E-SAFETY POLICY

This is a whole school policy that applies to all sections of the School, including Early Years

Persons responsible for this policy:
Director of IT
Designated Safeguarding Lead

This policy was reviewed in:
Sept 2023

E-SAFETY POLICY

1. AIMS

Dulwich Prep London aims to:

- have robust processes in place to ensure the online safety of pupils, staff, volunteers and Governors;

- identify and support groups of pupils that are potentially at greater risk of harm online than others;

- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology; and

- 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 and extremism;

- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;

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

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. LEGISLATION AND GUIDANCE

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

- Teaching online safety in schools

- Preventing and tackling bullying and cyber-bullying: advice for Head Masters and school staff

- Searching, screening and confiscation

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education

Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3.   ROLES AND RESPONSIBILITIES

3.1.   The Governing Body

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

The Governing Body 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 Body will also make sure all staff receive regular online safety updates, as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (**DSL**).

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

The Governing Body 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 Governing Body will review the DfE filtering and monitoring standards, and will discuss with IT staff 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; and

●   having effective monitoring strategies in place that meet their safeguarding needs.

The Governor who oversees online safety is Henrietta Deasy in her role of the Safeguarding Governor.

All Governors will:

●   ensure they have read and understand this policy;

●   agree and adhere to the terms on acceptable use of the School's ICT systems and the internet (Appendix 3);

- ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures; and

- 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 Head Master

The Head Master 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 are set out in the School's Safeguarding (Child Protection) Policy, as well as relevant job descriptions.

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

- supporting the Head Master in ensuring that staff understand this policy and that it is being implemented consistently throughout the School;

- working with the Head Master and Governing Body 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 the School network;

- working with the Director of IT and the Network Manager to make sure the appropriate systems and processes are in place;

- working with the Head Master, Director of IT, the Network Manager 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 Safeguarding (Child Protection) Policy;

- ensuring that any online safety incidents are logged (see Appendix 5) 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's Behaviour, Rewards and Sanctions Policy;

- updating and delivering staff training on online safety;

- liaising with other agencies and/or external services if necessary;

- providing regular reports on online safety in school to the Head Master and/or Governing Body;

- undertaking annual risk assessments that consider and reflect the risks children face; and

- 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 Director of IT and the Network Manager

The Director of IT and the Network Manager are 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 School's ICT systems on a regular 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 (see Appendix 5) and dealt with appropriately in line with this policy; and

- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the School's Behaviour, Rewards and Sanctions Policy.

This list is not intended to be exhaustive.

3.5. All staff and volunteers

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

- 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 3), and ensuring that pupils follow the School's terms on acceptable use (Appendices 1 and 2);

- knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing. Staff are asked to email their concerns to the DSL;

- working with the DSL to ensure that any online safety incidents are logged (see Appendix 5) 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 Behaviour, Rewards and Sanctions Policy; and

- 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.

Staff will complete the self-audit set out in Appendix 4 at least annually.

3.6. Parents/carers

Parents/carers are expected to:

- notify a member of staff or the Head Master of any concerns or queries regarding this policy;

- for boys in Year 4 to Year 8 parents should ensure their child has read, understood and agreed to the terms on acceptable use of the School's ICT systems and internet (Appendix 2); and

- for pupils in Nursery to Year 3 parents should read and understand the terms on the acceptable use of the School's ICT systems and Internet and support their child accordingly.

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

- What are the issues? – UK Safer Internet Centre

- Hot topics – Childnet International

- Parent resource sheet – Childnet International

3.7. Visitors and members of the community

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

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

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

All schools have to teach:

- [Relationships education and health education](#) below Year 6.

- [Relationships and sex education and health education](#) Year 7 and above

In **Pre Prep (Years 1 & 2)**, pupils will be taught to:

- use technology safely and respectfully, keeping personal information private; and

- 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 **Lower and Middle School (Years 3 to 6),** will be taught to:

- use technology safely, respectfully and responsibly;

- recognise acceptable and unacceptable behaviour; and

- identify a range of ways to report concerns about content and contact.

By the **end of Year 6**, 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); and

- how to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

In **Upper School (Years 7 & 8)**, 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

- recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in **Senior School and above** will be taught:

- to understand how changes in technology affect safety, including new ways to protect their online privacy and identity; and

- how to report a range of concerns

By the **end of Year 11** 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 that 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 or harassment) and how to report, or find support, if they have been affected by those behaviours; and

- 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/CARERS ABOUT ONLINE SAFETY

The School will raise parents/carers' awareness of internet safety in mailings and in information via our school portal. This policy will also be shared with parents/carers.

The School will let parents/carers know:

- what systems the School uses to filter and monitor online use; and

- when appropriate, the School will inform parents 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 Head Master and/or the DSL.

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

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.

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. Form teachers or Life Skills teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Life Skills 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.

The School also sends information or has information on its website on cybersafety to parents/carers so they are aware of the signs and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the School will work to ensure the incident is contained. 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 Head Master, and any member of staff authorised to do so by the Head Master, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- poses a risk to staff or pupils;

- 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 Head Master / DSL / appropriate staff member

- explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it; and

- 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;

- 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 DSL / Head Master 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 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; and

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

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

- the DfE's latest guidance on searching, screening and confiscation;

- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people; and

- the School's Behaviour, Rewards and Sanctions Policy and the Searching Pupils Policy.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the School's Complaints Policy and Procedure.

