



ÉTABLISSEMENT
PARTENAIRE



aefe

Agence pour
l'enseignement français
à l'étranger

La Petite Ecole Française

73 Saint Charles Square

London W10 6EJ

Tel: 0208 960 1278

E-mail: admin@lapef.co.uk

Headteacher: Rebecca Stewart

Admin Head: Alix de Saint Quentin

Online Safety and Acceptable Use Policy

1. Introduction and Aims

Digital technologies are an important part of teaching, learning and communication at La Petite Ecole Française. The school uses technology to enrich learning, develop pupils' digital skills and support communication between the school and families.

Online safety encompasses the safe and responsible use of internet technologies, digital devices, communication platforms and online services. The school recognises the opportunities technology provides as well as the potential risks, and is committed to ensuring that pupils, staff and the wider school community are equipped with the knowledge, skills and understanding to use technology safely and responsibly.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and proprietor
- 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 school uses a range of digital devices, learning platforms and online resources to support teaching and learning, including tablets, computers, educational websites and communication platforms such as Educatable. These technologies are used to support learning, communication and the development of pupils' digital skills.

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, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes

Headteacher: Anthony Artist

Admin Head: Alix de Saint Quentin

Reviewed: RS/DM/ADS 24/09/26

- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education \(KCSIE\) 2026](#), and its advice for schools on: [Teaching online safety in schools](#), [Meeting digital and technology standards in schools and colleges](#), [Preventing and tackling bullying](#), [Relationships and sex education \(RSE\) and health education](#), and [Searching, screening and confiscation in schools](#).

It also refers to the DfE's [Prevent guidance on protecting children from radicalisation](#), and 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.

2. Roles and responsibilities

3.1 The Proprietor

The Proprietor has overall responsibility for ensuring that this Online Safety Policy is implemented effectively and for holding the Headteacher to account for its implementation.

The Proprietor will ensure that:

- online safety is recognised as an integral part of the school's safeguarding arrangements and is embedded across relevant policies, procedures and practice;
- appropriate resources, systems and support are available to enable the school to meet its online safety responsibilities;
- all staff receive appropriate online safety training as part of safeguarding and child protection training, including clear guidance on their roles and responsibilities relating to filtering and monitoring;
- pupils receive an age-appropriate online safety curriculum that is adapted, where necessary, to meet the needs of vulnerable pupils, pupils who have experienced abuse, and pupils with special educational needs and/or disabilities (SEND);
- effective filtering and monitoring systems are in place, regularly reviewed and support the school's safeguarding responsibilities.
- The Proprietor will ensure that the school reviews the Department for Education's filtering and monitoring standards and works with relevant IT providers to ensure that arrangements meet these standards. This includes ensuring that the school:
 - identifies and assigns clear roles and responsibilities for the management of filtering and monitoring systems;
 - reviews filtering and monitoring provision at least annually;
 - ensures that harmful and inappropriate content is blocked without unnecessarily restricting teaching and learning;

- has effective monitoring strategies in place that are proportionate and meet the school's safeguarding needs.

The Proprietor and any advisory governance body, where applicable, will:

- read and understand this policy;
- support and promote the school's approach to online safety;
- agree to and comply with the acceptable use requirements for the school's ICT systems and internet access (Appendix 2);
- ensure that online safety remains a continuous and interconnected element of the school's safeguarding approach;
- ensure that online safety education and safeguarding teaching are adapted where necessary to reflect the individual needs and circumstances of pupils.

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead (DSL)

The Headteacher is the school's Designated Safeguarding Lead (DSL). Details of the deputies are set out in our Safeguarding Children Policy as well as relevant job descriptions.

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

- Reviewing this policy annually and making sure 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
- Providing the Proprietor with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT provider to make sure the appropriate systems and processes are in place
- Working with the ICT provider and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 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 Proprietor
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

Headteacher: Anthony Artist
Admin Head: Alix de Saint Quentin
Reviewed: RS/DM/ADS 24/09/26

The school has identified the DSL as responsible for understanding and overseeing filtering and monitoring arrangements. The DSL works with the ICT provider to review the effectiveness of these systems and ensure that any concerns identified are appropriately investigated and addressed.

