CARR MANOR COMMUNITY SCHOOL

ONLINE SAFETY POLICY

THIS POLICY APPLIES TO STAFF, PUPILS, PARENTS/CARERS AND GOVERNORS

Adopted by the Governing Body: October 2025
Revised: September 2026
Review Date: October 2027

TABLE OF CONTENTS

Online Safety Policy 1
1. Aims 3
2. Legislation and Guidance 3
3. Roles and Responsibilities 3
The Governing Board 3
3.1 The Principal 4
3.2 The Designated Safeguarding Lead 4
3.4 The school's safeguarding lead and technical lead 4
3.5 All staff and volunteers 5
Parents and Carers 5
3.6 Visitors and members of the community 5
4. Educating pupils about online safety 5
5. Educating parents/carers about online safety 7
6. Cyber-bullying 7
6.1 Definition 7
6.2 Preventing and addressing cyber-bullying 7
6.3 Examining electronic devices 8
7. Acceptable use of the internet in school 8
8. Pupils using mobile devices in school 8
9. Staff using work devices outside school 9
10. How the school will respond to issues of misuse 9
11. Training 9
12. Monitoring arrangements 10
13. Links with other policies 10
Appendices 11
Appendix 1: EYFS and KS1 Acceptable Use Agreement (pupils and parents/carers) 11
Appendix 2: KS2, KS3 and KS4 Acceptable Use Agreement (pupils and parents/carers) 12
Appendix 3: Acceptable Use Agreement (staff, governors, volunteers and visitors) 13
Appendix 4: online safety training needs – self audit for staff 14

DRAFT

1. Aims

Our school aims to:

- have processes in place to meet the online safety of all of its users.
- 'Users' include, but are not limited to:
    - Pupils
    - Staff
    - Governors
    - Third party support

To operate an effective Online Safety Policy which protects all users in the whole school community in its use of modern technology.

- Such smart technology may include:
    - Mobile phones
    - IPads and other tablets
    - Desktop computers and laptops
    - Other digital devices.

2. Legislation and Guidance

The guidance for this policy is based on the DfE statutory safeguarding guidance, Keeping Children Safe in Education 2026, and should be read alongside the Department for Education statutory guidance Mobile Phones in Schools (updated 29 June 2026).

Other DfE and statutory guidance relevant to this policy includes:

- https://www.gov.uk/government/publications/mobile-phones-in-schools/mobile-phones-in-schools
- https://www.gov.uk/guidance/data-protection-in-schools/the-data-use-and-access-act-2025
- https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard
- https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- https://www.gov.uk/government/publications/preventing-and-tackling-bullying
- https://www.gov.uk/government/publications/searching-screening-and-confiscation
- https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Education Act 2011, the Equality Act 2010, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and amendments made by the Data (Use and Access) Act 2025 (DUAA).

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

3. Roles and Responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

DRAFT

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).
The governor who oversees online safety is Jermaine Benjamin.

All governors will:

- Ensure they read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT system and internet.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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 Principal

The Principal 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 Safeguarding team are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Principal, technical lead 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 child protection policy.
- Ensuring that any online safety incidents are logged 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 Relationship and Inclusion Policy.
- Updating and delivering staff training on online safety, keeping a record of staff training.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or governing board.

This list is not intended to be exhaustive.

3.4 The school's Safeguarding Lead and Technical Lead

The Technical Lead is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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 a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

DRAFT

- Ensuring that any online safety incidents are logged 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's Inclusion and Relationships Policy.

The Safeguarding Lead is responsible for:

- Monitoring the compliance of this online safety policy, to ensure that all users including staff and pupils, adhere to the policy.
- To address concerns regarding inappropriate use or potential breaches of this policy.
- The Safeguarding Lead will be the primary point of contact for reporting and addressing such matters.
- Will provide and develop training needs to ensure all users are informed about acceptable use of technology and their potential risks, and importance of online safety.
- Collaborate with the relevant authorities to oversee the response to any incidents involving the misuse of technology or potential harm to individuals within the school community. We work with external agencies such as the police, or child protection organisations to address serious breach of online safety or instances of potential harm.
- Will participate in regular reviews of this Online Safety Policy. Providing insights and recommendation for updates based on emerging trends and potential risk to safeguarding.

