- ensuring the designated safeguarding lead (DSL) understands the filtering and monitoring systems and processes in place
- ensuring that the school's IT systems are secure and protected against cyber attacks from viruses and malware, and that such cybersecurity safety mechanisms are updated regularly
- organising full security checks and monitoring the school's IT systems on a termly 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 4) and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying, including sexual harassment online, are dealt with appropriately in line with the school behaviour policy
- ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse, and some pupils with SEND, 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
- ensure that the Internet Watch Foundation (IWF) and Counter Terrorism Internet Referral Unit (CTIRU) blocklists remain active at all times. Staff and system administrators must not disable these lists under any circumstances.

This list is not intended to be exhaustive.

4.5 All staff and visitors

All staff and visitors are responsible for:

- reading and understanding 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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying, including sexual harassment online, are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

4.6 Parents

Parents are expected to:

- ensure their child has read, understood, and agreed to the terms on acceptable use of the school's IT systems and internet (appendix 1)
- be responsible for what children are accessing online at home if their child is using a Chromebook
- notify a member of staff of any concerns or queries regarding this policy
- attend online safety training provided by the school

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

- What are the issues? – UK Safer Internet Centre
  Provides guidance on online risks and how parents can support children.
- Hot Topics – Childnet International
  Covers current online safety topics that concern children and young people.
- Parent Factsheet – Childnet International
  A practical factsheet for parents about online safety.
- Healthy Relationships – Disrespect Nobody
  Guidance on helping children understand healthy relationships online and offline.
- NSPCC Share Aware
  Supports parents in having conversations with children about online safety and responsible sharing.

5. Educating pupils about online safety

Pupils are taught about online safety as part of the curriculum.

Key Stage 1:

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

Key Stage 2:

- 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) whom they do not know

The safe use of the internet and social media will also be covered in other subjects where relevant, and schools use assemblies to raise pupils' awareness of the dangers that can be encountered online.

6. Educating parents about online safety

Schools raise parents' awareness of internet safety in letters or information via the website.
If parents have any queries or concerns in relation to online safety, these are addressed in the first instance by the DSL or IT leader.

7. Cyber-bullying

7.1 Definition

Cyber-bullying is bullying that takes place online, e.g., through social networking sites, messaging apps, or gaming sites. Like other forms of bullying, it is the repetitive, intentional, and harmful behavior of one person or group toward another person or group.

7.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We ensure that pupils know how they can report incidents and are encouraged to do so, including when they are a witness rather than the victim. Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying, e.g., personal, social, health, and economic (PSHE) education. All staff receive training on cyber-bullying, its impact, and ways to support pupils, as part of safeguarding training (see section 11 for more details). 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. When resolving an incident of cyber-bullying, the school follows the processes set out in the anti-bullying policy. The DSL considers whether the incident should be reported to the police if it involves illegal material and works with external services if necessary.

7.3 Examining electronic devices

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

- poses a risk to staff or pupils
- is identified in the school rules as a banned item for which a search can be carried out
- is evidence in relation to an offence

If the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also do the following before a search:

- make an assessment of how urgent the search is. If the search is not urgent, they will seek advice from the headteacher or DSL
- 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 cooperation
- always carry out the search with another staff member present

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

- the DfE's latest guidance on searching, screening and confiscation
- UKCCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- our behaviour policy and staff code of conduct

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that has been 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 staff member should reasonably suspect that the device has, or could be used to:

- cause harm
- undermine the safe environment of the school or disrupt teaching
- commit an offence

When deciding if there is a good reason to erase data or files from a device, the headteacher or DSL 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:

- they reasonably suspect that its continued existence is likely to cause harm to anyone
- the pupil and/or the parent refuses to delete the material themselves

If inappropriate material is found on the device, it is up to the headteacher or DSL 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.

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

8. Acceptable use of the internet in school

All pupils, parents, staff, volunteers, and those in governance are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 and 2). Visitors are 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 monitor the websites visited by pupils, staff, volunteers, those in governance roles, and visitors (where relevant) to ensure they comply with the above.

9. Mobile phones or other personal devices

9.1 Pupils' Use of Mobile Phones and Personal Devices

Under Section 89 of the Education and Inspections Act 2006, the Headteacher has the authority to regulate pupils' behaviour on school premises, including the possession and use of mobile phones and electronic devices.

