Online Safety

Policy date:	February 2024
This policy was developed by:	Madeleine Denyer
In consultation with:	Teaching Staff
This policy was approved by:	Safeguarding Governor on 19.03.24
Date of policy review:	February 2025

Contents:

1. Aims 1
2. Legislation and Guidance 2
3. Roles and Responsibilities..... 3
4. Educating Children about Online Safety 11
5. Educating Parents/Carers about Online Safety 11
6. Cyber-Bullying..... 12
7. Socal Networking..... 13
8. The School Website..... 13
9. Acceptable Use of the Internet in School..... 13
10. Staff using Work Devices Outside School 13
11. How the School will respond to Issues of Misuse 14
12. Training 14
13. Monitoring Arrangements 14
13. Appendix 1 – Children's Acceptable Use Policy 15
14. Appendix 2 – Parents/Carers Acceptable Use Policy 16
15. Appendix 3 – Staff Acceptable Use Policy 17
16. Appendix 4- Online Safety Contacts and References..... 18

Our Values and Creating an Online Safety Ethos

A holistic approach has been taken to writing the Online Safety Policy to ensure that safe practice for all members of the school community is embedded.

At Stanford Infant School we celebrate
friendship, respect, creativity and courage.
Our safe and happy learning environment
engages challenges and inspires our learners on the beginning
of a journey of learning forever.

'Exploring and Learning Together, Inspiring Each Other'

1. Aims

Stanford Infant School:

- Believes that online safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
- Identifies that the interne and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manager and respond to risk and be empowered to build resilience online.
- Has a duty to provide the community with quality internet access to raise education standards, promote achievement, support professional word of staff and enhance management functions.
- Identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of Stanford Infant School's online safety policy is to:

- Have robust processes in place to ensure the online safety of children, staff, volunteers and governors.
- Identify and support groups of children 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 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 has due regard to all relevant legislation and guidance and is based on the is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Keeping children safe in education 2023'
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

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.

The policy also takes into account the National Curriculum Computing Programmes of Study.

This policy operates in conjunction with the following school policies:

- Acceptable Use Agreements
- Anti-Bullying Policy
- Child Protection and Safeguarding Policy
- Data Protection Policy
- Positive Relationships and Behaviour Regulation Policy
- Social Media Policy
- Staff Code of Conduct
- Use of Images Policy

3. Roles and Responsibilities

3.1 The Governing Board

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

The Governing Board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
The Governing Board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
The Governing Board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

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

The Governing Board will:

- Ensure that there are appropriate filtering and monitoring systems in place

- Ensure that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

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 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 Head Teacher

The Head Teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Working with the Technical Consultant to make sure the appropriate systems and processes are in place

The Head Teacher will ensure that online safety is a running and interrelated theme throughout the school's policies and procedures, including those relating to the curriculum.

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's Designated Safeguarding lead (DSL) 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:

- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

- Working with the Head Teacher and Governing Board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Working with the Head Teacher, Technical Support Advisor 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 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 Anti-Bullying Policy.
- Updating and organising the delivery of 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 Teacher and/or Governing Board.
- 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 Technical Consultant

The Technical Support Advisor 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 children 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 weekly 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 and dealt with appropriately in line with this 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.
- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet **(Appendix 3)**, and ensuring that children follow the school's terms on acceptable use (Appendices 1 and 2).
- Knowing that the Head Teacher, alongside the Technical Support Advisor, is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing the Head Teacher or ICT Support immediately.
- Following the correct procedures 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 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 Anti-Bullying 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 The Designated Safeguarding Lead (DSL) & DDSL

Details of the school's Designated Safeguarding lead (DSL) and deputies are set out in our Child Protection and Safeguarding Policy, as well as relevant job descriptions.

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

- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the Head Teacher 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 Head Teacher to make sure the appropriate systems and processes are in place;
- Working with the Head Teacher, School's Technical Consultant 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 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 Anti-Bullying 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 Teacher and/or Governing Board;
- Undertaking annual risk assessments that consider and reflect the risks children 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.

3.7 The School's Technical Consultant

The School's Technical Consultant 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 children 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 weekly 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 and dealt with appropriately in line with this policy.

This list is not intended to be exhaustive.

3.8 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 children follow the school's terms on acceptable use (Appendix 1);
- Knowing that the School's Technical Consultant is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by contacting the ICT Service Desk;
- Following the correct procedures 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 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 Anti-Bullying 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.

3.9 Parents/Carers

Parents/carers are expected to:

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

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/Parent Resource Sheet – Childnet
- Keeping children safe online - NSPCC
- Help your children get the most out of the internet – Think U Know
- Because children deserve a safe digital world – Internet Matters

3.10 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 Children about Online Safety

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

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage (KS) 1**, children will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

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

Online safety teaching is always appropriate to children's ages and developmental stages.

Children are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours children learn through the curriculum include the following:

- How to evaluate what they see online.
- Acceptable and unacceptable online behaviour.
- How and when to seek support.

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 letters or other communications home, and in information via the Online Safety Page on our school website. This policy will also be shared with parents/carers.

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

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

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 Positive Relationships and Behaviour Regulation policy).

6.2 Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that children 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 children, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

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

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

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

6.4 Artificial Intelligence (AI)

The school will take steps to prepare children for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration to the children's age.

Generative artificial intelligence (AI) tools are now widespread and easy to access.