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, including the school's mobile phone and personal smart-device expectations.
- Implementing this policy consistently and modelling appropriate use of personal mobile phones and smart technology around pupils.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged 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's Inclusion and Relationships 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'.

3.6 Parents and carers

Parents and carers are expected to:

- Notify a member of staff or the Principal 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 and carers can seek further guidance on keeping children safe online from the following organisations and websites:

- https://saferinternet.org.uk/guide-and-resource/what-are-the-issues
- https://www.childnet.com/help-and-advice/parents-and-carers
- https://www.childnet.com/resources/parents-and-carers-resource-sheet/
- https://www.disrespectnobody.co.uk/

DRAFT

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

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

Carr Manor Community School - Primary Phase

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 phase, 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.

Carr Manor Community School - Secondary Phase

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy and understanding the school's expectations for personal mobile phones and smart devices.
- Recognise inappropriate content, contact and conduct and know how to report concerns.

Pupils in Key Stage 4 will be taught:

DRAFT

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity, and the risks and benefits associated with personal smart devices and emerging technologies.
- How to report a range of concerns.

By the end of secondary phase, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse, harassment - including sexual, peer-on-peer abuse) and how to report or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

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 and 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.
Online safety will also be covered during MYCAT evenings and primary information events. If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.
Concerns or queries about this Policy can be raised with any member of staff or the Principal.

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 Inclusion and Relationships 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.

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.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Relationship and Inclusion 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

School staff may search pupils and their possessions, including electronic devices, where the legal requirements and the school's procedures for searching, screening and confiscation are met. Any search of an electronic device will be carried out in accordance with the latest DfE guidance and the school's Behaviour Policy, with safeguarding considerations applied where relevant.

Where a search of an electronic device is authorised, staff will follow the latest DfE guidance on searching, screening and confiscation. Staff will not access, copy, delete or retain content beyond what is permitted and necessary under the relevant guidance and school procedures.

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules.

If concerning, harmful or potentially illegal material is found on a device, staff will seek advice from the DSL or another appropriate senior member of staff and follow safeguarding, behaviour and police-reporting procedures as appropriate.

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline) and/or
- Report it to the police*.

* Devices may be confiscated and retained where permitted by the school's Behaviour Policy and the latest DfE searching, screening and confiscation guidance. Where there is a safeguarding concern, staff must follow the school's safeguarding procedures and seek advice from the DSL.

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

- The DfE's latest guidance on screening, searching 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.

DRAFT

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 1-3). 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 personal mobile phones and other personal smart devices into school where permitted by the school's Mobile Digital Technologies arrangements. Between 8:25am and 3:00pm, pupils must not use or have access to these devices, including during lessons, movement between lessons, breaktimes and lunchtimes. Devices must remain out of sight, silent and switched off unless an agreed exception applies.

- This includes mobile phones and other personal smart technology with similar functionality, such as devices capable of sending or receiving notifications or messages via mobile networks or recording audio or video.
- Any exception must be authorised by the school and must be based on an identified educational, medical, safeguarding, SEND/disability or other legitimate need, in line with the Mobile Digital Technologies policy.

Any agreed use or exception relating to personal mobile phones or smart devices must be in line with the Mobile Digital Technologies policy, the Behaviour Policy and the relevant acceptable use agreement.

Any breach of the Mobile Digital Technologies policy, Behaviour Policy or Acceptable Use Agreement may result in a proportionate response in line with the school's Behaviour Policy, including confiscation where permitted.

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).
- 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.
- Keeping operating systems up to date – always install the latest updates.
- Not accessing, or attempting to access any inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material).

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.

DRAFT

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 the technical team.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, or breaches the school's Mobile Digital Technologies expectations, we will follow the procedures set out in our policies. 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, the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct and the Guidance for Safer Working Practice. 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, and will follow safeguarding and information-sharing procedures where appropriate.