7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils from Years 4 to 8, parents/carers of all pupils, 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 to 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in Appendices 1 to 3.

8. PUPILS USING MOBILE DEVICES AT SCHOOL

Pupils may bring mobile devices into school, but must be left in the trolley on entry to The Street. Mobile phones can be collected on leaving the school premises. Pupils are not permitted to use them during:

- lessons;

- tutor group time; or

- clubs before or after school, or any other activities organised by the School.

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

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the School's Behaviour, Rewards and Sanctions Policy, which may result in the confiscation of their device.

9. STAFF USING WORK DEVICES OUTSIDE SCHOOL

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

- keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);

- regularly changing passwords;

- the IT support team will ensure hard drives are 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 (this will be the responsibility of the IT Team); and

- keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way that would violate the School's terms of acceptable use, as set out in Appendix 3.

When in the presence of pupils 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 Director of IT or Network Manager.

10. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the School's ICT systems or internet, we will follow the procedures set out in the Behaviour, Rewards and Sanctions Policy and terms of 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. 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. An online Educare course on Cyber safety is regularly taken by all staff.

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 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:

    o abusive, harassing, and misogynistic messages;

    o non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups; or

    o sharing of abusive images and pornography, to those who don't want to receive such content; and

- 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; and

- 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 Deputy Designated Leads 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 Safeguarding (Child Protection) Policy.

12. MONITORING ARRANGEMENTS

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 5.

This policy will be reviewed every year by the Director of IT. At every review, the policy will be shared with the Governing Body. The review (such as the one available here) 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 E-Safety Policy is linked to our:

- Safeguarding (Child Protection) Policy;

- Behaviour, Rewards and Sanctions Policy;

- Staff disciplinary procedures;

- Data Protection Policy;

- Privacy Notice;

- Complaints Policy and Procedure;

- Mobile Phones Policy;

- Staff ICT and internet acceptable use policy; and

- Staff Social Media Policy.

APPENDIX 1: EYFS AND PRE-PREP ACCEPTABLE USE AGREEMENT

For pupils with confirmation and agreement from parents/carers

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

When I use the School's ICT systems and use the internet in School I will:
● Have permission from the teacher before using them
● Only use websites that a teacher or adult has told me or allowed me to use
● Tell my teacher immediately if:
  ▪ I click on a website by mistake
  ▪ I receive messages from people I don't know
  ▪ I find anything that may upset or harm me or my friends
● Use School devices for School work only
● Be kind to others and not upset or be rude to them
● Look after the School's 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 correct digital platform
● Not take images of others without their permission
● 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.

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.
Signed (parent/carer):   **Date:**

APPENDIX 2: YEARS 3 TO 8 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 this acceptable use agreement.

When I use the School's ICT systems and use 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 appropriate adult) immediately if I find any material which might upset, distress or harm me or others
- Save my work on the correct digital platform
- Always log off or shut down a computer when I've finished working on it
- If I have arrangements to print work I will check with my teacher before sending to print
- Ensure my iPad is ready and charged for the working day

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
- 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
- Take images of others without their permission
- 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 hand it in on arrival at School
- I will not use it during lessons, tutor group time, clubs or other activities organised by the School
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the School will monitor the websites I visit and that there will be consequences if I 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:**

APPENDIX 3: ACCEPTABLE USE AGREEMENT (STAFF, GOVERNORS, VOLUNTEERS AND VISITORS)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS
Name of staff member/Governor/volunteer/visitor:
When using the School's ICT systems and accessing the internet in School, or outside School on a work device (if applicable), I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● Use them in any way that could harm the School's reputation ● 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 asking their permission and ensuring I am aware of those pupils for whom permission for photographs has not been given by their parents ● 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
When in the presence of pupils I will only use the School's ICT systems and access the internet in school, for educational purposes. Outside school, when not in the presence of pupils and when using a work device, I will use the system for the purpose of fulfilling the duties of my role, or for limited personal use. 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 Director of IT or Network Manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the School's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
Signed (staff member/Governor/volunteer/visitor):	**Date:**

APPENDIX 4: ONLINE SAFETY TRAINING NEEDS – SELF-AUDIT FOR STAFF

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Comment**
Name of the person who has lead responsibility for online safety in school?	
Describe the ways pupils can abuse their peers online?	
What should you do if a pupil approaches you with a concern or issue?	
When did you last read the School's acceptable use agreement for staff, volunteers, Governors and visitors?	
When did you last read the School's acceptable use agreement for pupils and parents/carers?	
Can you describe (in simple terms) the filtering and monitoring systems on the School's devices and networks?	
What are your roles and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the School's ICT systems?	
What is the School's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

To be used annually with staff

APPENDIX 5: ONLINE SAFETY INCIDENT REPORT LOG

Case No	Date of Sanction	Name of Pupil involved	Section	Class	Staff adding	Nature of the incident	Action taken/ sanction given	Contact home	Follow up required	Date of Resolution