Grangefield School
Flying high. Spreading our wings.

Grangefield Primary School

Online Safety Policy

Last Review Date:	January 2026
Next Review Date:	January 2027

Contents

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, including AI-generated material such as deepfake images, misleading information and synthetic media, pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education 2024, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying
- Searching, screening and confiscation

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy also reflects the Online Safety Act 2023, which places duties on online service providers to reduce the risk of children encountering harmful content. While schools are not regulated by the Act, we recognise that pupils may still encounter risk online, and we maintain our responsibility to educate, safeguard and respond to online harm.

3. ROLES AND RESPONSIBILITIES

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

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

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those 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.

Monitoring systems will be used in a proportionate, risk-based way, in line with DfE guidance, balancing safeguarding needs with pupils' and staff members' rights to privacy

The governor who oversees online safety is Christine Hughes.

All governors 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 1)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions. At Grangefield School the head teacher is the DSL and the Deputy Head Teacher is a deputy DSL.

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
- Reviewing this policy annually and ensuring the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the IT support technician to make sure the appropriate systems and processes are in place
- Working with the IT support technician and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged on CPOMs or within staff personnel files 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 2 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The IT Support technician

The IT Support Technician is responsible for:

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

- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's IT systems on a termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (appendix 1A), and ensuring that pupils understand age appropriate rules on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing the DSL.
- Following the correct procedures by informing the DSL 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 on CPOMs, or within staff personnel files, and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Supporting their child with acceptable use of the school's ICT systems and internet

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 International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 1).

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

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

- In **Key Stage 1**, pupils will be taught to:
- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Pupils in **Key Stage 2** will be taught to:
- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- By the **end of primary school**, pupils will know:
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to recognise unreliable or AI-generated content, including images, videos and text that may appear real but are not.
- 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.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

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 via the school's website.

Online safety will also be covered during information evenings for parents.

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 classes.

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

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

When appropriate, the school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

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

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from a member of the SLT.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the authorised staff member, in conjunction with a member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, authorised staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

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

- **Not** view the image

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

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

Staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix 1). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Pupils will agree acceptable use rules at the start of each academic year, and any breach of these will be dealt with in line with the school behaviour policy.

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

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

More information is set out in the acceptable use agreements in appendix 1.

8. PUPILS USING MOBILE DEVICES IN SCHOOL

In Years 5 and 6, pupils may bring mobile devices into school for the sole purpose of having a form of contact in walking to and from school, but are not permitted to use them:

At any point during the school day

During Clubs before or after school, or any other activities organised by the school

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. STAFF USING WORK DEVICES OUTSIDE SCHOOL

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- All documentation and data linked to work is saved on the school network and is not stored locally on the laptop.
- 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 (IT technician in school)
- 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 1.

Work devices must be used as specified in the Acceptable User Agreement Policy (Appendix 1)

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

10. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in 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 which 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 Friday emails and staff meetings.

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

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages

    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
  - Training will also help staff:
  - Develop better awareness to assist in spotting the signs and symptoms of online abuse
  - Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
  - Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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

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. This is carried out via CPOMS (the schools online portal used for Safeguarding and behaviour within the school).

This policy will be reviewed every year by the HT/DSL. At every review, the policy will be shared with the governing board.

13. LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures and Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- Grangefield School Staff and Volunteer Acceptable User Policy Agreement (see Appendix 1)

APPENDIX 1: GRANGEFIELD SCHOOL ACCEPTABLE USE POLICY AGREEMENT (STAFF AND REGULAR VOLUNTEERS)

This policy has been written in collaboration with all staff employed by the school. Its aim is to safeguard staff against risks posed to themselves and to those in their care through digital technology. Because of the speed of emerging technology, the policy will be reviewed and signed annually by all school staff and those training within the school.

Access

- I will keep any school related user names and passwords confidential. (Please note that Head Teacher, Administrator and IT Technician know where log–in details and passwords can be found in case of absence. They will only be used in extenuating circumstances).
- If I believe other persons may have gained access to my log-in and password details, I will inform the IT subject leader and the person with responsibility for online safety so that they can be changed.