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 s afeguarding 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:

- Technology is a significant component in many safeguarding and wellbeing issues and children are at risk of online abuse. Staff will also be familiar with the school's mobile phone-free approach and the need to model appropriate use of personal smart devices.
- 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 do not 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 the risks up.
- 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 Safeguarding team will undertake child protection and safeguarding training, which will include online safety, at least every 3 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 records safeguarding issues related to online safety using CPOMS.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the Governing Body. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online, the effectiveness of filtering and monitoring, and any significant changes in technology, safeguarding practice or data-protection requirements.

13. Emerging technologies

13.1 Artificial Intelligence

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school is allowed. Such technologies include

- Generative Artificial Intelligence - (GenAI) are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Microsoft Co-Pilot
- AI and LLM (Large Language Models) technologies have the potential to enhance learning, support teaching, and streamline administrative tasks. However, it is essential to use these tools responsibly to ensure the safety and privacy of all users.
- The school 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 content created using AI to include someone's likeness.

13.2 AI Chatbots & Cyberbullying

- The school will treat any use of AI to bully pupils in line with the school's Inclusion and Relationships Policy.
- Staff should be aware of the risks of using AI tools whilst they are still being developed and should understand the level of risk where new AI tools are being used.
- Pupils should be aware of AI Chatbots or Virtual Friends. This is a computer program designed to have conversations and dialogue with users like a real person.
- Be aware that AI and LLM technologies may produce biased or inaccurate information. Always verify AI-generated content through reliable sources.
- Users are responsible for the content they generate with AI tools. Do not use AI to produce harmful, offensive, or inappropriate content.
- Do not use AI tools for bullying, harassment, or any form of misconduct. Report any incidents to the DSL or another appropriate member of the safeguarding team.

13.3 Training and Awareness

- Provide regular training for staff on the safe and effective use of AI and LLM technologies.
- Educate pupils on the benefits and risks of AI and LLM technologies, including responsible usage practices.
- Inform parents about the use of AI and LLM technologies in the school and involve them in discussions about eSafety.

14. Links with other policies

This Online Safety Policy is linked to our:

- Safeguarding and Child Protection Policy
- Relationship and Inclusion Policy
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable Use Agreements and filtering and monitoring procedures
- Mobile Digital Technologies policy
- Behaviour Policy

14.1 Filtering and monitoring systems in school:

In line with the expectations in KCSIE 2026 and the DfE filtering and monitoring core standard, the school has in place effective filtering and monitoring systems (Surf Protect and Classroom Cloud) to help ensure that pupils and staff remain safe online. Alerts from both systems are sent to:

- Safeguarding leads in the case of pupil alerts
- Principal/Vice Principal for all staff alerts.

Such alerts are followed up with individual pupils and staff, where appropriate, and are handled in accordance with safeguarding, data-protection and staff/pupil procedures. Filtering and monitoring arrangements are reviewed regularly for effectiveness, including appropriate testing, escalation and record keeping.

DRAFT

The school will ensure that filtering and monitoring arrangements are supported by appropriate data-protection documentation, including relevant privacy information, lawful-basis considerations, access controls, retention arrangements and data protection impact assessments where required.

Appendices

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

<table>
<tr><td colspan="2">ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS</td></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">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/Coach immediately if:
o I click on a website by mistake
o I receive messages from people I don't know
o I find anything that may upset or harm me or my friends
• Use school computers for schoolwork only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a member of staff 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 or Microsoft Teams
• 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.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

DRAFT

Appendix 2: KS2, KS3 and KS4 '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:

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
- 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 which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

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

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

- I will not use it 8:25am and 3pm. It will be kept switched off, silent and out of sight in lessons, around school, over breaktime and lunchtime.

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

Signed (pupil):	Date:

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

Signed (parent/carer):	Date:

DRAFT

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF MEMBER/GOVERNOR/VOLUNTEER/VISITOR	
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'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 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. I acknowledge that when utilising the school's wireless connection on a personal device, the browsing history or background application refresh of a smartphone or tablet application may remain active. This could potentially trigger a SurfProtect alert should the content be considered inappropriate.	
Signed (staff member/governor/volunteer/visitor):	Date:

DRAFT

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

Online Safety Training Needs Audit	
Name of staff/volunteer:	Date:
Questions	Yes/No
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?	
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?	

DRAFT