

Online Safety Policy

St Martin's School



Reviewed by:	Tamara Spencer
---------------------	----------------

Last reviewed on:	October 2026
--------------------------	--------------

Next review due by:	October 2027
----------------------------	--------------

Approved by:	Tim Shenton
---------------------	-------------

Contents

1. Aims	2
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety.....	6
5. Educating parents/carers about online safety	7
6. Cyber-bullying	7
7. Acceptable use of the internet in school	8
8. Pupils using mobile devices in school.....	9
9. Staff using work devices outside school	10
10. How the school will respond to issues of misuse	10
11. Training	10
12. Monitoring arrangements	11
Appendix 1: KS1 acceptable use agreement.....	13
Appendix 2: KS2 acceptable use agreement.....	14
Appendix 3: acceptable use agreement (staff and volunteers).....	15
Appendix 4: online safety training needs – self-audit for staff.....	16
Appendix 5: online safety incident report log	17

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- 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, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation and conspiracy theories.
- **Contact** – being subjected to harmful online interaction with other users or generative AI applications that simulate such interactions, 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, including explicit images generated or digitally altered using artificial intelligence. (consensual and non-consensual making or sharing of nudes and semi-nudes

and/or videos, including images or videos generated or digitally altered using artificial intelligence, such as deepfakes), 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 (2026), 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, Sex Education and Health Education (RHSE)
- Searching, screening and confiscation

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

It reflects existing legislation and guidance, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. It also reflects applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025. It also reflects the Education Act 2011 and statutory powers relating to searching, screening and confiscation in schools and the Department for Education's Searching, Screening and Confiscation guidance. The school's procedures for searching, screening and confiscation, including the handling of electronic devices, will be followed when exercising these powers. The school's procedures for searching, screening and confiscation will be followed when exercising these powers. This policy should be read alongside the school's Child Protection and Safeguarding Policy, Behaviour Policy, Staff Code of Conduct, Mobile Phone Policy, Acceptable Use Agreements, Data Protection Policy and relevant risk assessments.

3. Roles and responsibilities

3.1 The Proprietors

The proprietors have overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

3.2 The Online Safety Lead (OSL)

The OSL 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 OSL 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 OSL 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 OSL should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The OSL 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 school will maintain a documented filtering and monitoring review at least annually. The review will consider the age and risk profile of pupils, including pupils who may be particularly vulnerable, the use of school-managed and personal devices where applicable, remote access, generative AI, changes to technology and network configuration, known safeguarding incidents, teaching requirements and the effectiveness and limitations of the filtering

and monitoring systems. The review will be undertaken by the member of the senior leadership team responsible for filtering and monitoring, with the DSL and IT support/provider, and the findings and any resulting actions will be reported to the proprietors and recorded.

The school will maintain appropriate monitoring arrangements and review monitoring reports and alerts in accordance with its safeguarding needs. High-risk safeguarding alerts will be escalated to the DSL without delay.

The headteacher 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.

The OSL will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that 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

3.3 The Headteacher

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

3.4 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputy/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:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the proprietors 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 ICT manager to make sure the appropriate systems and processes are in place
- Working with the ICT 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 and safeguarding 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 proprietors
- 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.

3.5 The ICT manager

The ICT 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 ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on an ongoing 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

This list is not intended to be exhaustive.

3.6 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 ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing who is responsible for the school's filtering and monitoring arrangements and understanding their own responsibilities for reporting concerns, failures or inappropriate content identified through those systems by notifying the DSL (who will inform the ICT manager & headteacher)
- Following the correct procedures by contacting Advise Consulting if they need to bypass the filtering and monitoring systems for educational purposes
- 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.

3.7 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 – [Childnet](#)
- Parent resource sheet – [Childnet](#)

3.8 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 Digital Technology curriculum.

As an independent primary school, the school provides Relationships Education in accordance with the statutory requirements and has regard to the Department for Education's statutory guidance on Relationships Education, Relationships and Sex Education and Health Education.

The school also provides personal, social, health and economic education (PSHE) in accordance with the Independent School Standards, including appropriate health education.

Online safety is incorporated into Relationships Education, PSHE, safeguarding and the wider curriculum as appropriate.

In **Key Stage (KS) 1**, pupils will be taught to:

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

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

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

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online

- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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 on our website.

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 teachers will discuss cyber-bullying with their class.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (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. Online bullying and other harmful online behaviour may constitute child-on-child abuse. Where an incident involves sexual harassment, sexual violence, abuse, exploitation, threats, coercion or other safeguarding concerns, it will also be dealt with in accordance with the school's Child Protection and Safeguarding 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.

Where an incident involves potentially illegal material or activity, the DSL will consider whether a referral to the police or another appropriate agency is required, in accordance with the school's Child Protection and Safeguarding Policy and relevant safeguarding guidance. Staff must not intentionally view, copy, print, download, share, store or save an indecent image of a child or other potentially illegal child sexual abuse material. Where a device or material may contain such an image, staff should avoid viewing the material and refer the matter immediately to the DSL or deputy DSL, who will determine the appropriate safeguarding response in accordance with current DfE and UKCIS guidance.

6.3 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are increasingly accessible to children and adults. The school recognises that AI can provide educational benefits but may also create safeguarding, privacy and online-safety risks.

AI may be used to create or alter text, images, audio and video and can be used to impersonate individuals, facilitate bullying or harassment, create misleading or harmful content, or generate inappropriate or sexually explicit material.

The school will respond to AI-related safeguarding concerns in accordance with this policy, the Child Protection and Safeguarding Policy, Behaviour Policy and other relevant school procedures.

