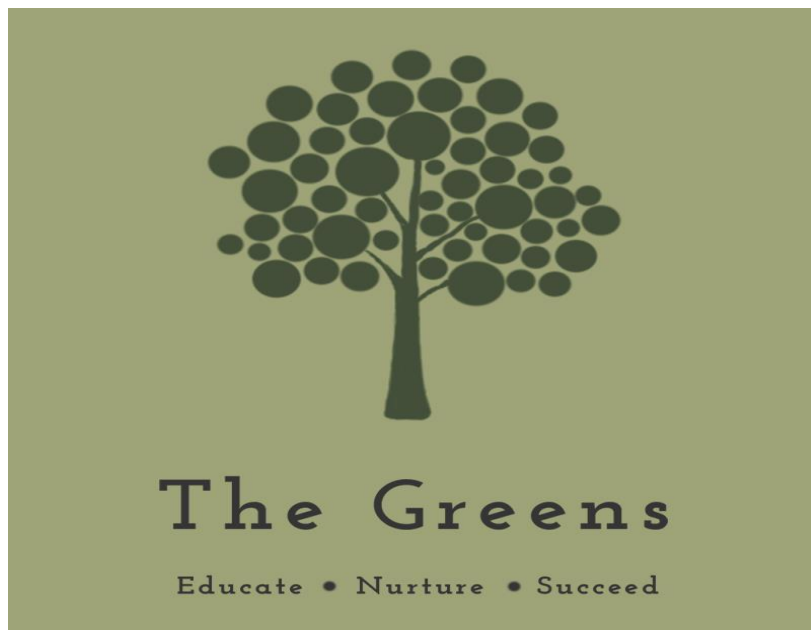


Online safety policy



Approved by:	Melanie Entwistle	Date: 01/03/2021
Last reviewed on:	01/04/2022. 05/03/2023 05/03/2024 01/02/2025 02/02/2026	
Next review due by:	01/02/2027	

Contents

1. Aims	2
---------------	---

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

1. Aims

Our school aims to:

- o Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors
- o Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- o Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

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

- o [Teaching online safety in schools](#)
- o [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- o Relationship and sex education (RSE) and health Education.
- o [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.

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 and requirements for training and monitor online safety logs as provided by Zena Bruder the designated safeguarding lead (DSL).

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that 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's 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:

- o Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- o Reviewing filtering and monitoring provisions at least annually
- o Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- o Having effective monitoring strategies in place that meet the school's safeguarding needs
- o The governor who oversees online safety is Louise Hodson.

All governors will:

- o Make sure they have read and understand this policy
- o Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- o Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- o Make sure 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 head of school 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 DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

- o Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- o Working with the headteacher and governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- o Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- o Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- o Working with the ICT manager to make sure the appropriate systems and processes are in place

- o Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- o Managing all online safety issues and incidents in line with the school's child protection policy
- o Responding to safeguarding concerns identified by filtering and monitoring
- o Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- o Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- o Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- o Liaising with other agencies and/or external services if necessary
- o Providing regular reports on online safety in school to the headteacher and/or governing board
- o Undertaking annual risk assessments that consider and reflect the risks pupils face
- o 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 ICT manager

The ICT manager is responsible for:

- o 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
- o Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- o Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- o Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- o Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- o Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy. This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- o Maintaining an understanding of this policy
- o Implementing this policy consistently
- o 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)
- o 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 reporting to the DSL/Headteacher
- o Following the correct procedures by reporting to the DSL/Headteacher if they need to bypass the filtering and monitoring systems for educational purposes
- o Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- o Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- o Notify a member of staff or the head of school of any concerns or queries regarding this policy
- o 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 can seek further guidance on keeping children safe online from the following organisations and websites:

- o What are the issues? - [UK Safer Internet Centre](#)
- o Hot topics - [Childnet International](#)
- o Parent factsheet - [Childnet International](#)
- o Healthy relationships – [Disrespect Nobody](#)

3.7 Visitors and members of the community

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

4. Educating pupils about online safety

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

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

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

- o Use technology safely and respectfully, keeping personal information private
- o 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:

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

By the end of primary school, pupils will know:

- o That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- o That people sometimes behave differently online, including by pretending to be someone they are not
- o That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others, including when we are anonymous
- o The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- o How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- o How information and data are shared and used online

- o How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- o What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- o How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- o The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- o Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- o How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- o Where and how to report concerns and get support with issues online

4.2 Pupils will be taught practical cyber security skills

This section is based on the DfE's [non-statutory cyber security standards for schools and colleges](#).

All pupils will receive age-appropriate training on safe internet use, including:

- o Methods that hackers use to trick people into disclosing personal information
- o Password security
- o Social engineering
- o The risks of removable storage devices (e.g. USBs)
- o Multi-factor authentication
- o How to report a cyber incident or attack
- o How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

5. Educating parents about online safety

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

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head of school

Concerns or queries about this policy can be raised with any member of staff or the head of school.

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 one 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/form teachers will discuss cyber-bullying with their tutor groups.

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

All staff, 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 so that 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 consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

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. 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 e.g. DPO/DSL, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

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

- o 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 the headteacher / DSL / appropriate staff member
- o Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- o 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:

- o Cause harm, and/or
- o Undermine the safe environment of the school or disrupt teaching, and/or

- o Commit an offence

If inappropriate material is found on the device, it is up to the headteacher with the DSL / other 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 whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

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

- o **Not** view the image
- o 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:

- o The DfE's latest guidance on [searching, screening and confiscation](#)
- o UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- o Our behaviour policy

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

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

The Greens ENS recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The Greens ENS will treat any use of AI to bully pupils very seriously, in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our AI usage policy.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

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

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- o Lessons
- o Tutor group time
- o Clubs before or after school, or any other activities organised by the school
- o Or any time during the school day

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

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.

Students are to hand in their Phones on arrival and will be given back to them at the end of the day.

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:

- o 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)
- o 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
- o Making sure the device locks if left inactive for a period
- o Not sharing the device among family or friends
- o Installing anti-virus and anti-spyware software
- o Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which 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 ICT manager.

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. 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 disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The school will consider whether incidents 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 emails, e-bulletins and staff meetings).

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

- o Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- o 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
- o Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- o Develop better awareness to assist in spotting the signs and symptoms of online abuse
- o Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- o 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 policy will be reviewed every year by the Head of school/ 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:

- o Child protection and safeguarding policy
- o Behaviour policy
- o Staff disciplinary procedures
- o Data protection policy and privacy notice

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

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

Name of pupil:

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

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

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I click on a website by mistake
- I receive messages from people I do not know
 - I find anything that may upset or harm me or my friends
- Use school computers for schoolwork only
- I will 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 do not follow the rules.

Signed (pupil):

Date:

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

Signed (parent/carer):

Date:

Appendix 2: KS2, KS3 and KS4 acceptable use agreement

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

Name of pupil:

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

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 username and passwords safe and not share these with others
- Always keep my confidential information safe 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 which might upset, distress or harm me or others
- Always log off or shut down a computer when I am finished working on it

I will not:

- Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.

Signed (pupil):

Date:

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

Signed (parent/carer):

Date:

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

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

Name of staff member/governor/volunteer/visitor:

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

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, or pornographic nature (or create, share, link to or send such material)
- Use them in any way 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 am not authorised to access, modify or share
- Promote private businesses, unless that business is 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 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 ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

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

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?	
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?	
Do you continually 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