In line with this duty, the school prohibits the use of mobile phones and similar electronic devices (e.g smartwatches) by pupils during the school day.

Where a pupil brings a mobile phone to school, the device must be switched off and handed to the school office or stored securely as directed by the Headteacher.

9.2 Staff Use of Mobile Phones

In accordance with safeguarding duties under the Keeping Children Safe in Education, staff must ensure that personal mobile phone use does not compromise supervision, professional boundaries, or safeguarding responsibilities.

Personal mobile phones must not be used by staff when supervising pupils. except where necessary for safeguarding, health and safety, or operational reasons. This may include:

- emergency evacuations (e.g. fire drills)
- supervising off-site trips
- supervising residential visits
- where a member of staff has an acutely ill dependent and prior agreement has been obtained from the Headteacher

In these circumstances, staff must:

- use their mobile phones in an appropriate and professional manner, in line with the Staff Code of Conduct
- not use personal devices to take photographs or recordings of pupils, or anything that could identify a pupil
- not share personal phone numbers with parents; where contact is required, communication must take place via the school office

The school office number remains the primary point of contact for emergencies during the school day, ensuring clear safeguarding oversight and appropriate record-keeping.

9.3 Reasonable Adjustments

The school will comply with its duties under the Equality Act 2010 to make reasonable adjustments for pupils with disabilities and to avoid substantial disadvantage.

Where a mobile phone or electronic device is required as an auxiliary aid, or is necessary to support a pupil's medical needs, disability, or safeguarding requirements, an exception to the general restrictions may be permitted.

This may include, for example:

- use of a device to monitor a medical condition (e.g., glucose levels for pupils with Type 1 Diabetes)
- use of assistive technology to support communication or learning
- specific arrangements linked to safeguarding, SEND or care responsibilities

Any agreed adjustment must be authorised by the Headteacher and recorded appropriately within the pupil's individual support or healthcare plan.

10. Staff using work devices outside school

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

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

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

11. Staff and pupil Google accounts

Staff and pupil Google accounts will be retained for 1 year after they leave. They will then be deleted.

12. How the school will respond to issues of misuse

Where a pupil misuses a school's IT systems or internet, they follow the procedures set out in the 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. 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.

13. Training

All new staff members 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 receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required.

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

- technology is a significant component in many safeguarding and well-being issues, and children are at risk of online abuse
- physical abuse, sexual violence, and initiation/hazing-type violence can all contain an online element
- children can abuse their peers online through:
    - abusive, harassing, and misogynistic messages
    - non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - sharing of abusive images and pornography, to those who don't want to receive such content

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 DSLs and the DDSLs 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.

Volunteers will receive training appropriate to their role in school. More information about safeguarding training is set out in our child protection and safeguarding policy.

14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be downloaded from CPOMS

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet-connected devices and may include:

- physically monitoring by staff watching the screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

This policy will be reviewed annually by the CEO and approved by the Trust Board.

14.1 Online radicalisation and extremism

Letta Trust's filtering systems are in place to protect pupils and staff from accessing extremist content.

Any concerns regarding a pupil or staff member being radicalised online are managed in line with the Trust's Child Protection and Safeguarding Policy and Prevent Duty training.

15. Cyber security

The school recognises that cyber incidents and attacks present a serious risk to education settings, with potential impacts including safeguarding concerns, significant data breaches, disruption to teaching and learning, financial loss, reputational damage, and even school closure.

To manage these risks, the school:

- Has reviewed the DfE Cyber Security Standards for Schools and Colleges (January 2025) and is actively working toward meeting these standards.

- Acknowledges that cyber incidents may be intentional and unauthorised attempts to access, change, or damage data and digital systems. These may come from external or internal sources.
- Understands the risks to safeguarding, particularly the compromise of sensitive personal data relating to children, staff, and families.
- Recognises that disruption caused by cyber incidents may directly impact student outcomes.