Particular attention will be given to:

- AI-generated or digitally altered images, including deepfakes and AI-generated nudes or semi-nude images;
- AI being used to bully, harass, threaten, impersonate or humiliate another person;
- pupils being exposed to harmful, inappropriate or age-inappropriate AI-generated content;
- pupils sharing personal, sensitive or identifying information with AI systems;
- inappropriate contact or interactions between pupils and AI applications;
- misinformation, disinformation and manipulated media;
- the use of AI to facilitate sexual harassment, abuse or exploitation.

Where a pupil or member of staff reports AI-generated or AI-manipulated harmful material, the school will consider the safeguarding implications and take appropriate action. Where the matter may constitute child-on-child abuse, sexual harassment, sexual violence or another safeguarding concern, it will be dealt with in accordance with the Child Protection and Safeguarding Policy.

The school will consider safeguarding, age appropriateness, data protection, security, filtering and monitoring before introducing pupil-facing generative AI tools. Staff must not introduce or require pupils to use new AI tools without appropriate school approval.

The school will provide age-appropriate education about AI, including its potential benefits and risks, as part of its wider digital literacy, safeguarding and online-safety provision.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 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. School devices should not be used to view, share, create or otherwise access terrorist or extremist material.

We will monitor the websites visited by pupils, staff, volunteers, proprietors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

Where filtering and monitoring involve the processing of personal data, the school will ensure that this is undertaken in accordance with applicable data protection legislation and the school's Data Protection Policy and Privacy Notices. Where appropriate, the school will undertake and maintain a Data Protection Impact Assessment (DPIA) relating to technical monitoring. Access to monitoring information will be restricted to authorised individuals and information will be retained only for as long as necessary.

More information is set out in the acceptable use agreements in appendices 1 to 3.

7.1 Filtering and monitoring

The school has appropriate filtering and monitoring systems in place on school-managed devices and networks to safeguard pupils from harmful and inappropriate online content and activity.

The school's filtering and monitoring arrangements will:

- block or restrict access to harmful and inappropriate content without unreasonably impacting teaching and learning;
- take account of the age and risk profile of pupils and the school's safeguarding needs;
- provide appropriate monitoring and alerting arrangements;
- allow safeguarding concerns and high-risk alerts to be escalated to the DSL without delay;
- be reviewed at least annually and following significant changes to technology, network configuration or safeguarding risks;
- be tested and reviewed to identify any weaknesses or inappropriate gaps in provision.

The school will maintain a documented record of its annual filtering and monitoring review, including identified risks, findings and actions.

The member of staff responsible for filtering and monitoring will work with the DSL and the school's IT provider to ensure that systems remain appropriate and effective.

All users of school IT systems will be informed that filtering and monitoring are in operation. Further information about the processing of personal data through filtering and monitoring is provided in the school's Privacy Notice and Data Protection Policy.

Where technical monitoring involves the processing of personal data, the school will consider and document the relevant data protection risks and will undertake a Data Protection Impact Assessment where appropriate.

Staff must report suspected failures or weaknesses in filtering and monitoring systems promptly to the DSL and the person responsible for IT systems.

8. Pupils using mobile devices in school

The school is a mobile-phone-free environment by default.

Pupils must not have access to or use mobile phones or other smart technology with similar communications, recording or notification functionality during the school day, including lessons, breaktimes, lunchtimes and periods between lessons.

Where a pupil needs to bring a mobile phone to school because of their journey to or from school or for another legitimate reason, the device must be switched off and handed into the school office on arrival, unless an alternative arrangement has been agreed in advance.

If a pupil is found to have a mobile phone or other prohibited smart technology during the school day, the device will be dealt with in accordance with the school's Mobile Phone Policy and Behaviour Policy.

The school will ensure that its approach to mobile phones and smart technology is applied consistently and takes account of pupils' individual needs and any reasonable adjustments required under the Equality Act 2010.

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
- 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 of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software as applicable
- 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 Advise Consulting.

10. How the school will respond to issues of misuse

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

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff conduct policy. 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). Training will include the school's filtering and monitoring arrangements, the identification and escalation of monitoring alerts, AI-related safeguarding risks, and the school's procedures for responding to harmful online content, including AI-generated or digitally manipulated images.

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

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

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

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 at least annually by the headteacher and shared with the proprietors. It will also be reviewed following any significant change in legislation, statutory guidance, technology, filtering or monitoring provision, or safeguarding risk.

Each annual review will be supported by a documented online-safety risk assessment which considers and reflects the risks pupils face online, including emerging risks associated with artificial intelligence, social media, online gaming, harmful content, online abuse and changes in technology. The annual review will also consider the effectiveness of the school's filtering and monitoring arrangements and any actions arising from incidents, monitoring reports or safeguarding concerns.

Appendix 1: KS1 acceptable use agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS

Name of pupil:

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

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

Signed (pupil):

Date:

Appendix 2: KS2 acceptable use agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS

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: to view terrorist or extremist material, 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 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 turn it off and hand it into the school office for safe keeping for the duration of the school day, in line with the school's policy of no mobile phones or devices in pupil's possession during school hours

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:

Appendix 3: acceptable use agreement (staff and volunteers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF AND VOLUNTEERS

Name of staff member/volunteer:

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
- This includes accessing school files/Sharepoint/Onedrive on personal laptops/devices
- Share my password with others or log in to the school's network using someone else's details
- View, share, create or otherwise access terrorist or extremist material
- 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 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/volunteer):

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

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