Oakley School

Skills for Life and Independence

Online Safety Policy

Date written: September 2025

Date agreed and ratified by Governing Body: 7th October 2025

Date of next review: September 2026

Appendices: 3

Key Contact Personnel in School

Designated Safeguarding Lead: Sophie Tillman-Harries

Deputy Designated Safeguarding Leads: Claire Bingham, Nicola Fosker

and Sophie Rees

Headteacher: Sam Perryman

Named Safeguarding Governor: Lizzie Bentley Bowers

Other key staff: Zoey Jenks, School Business Manager

This is a core policy that forms part of the induction for all staff. It is a requirement that all members of staff have access to this policy and acknowledge they have read and understood its contents.

This policy will be reviewed at least annually and/or following any updates to national and local guidance and procedures.

Contents

Contents		Page number
1.	Aims	3
2.	Legislation and guidance	3
3.	Roles and responsibilities	4
4.	Educating pupils about online safety	7
5.	Educating families about online safety	8
6.	Cyber-bullying	9
7.	Acceptable use of the internet in school	12
8.	Pupils using mobile devices in school	12
9.	Staff using work devices outside school	12
10.	How the school will respond to issues of misuse	13
11.	Training	13
12.	Monitoring arrangements	14
13.	Links with other policies	14
	Appendix 1	15
	Appendix 2	17
	Appendix 3	18

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, families, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism and misinformation, disinformation and conspiracy theories.
- **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 scam

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff
- Relationships and sex education
- 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.

This policy also reflects the Online Safety Act 2023, which places legal duties on online platforms to protect children from harmful content. While schools are not directly regulated by the Act, we play a vital role in educating pupils and families about online risks and reporting mechanisms. See Ofcom's guidance for parents for support.

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 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), Sophie Tillman-Harries.

In accordance with the Department for Education's Filtering and Monitoring Standards (2023), 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 and report incidents effectively.

The governor who oversees online safety is Lizzie Bentley Bowers, Chair of Governors.

All governors will:

- Ensure that 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 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school 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 and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT technician to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT technician, deputies 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 and safeguarding policy
- Ensuring that any online safety incidents are logged on CPOMS 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 pupil engagement, behaviour and wellbeing policy
- Updating and delivering staff training on online safety (Appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and / or governing board
- Undertaking annual risk assessments that consider and reflect the risks children and young people face
- 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 Technician

The ICT 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 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 schools ICT systems on at least a short termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the pupil engagement, behaviour and wellbeing policy

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 ICT systems and the internet (Appendix 2), and ensuring that pupils follow the school's terms on acceptable use (Appendix 1).
- 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 and processes failing by Smoothwall.
- Following the correct procedures by Smoothwall 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 and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the pupil engagement, behaviour and wellbeing 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 Families

Families are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child or young person has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendix 1)

Families can seek further guidance on keeping children and young people 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
- 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 2).

4. Educating pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum throughout the whole school to raise awareness and promote safe and responsible internet use amongst pupils.

Oakley School is aware that our pupils are considered to be more vulnerable online due to a range of factors. This includes, but not limited to children and young people in care, children and young people with SEND or mental health needs, children and young people with English as an additional language and children and young people experiencing trauma or loss.

Oakley School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils through lessons assemblies and by supporting parents.

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

As part of the Self-Regulation strand in Personal, Social, Emotional Development in the Oakley Learning Journey, where the focus is on stage and not age, pupils will:

Band 7:

- Understand basic e-safety rules, e.g. stranger danger, using appropriate language

Band 8:

- Follow basic e-safety rules and understands associated dangers with being online
- Know that they and others have the right to privacy, and who to talk to if we feel uncomfortable (online and offline)
- Explain and demonstrate how to ask for help and who to go to if they think they have made a mistake online (e.g. have created, provided or shared a photo or picture which they now regret)

Band 9:

- Describe specific ways of keeping themselves safe online, e.g. secure passwords, never giving out personal details/passwords, not lending mobile phone, covering a computer's camera when not in use

Band 10:

- Explain what is meant by the term 'explicit image/photo'
- Describe specific ways of keeping themselves safe online, e.g. secure passwords, never giving out personal details/passwords, not lending mobile phone, covering a computer's camera when not in use
- Explain that the sharing of explicit pictures/photos (e.g. forwarding a text or email, 'sharing' on social media) may be a serious criminal offence

- Explain that there are 'scams' (ways that people may try to trick us online); and identifies how they may be deceived e.g. phishing, fake email addresses
- Explain and demonstrate how to ask for help and who to go to if they think they have made a mistake online (e.g. have created, provided or shared a photo or picture which they now regret)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Teaching about safeguarding, including online safety, will be adapted for vulnerable children and young people or victims of abuse and pupils with SEND.