The school uses EXA SurfProtect filtering and monitoring services to support online safety. The system generates alerts where potentially harmful or inappropriate activity is identified. Alerts are reviewed by the DSL or an appropriately trained and authorised member of staff acting on their behalf, and concerns are assessed and managed in accordance with the Safeguarding Children Policy. The DSL works with the ICT provider where technical support or further investigation is required.

3.4 The ICT provider

The ICT provider supports the school by:

- 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 make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

The school maintains appropriate technical security measures, including malware protection, secure systems and support from external IT providers where required, to protect school systems, devices and data.

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 making sure 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
- Working with the DSL to make sure that any online safety incidents are logged on MyConcern and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

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

Parents should model safe and responsible online behaviour and avoid sharing images, information or comments about pupils, staff or the school without appropriate permission.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? <https://saferinternet.org.uk/guide-and-resource/what-are-the-issues>
- Help and advice for parents/carers <https://www.childnet.com/help-and-advice/parents-and-carers>
- Parents and carers resource sheet <https://www.childnet.com/resources/parents-and-carers-resource-sheet/>

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 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

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

Pupils are taught about online safety through the PSHE curriculum. Online safety education is delivered progressively from GS to CM2 and is adapted to be age appropriate. Online safety education includes helping pupils to evaluate online information critically, recognise misinformation and disinformation, understand persuasive techniques used online, make informed decisions about sharing information, recognise online risks and know how to seek help when they encounter something concerning.

Through the curriculum, pupils learn how to use technology safely, respectfully and responsibly; how to protect their personal information; how to recognise acceptable and unacceptable online behaviour; how to evaluate digital content critically; and how to seek help and report concerns about online content, contact or behaviour.

The school's PSHE curriculum is set out in the PSHE and RSE Policy which provides further detail on pupils' learning about online relationships, privacy, consent, online risks, harmful content and contact, social media, digital wellbeing and seeking support. The curriculum is reviewed annually and updated where necessary to reflect changes in technology, national guidance and emerging online risks. This includes ensuring pupils receive age-appropriate education about Artificial Intelligence (AI), deepfakes, misinformation and other developments that may affect their safety and wellbeing online.

4.2 Artificial Intelligence (AI)

The school recognises that Artificial Intelligence (AI) is becoming an increasingly common part of children's digital lives through search engines, educational platforms, apps and other online services. AI offers valuable opportunities for learning but also presents new risks that pupils need to understand.

Headteacher: Anthony Artist

Admin Head: Alix de Saint Quentin

Reviewed: RS/DM/ADS 24/09/26

As part of the school's online safety education, pupils will receive age-appropriate guidance to help them:

- understand that AI-generated information may not always be accurate, reliable or unbiased;
- recognise that AI-generated images, videos and audio (including "deepfakes") may appear real but can be misleading or false;
- understand the importance of not sharing personal, confidential or identifying information with AI tools or chatbots;
- think critically about information obtained from AI and other online sources;
- understand that AI should be used responsibly, ethically and respectfully;
- recognise that AI can sometimes generate inappropriate, harmful or offensive content and know how to report concerns to a trusted adult;
- understand that AI must never be used to bully, harass, impersonate or deceive others;
- understand that any use of AI to support learning should be undertaken only with the guidance of staff and in accordance with school expectations.

Staff will ensure that discussions about AI are appropriate to pupils' age and level of understanding and will adapt teaching as technology continues to develop.

4.3 Supporting pupils, including SEND

Pupils are encouraged to speak to a trusted adult if they experience or encounter anything online that makes them feel worried, uncomfortable or unsafe. Staff reinforce that the same expectations of respect, kindness and appropriate behaviour apply both online and offline.

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.

4.4 Pupils will be taught practical cyber security skills

Pupils receive age-appropriate teaching about cyber security through Computing and other relevant curriculum areas. This includes understanding how to protect personal information, use secure passwords, recognise online risks such as scams and attempts to obtain personal information, and report concerns or incidents.