In line with NCSC guidance ('Cyber-security in schools: questions for governing bodies and Trustees'), the school ensures that the governing body and senior leaders regularly review and discuss cyber security risks. The following principles guide our approach:

1. Risk Awareness – Governors and leaders are aware of cyber threats and their potential impact.
2. Accountability – Cyber security is led and overseen at senior leadership and governance levels.
3. Policies & Procedures – Cyber security is embedded within safeguarding, data protection, and online safety policies.
4. Training & Awareness – Staff and pupils receive appropriate training to recognise and respond to cyber risks.
5. Resilience & Response – The school has procedures in place to prevent, detect, respond to, and recover from cyber incidents.
6. Review & Improvement – Policies, systems, and practices are regularly reviewed and improved in light of new threats and guidance.

The school is committed to protecting its digital technology, networks, and data to safeguard the education and well-being of all members of its community.

16. Online peer-on-peer sexual violence and harassment

Letta Trust recognises that peer-on-peer abuse can occur online. Examples include:

- Non-consensual sharing of sexual images and videos
- Sexualised cyberbullying
- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

Letta Trust addresses all concerns regarding online peer-on-peer abuse, whether or not the incident occurs on Trust premises or using Trust-owned devices.

Concerns about online peer-on-peer abuse must be reported to the Designated Safeguarding Lead (DSL) and will be managed in accordance with the Trust's Child Protection and Safeguarding Policy.

17. Links with other policies:

- Child protection and safeguarding policy
- Whistleblowing policy
- Behaviour and anti-bullying policy
- Staff code of conduct
- Information governance policy
- Complaints procedure
- Remote learning and communication with families
- Outbreak management and remote learning plan

Appendix 1: Acceptable use agreement (pupils, parents or carers)

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

When using the school's IT systems and accessing the internet in school, I will:

- Only use the Internet for schoolwork, research and homework
- Always make sure there is a teacher or other member of staff present
- When using the Internet at school make sure that I follow my teacher's instructions
- Surf with a friend or another pupil. Two heads are better than one!
- Be a wise surfer. Never access inappropriate websites, never access social networking sites unless this is allowed as part of a learning activity and never use chat rooms
- Ask "Is it true?" and not assume that information published online or in emails is true
- Keep passwords and login names private
- Log in to the school's network using someone else's details
- Only write to email addresses approved by my teachers or parents
- Check with a teacher before opening attachments in emails or following links in emails
- Be careful what I write and make sure not to write things that could upset and offend others
- Never give out personal information such as address or telephone number online
- Never put others in danger by giving out personal information about them online
- Use CEOP to report any inappropriate online activity or tell an adult if I have a problem
- Ignore negative emails and let my teacher know if I'm sent anything I don't like
- Use any inappropriate language when communicating online, including in emails
- Report Cyber-bullying immediately
- Never arrange to meet anyone offline without adult supervision
- Let a teacher or other member of staff know if I find material which might upset or harm me or others
- Remember that some websites and social media are illegal for Under 13s
- Always respect the privacy of other users' files
- Report anything that breaches these rules immediately to my teacher
- Log off or shut down a computer when I've finished working on it

Mobile phones

Pupils: I agree to help keep my school a phone-free space. If I bring a phone for my journey, I will hand it in at the office as soon as I arrive. I will make sure my phone (and smartwatch) is never used, seen, or heard during the school day so that I can focus on my learning and my friends.

Parents: I will support the school's decision to be a phone-free environment. I understand this helps my child stay focused and safe. If I need to get an urgent message to my child, I will call the school office instead of their personal phone.

I understand that the school will monitor the websites I visit at school or when using school equipment.

If I do not understand any part of this Acceptable Use Policy, I will ask a member of staff.

Signed (pupil):	**Date:**
Parent or 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 for bringing a mobile phone to school. I will make sure my child understands these.	
Signed (parent or carer):	**Date:**

Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's IT systems and the internet: agreement for staff, governors, volunteers and visitors	
Name:	
When using the school's IT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details unless I am required to do so as part of my job	
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 • 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. • let the designated safeguarding lead (DSL) and IT leader 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 • always use the school's IT systems and internet responsibly, and ensure that pupils in my care do so too • not use personal devices in the presence of children or use these to take pictures of children I agree that the school will monitor the websites I visit at work or on a work device.	
Signed:	**Date:**

Appendix 3: Online safety training needs – self-assessment for staff

Online safety training needs audit	
Name:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with an online safety concern?	
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?	
Do you regularly change your password for accessing the school's IT 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? Please record them here.	