7. Social Networking

The use of Social Media by staff and children will be managed in line with the school's Social Media Policy.

8. The School Website

The Head Teacher will be responsible for the overall content of the School Website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

9. Acceptable Use of the Internet in School

All 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).

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.

10. 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 that would violate the school's terms of acceptable use, as set out in Appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the school's Technical Support Advisor.

11. How the School will respond to Issues of Misuse

Where a child misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Positive Relationships and Behaviour Regulation, Anti-Bullying and Children's Acceptable Use Policies. 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 Code of Conduct and Acceptable Use Policy. 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.

12. 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 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 children can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence children to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL 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.

13. Monitoring Arrangements

This policy will be reviewed annually by the Head Teacher. At every review, the policy will be shared with the Governing Board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks children face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Any changes made to this policy are communicated to all members of the school community.

Appendix 1 – Children's Acceptable Use

Follow the **SMART** rules to keep safe online:

S - SAFE: Keep safe by being careful not to give out personal information to people, including your full name, address and phone number.

M - MEETING: Meeting someone you have only been in touch with online can be dangerous, you should never meet up with someone you have met online.

A - ACCEPTING: Accepting emails and instant messages or opening files, pictures or texts from people you don't know or trust can lead to problems, they may contain dangerous viruses. If you are not sure about something you have received, delete it and then find a grown up you trust and tell them.

R - RELIABLE: Remember that information you find on the internet may not be true, and that someone you are talking to online may be lying about who they are.

T - TELL: Tell your home grown-ups or a trusted adult if someone or something makes you feel uncomfortable or worried online. Examples of trusted adults could be your teacher or your Head Teacher.

Appendix 2 – Parents/Carers Acceptable Use

Online channels are an important way for parents/carers to communicate with, or about, our school. Our ongoing aim is to work in partnership with our families. We developed a 'Code of Conduct' to set out clear guidelines for how we expect parents/carers to conduct themselves on social media and when using messenger apps, such as WhatsApp. This is so we can continue to work together in an atmosphere of open collaboration and mutual understanding.

The school uses the following channels:

- Email direct from the School Office.
- We use 'SchoolPing' for all of our school information and announcements.
- We use a system called 'Classlist' to enable our families to communicate easily with each other. 'Classlist's' system offers high levels of security and privacy and is designed to comply fully with the new data protection regulations.
  More information is available at www.classlist.com, including the Privacy Notice, which explains how personal information is managed and protected.
  Classlist will enable you to contact other parents/carers safely and securely and to keep up to date with events organised by the Parent, Teacher and Friends Association (PTFA). All requests to join Classlist will be approved by the school or Class Reps before they are validated.
  We expect 'Classlist' to negate the use of other social media apps when discussing anything related to Stanford Infant School.

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, chats through WhatsApp.

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups or personal social media to complain about or criticise members of staff. This is not constructive and the school cannot improve or address issues unless they are raised in an appropriate way.
- Use private groups or personal social media to complain about, or try to resolve, a behaviour issue involving other children. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident.
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers.

Appendix 3 – Staff Acceptable Use

Stanford Infant School
Staff Acceptable Use Policy

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for children's learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that children receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications;
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, etc) out of school, and to the transfer of personal data (digital or paper based) out of school;

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school;
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it;
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission;
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions;
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the School Website) it will not be possible to identify by name, or other personal information, those who are featured;
- I will not use chat or social networking sites in school in accordance with the school's policies;
- I will only communicate with children and parents/carers using official school systems. Any such communication will be professional in tone and manner. Staff must not use their personal email addresses / mobile phones / social networking sites for such communications;
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses;
- I will not use personal email addresses on the school ICT systems;
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes);

- I will ensure that my data is regularly backed up, in accordance with relevant school policies;
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials;
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work;
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies;
- I will not disable or cause any damage to school equipment, or the equipment belonging to others;
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. OneDrive must be used to view digital personal data outside of the local network. Paper based Protected and rrestricted data must be held in lockable storage;
- I understand that the data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority;
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work;
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school;
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Appendix 4 – Online Safety Contacts and References

There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Brighton and Hove Support and Guidance
BHCC Local Safeguarding Children Board (LSCB)
https://www.bhscp.org.uk/

National Links and Resources

Action Fraud: www.actionfraud.police.uk
BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre):
www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Common Sense Media: https://www.commonsensemedia.org/

Educate Against Hate: https://www.educateagainsthate.com/

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

London Grid for Learning LGfL: https://lgfl.net/

Lucy Faithfull Foundation: www.lucyfaithfull.org

My Family's Digital Toolkit:
My Family's Digital Toolkit - tailored online safety advice | Internet Matters
The charity produces a wealth of practical information and guidance on keeping children and young people safer online across four age ranges from 0-4 yrs to 14+ with guidance on, for instance, setting controls for devices and platforms.

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Zone: https://parentzone.org.uk/

Professional Online Safety Helpline:
www.saferinternet.org.uk/about/helpline

PSHE Association: https://pshe-association.org.uk/

SWGfL Safe, Secure Online: https://swgfl.org.uk/

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

The Use of Social Media for Online Radicalisation:
https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Think U Know: www.thinkuknow.co.uk

UK Council for Child Internet Safety (UKCCIS):
https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: https://360safe.org.uk/