Cyber security education is adapted according to pupils' age and understanding and is supported by the school's wider safeguarding and data protection procedures.

Online relationships, cyberbullying, digital wellbeing and responding to harmful online content or contact are covered through the school's PSHE and Relationships Education curriculum.

4.5 Email and digital communication

Pupils who are provided with school email accounts (CM1 and CM2) are taught how to use email safely and responsibly. They must only use school email accounts for approved educational purposes and must report inappropriate messages or content to a member of staff.

Pupils are taught to communicate respectfully online, protect their personal information, keep passwords secure and recognise risks associated with electronic communication, including inappropriate contact, phishing attempts and harmful content.

Pupils must not use school email accounts to create personal accounts on websites, apps or online services unless this has been specifically authorised by the school for educational purposes.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or Educartable. This policy will also be shared with parents/carers. The school may also provide information about online safety through parents' evenings, workshops, newsletters or other communications.

The school will let parents/carers know:

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

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

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

Where online platforms are used for communication or learning, access is managed appropriately and parents/carers are informed about the purpose of the platform and how it is used. Staff are responsible for ensuring that content shared through school platforms is appropriate and reflects the school's safeguarding expectations.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the Promotion of Good 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 encourage them 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 for CE1 to CM2 will discuss cyber-bullying with their classes during Personal, Social, Health and Economic education (PSHE) lessons and during assemblies.

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.

Headteacher: Anthony Artist

Admin Head: Alix de Saint Quentin

Reviewed: RS/DM/ADS 24/09/26

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

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

6.3 Examining electronic devices

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

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence
- Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
 - Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher
 - 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
 - Seek the pupil's co-operation

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

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

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

If inappropriate material is found on the device, it is up to the Headteacher 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:

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

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

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

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

La Petite Ecole Française 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.

La Petite Ecole Française will treat any use of AI to bully pupils very seriously, in line with our Anti-Bullying 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.

7. Acceptable use of the internet in school

Access to the internet and digital technologies is age-appropriate for GS to CM2 students and proportionate to pupils' developmental stage. Pupils use online resources under staff supervision and in accordance with the school's acceptable use expectations. Pupils are provided with clear expectations regarding the purpose of internet use and are taught to use online resources safely, responsibly and respectfully.

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 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.

The school uses filtering and monitoring systems to identify potentially harmful or inappropriate online activity. These systems may monitor internet usage by pupils, staff, volunteers, governors and visitors where relevant.

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

8. Pupils using mobile devices in school

In line with the Mobile Phones, Cameras and Recording Devices Policy, pupils must not bring mobile phones into school, and they are not allowed to wear smart watches or connected watches. If a pupil is found in possession of a mobile phone, the procedures set out in the Promotion of Good Behaviour Policy will be followed.

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
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in Appendix 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 Headteacher.

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 Promotion of Good Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's 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 and Grievance Procedure and 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training for staff, proprietor, governors and volunteers

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 are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and 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.

The Proprietor and any advisory governance body members will receive appropriate 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 in MyConcern. This includes concerns arising from online activity, filtering and monitoring alerts, cyber-bullying, inappropriate content or contact, and misuse of digital systems. Filtering and monitoring alerts are reviewed regularly, and appropriate actions are recorded where required.

13. Links with other policies

This Online Safety and Acceptable Use Policy is linked to our:

- Safeguarding Children Policy
- Promotion of Good Behaviour Policy
- Personal, Social, Health and Economic education (PSHE) and Relationships and Sex (RSE) Education policy
- Disciplinary and Grievance Procedure
- Code of Conduct
- Data protection Policy
- Privacy Policy
- Complaints Procedure

14. Policy Review

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the Proprietor. 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.

**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 this acceptable use agreement.

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

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: 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

I will not bring a personal mobile phone or other personal electronic device into school.

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:

**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 artificial intelligence tools responsibly and only in accordance with school guidance, ensuring that confidential information about pupils, families or staff is not entered into AI systems without approval.
- Use them in any way that could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- 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 that might upset, distress or harm them or others, and will also do so if I encounter any such material.

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

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

Date:

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?	