Online safety education at Oakley School supports pupils' mental wellbeing. Staff:

- Collaborate with mental health leads and pastoral teams
- Recognize signs of online-related distress and respond appropriately
- Promote safe digital habits as part of PSHE and RSE

The curriculum promotes digital resilience and critical thinking. Pupils learn to:

- Evaluate online content, manage risks and make safe choices
- Engage with resources such as Parent Zone's Everyday Digital to support learning and family engagement

5. Educating families about Online Safety

The school will raise family's awareness of internet safety in letters or other communications home, Family Workshops and in information via our website. This policy will also be shared with families.

Online safety will also be covered during pupil progress evenings.

The school will also let families know:

- What systems the school uses to filter and monitor online use
- What their children and young people are being asked to do online, including safe sites they will be asked to access and who from the school (if anyone) their child or young person will be interacting with online

If families 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.

Families and pupils are signposted to national resources for reporting concerns and accessing support:

- CEOP Safety Centre
- UK Safer Internet Centre
- Internet Watch Foundation
- Childnet
- NSPCC Online Safety

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 pupil engagement, behaviour and wellbeing policy).

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Personal, Social and Emotional Development in the Oakley Learning Journey, 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 families so that they are aware of the signs, how to report it and how they can support children and young people who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the behaviour, support and wellbeing 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 (as set out in the school's Child Protection and Safeguarding policy) 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 the headteacher and DSLs
- 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 pupils 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 'good reason' to do so.

When deciding whether there is '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 staff member in conjunction with the DSL or 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 if 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:

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

If a staff member **suspects** a device **may** contain an indecent image of a child or young person (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 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 screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's Pupil Engagement, Behaviour and Wellbeing policy / Child Protection and Safeguarding 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 artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and families may be familiar with generative chatbots such as ChatGPT and Google Bard.

Oakley 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.

Oakley School will treat any use of AI to bully pupils in line with our anti-bullying policy / behaviour, support and wellbeing policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of the internet in school

All pupils, families, 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 and 2). 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 and restrict access through filtering and monitoring systems where appropriate.

More information is set out in the acceptable use agreements in Appendices 1 and 2.

8. Pupils using mobile devices in school

Only young people in Phases 3 and 4 are allowed to carry their own mobile phones in school. Mobile phones are not permitted to be used during:

- Lessons
- Class time
- Lunch/break times
- Clubs before or after school, or any other activities organised by the school

If pupils bring their mobile phones to school they should be collected by the teacher, kept in a safe place and returned at the end of the day.
Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Appendix 1).

- Any breach of the acceptable use agreement by a pupil will trigger a meeting with the child or young person's family and in line with the school's pupil engagement, behaviour and wellbeing policy.

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 by always installing 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 2.

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 ICT Technician and DSL.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. 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 and Acceptable Use of Technology Policies (AUP). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

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 and young people are at risk of online abuse
- Children and young people 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

Staff are encouraged to use trauma-informed language in all safeguarding contexts. This includes:

  - Avoiding labels such as 'victim' or 'perpetrator' unless preferred by the child
  - Using terms that are age-appropriate, sensitive and respectful of individual experiences

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 on CPOMS.

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Pupil engagement, behaviour and wellbeing policy
- Anti-bullying Policy
- Staff disciplinary procedures
- Staff Code of Conduct and Acceptable Use of Technology Policies (AUP)
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Relationship Sex Education (RSE) and Personal Social Health Education (PSHE)

Appendix 1: Oakley Pupils and Families acceptable use agreement

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:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I select a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it
- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: 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 keep it in my school bag or hand it to the class team. I will not use it during lessons, 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

Please confirm you and have read and agree with this acceptable use policy by clicking here and completing the acceptance form.

Appendix 2: Staff, Governors, Volunteers and Visitors acceptable use agreement

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.

Please confirm you and have read and agree with this acceptable use policy by clicking here and completing the acceptance form.

Thank you

Appendix 3: 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?	