Content

- When on the school premises or using school equipment, I will not browse or download material that could be considered inappropriate or offensive to pupils, colleagues, parents or those from the wider school community.
- I will report any accidental access to illegal, inappropriate or harmful materials to the person responsible for online safety.
- I will not download any software or resources from the Internet that can compromise the network; or that are not adequately licensed.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I understand that Internet usage will be logged and this information could be made available to the Head Teacher on request.
- I accept that any laptop or IPAD loaned to me by the school; remains the property of the school and is provided to support my professional role but may also be used for responsible personal use. (The rules set out in this agreement also apply to use of school IT systems out of school).
- I will not use personal memory cards or camera phones to take or transfer images of pupils or colleagues.
- I agree not to download images of pupils and colleagues onto my personal equipment.
- I will only access and store sensitive/personal data and information on the school network, accessed through central hosting, and not on a local drive or memory stick.
- I will respect copyright and intellectual property rights whenever accessing online material.
- When I use my personal hand held/external devices (mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I will only use social networking sites in school when using a personal device and only during break times; when no pupils are present.
- I understand that this policy sits alongside the Online safety Policy which aims to educate about and protects the online safety of pupils, staff, volunteers and governors, within the school community.

Contact

- I will not send any communication to others within my professional community that could reasonably be considered offensive. This specifically includes, but is not exclusive to bullying and abuse.
- When communicating by e-mail on school business, I agree to only use the secure, county e-mail address, to ensure the protection of data and personal information.
- I will use the school office e-mail address or Class Dojo to communicate with parents and carers, not my personal or professional e-mail address.
- I agree to contact colleagues on their personal mobile phones only if they have given me prior permission to do so.
- When off-site, (for example on day visits and residential trips) I agree to contact parents/carers etc. using the trip site phone or school mobile phone if available, only using my personal one (with the number blocked) in an emergency.
- I understand that I should not contact parents or pupils using my mobile phone, or give them access to my personal mobile phone number, except in an emergency. (On occasions, there may be mitigating circumstances where parents are also friends and may be contacted through friendship – not professionally. In these circumstances, staff should discuss this with the Head Teacher and the details noted on page 3 of this agreement which will be kept securely in the school office. In the circumstance of it being the Head Teacher who has friends who are also parents, the head should inform the Governor with responsibility for online safety and the details noted in the same manner.)
- I agree that I will not make contact with pupils, parents or carers through a social networking site (or similar) and will ensure maximum security settings to prevent, as far as possible, pupils, parents and carers gaining access to my profile. (On occasions, there may be mitigating circumstances where parents are also friends and may be contacted through friendship – not professionally. In these circumstances, staff should discuss this with the Head Teacher and the details noted on page 3 of this agreement which will be kept securely in the school office. In the circumstance of it being the Head Teacher who has friends who are also parents, the head should inform the Governor with responsibility for online safety and the details noted in the same manner.)

Commerce

- I will not advertise or sell my services through digital technology connected in any way with the school.
- I will not access any gambling, auction or commercial sites during school working hours or in view of pupils, except in exceptional circumstances agreed by the Head Teacher. The Head Teacher will agree this with the relevant governor.
- I agree not to subscribe to any services, sites or goods on behalf of school without first asking for the permission of the relevant budget holder.

General

- I will not allow unauthorised individuals to access Email / Internet / Intranet etc.
- I will only use LA systems in accordance with any Corporate policies.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.

- I understand that family members and friends should not be allowed to use school equipment.
- I understand that I will be held responsible for any misuse of a laptop, or other school equipment issued to me.

Safeguarding

- If interacting with pupils on-line while working from home (Remote Learning), I will continue to follow existing school policies, with particular reference to Staff Code of Conduct, IT Acceptable Use Policy, Online safety Policy, the Safeguarding Policy and Annexes to the Safeguarding Policy (Covid 19 and Remote Learning), and to follow DFE guidance in Annex C of KCSiE.

Mitigating circumstances: (where the staff member is a parent at Grangefield who knows many parents in their child's class, indicate the year group and class of your child rather than each individual parents.)	
Please tick if you have discussed and/or recorded any "mitigating circumstances", as mentioned above, with the Head Teacher/Governor	

I agree to abide by the Grangefield School Acceptable Usage Policy.

Signed _____ Print name _____Date _____

2 copies of this AUP should be signed.

One copy to be retained by the member of staff, the second to be kept in the online safety file.

APPENDIX 1A: ACCEPTABLE USE AGREEMENT (STAFF, GOVERNORS, VOLUNTEERS AND VISITORS)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR GOVERNORS, VOLUNTEERS AND VISITORS

Name:

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

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

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 IT facilities and systems.

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

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's IT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (governor/volunteer/visitor):	**Date:**

APPENDIX 2: 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?	