Applecroft School

Online Safety Policy

Person Responsible:	Lead DSL
Review Cycle:	Annual
Date of Issue:	September 2025
Review Date:	September 2026

Online Safety Policy

1) Introduction:

School Vision:

'To create a positive and inspiring community that nurtures each individual and empowers leaders for life'.

School Mission Statement:

'Nurturing Potential, Inspiring Minds, Changing Lives'.

School Values:

- Ambition and Leadership
- Kindness and Supportiveness
- Respect and Honesty
- Determination and Resilience.

2) Aims:

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees
- 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, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

3) 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 headteachers 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.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

4) Roles and Responsibilities:

4.1 The Board of Trustees

The Board of Trustees has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Board of Trustees will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding leads (DSL).

The trustee who oversees online safety is Ben Kirby, who oversees all areas of safeguarding.

All trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 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

4.2 The Headteacher

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

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, IT Admin Assistant, other staff and SITSS as necessary, to address any online safety issues or incidents

- Reviewing the alerts provided by Senso, the school's monitoring software, and following up all relevant alerts with children, parents, staff and lettings as necessary
- Managing all online safety issues and incidents in line with the school Child Protection policy
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour & Discipline policy
- Updating and delivering staff training on online safety (Appendix 5 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or Board of Trustees.

This list is not intended to be exhaustive.

4.4 The Management of ICT:

The management of ICT in the school is conducted by an external service provider called SITSS. They are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems (Senso), which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

4.5 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)
- Working with the DSLs to ensure that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's Behaviour & Discipline policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it does happen here'

This list is not intended to be exhaustive.

4.6 Parents/Carers:

Parents/carers are expected to:

- Notify a DSL or the Headteacher of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendices 1 or 2)
- 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

4.7 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).

5) Educating pupils about online safety:

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

In the **Early Years Foundation Stage (EYFS)**, pupils will be taught:

- Ways in which the Internet can be used to communicate
- Recognise how people can be unkind online
- Recognise who personal information can be shared with

In **Key Stage 1**, pupils will be taught to:

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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

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

The safe use of 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.

6) Educating parents/carers about online safety:

The school will raise parents and carers awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

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

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

7) Cyber-Bullying:

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's Behaviour & Discipline policy.)

7.2 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. Staff will discuss cyber-bullying with their class.

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

All staff, trustees 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 details).

The school also signposts information on cyber-bullying to parents/carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour & Discipline 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.

7.3 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 a DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation.

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 staff member in conjunction with the DSL / 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 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
- 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 Behaviour and Discipline 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.

8) Acceptable use of the Internet in school:

All pupils, parents/carers, staff, volunteers and trustees 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, trustees, lettings and visitors (where relevant) to ensure they comply with the above.

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

9) Pupils using mobile devices in school:

Mobile Phones/Devices:

Pupils are allowed to bring personal mobile devices/phones to school if they are independent travellers (Y5 or Y6) but must not use them for personal reasons within the school day.

At the beginning of school, Year 5/6 pupils who have a mobile phone must immediately turn them off, hand them in to their class teacher and sign in a book that they have handed them in. They can then collect their phone and sign it out when leaving school at the end of the day. Under no circumstances are pupils permitted to use their mobile devices during the school day or to take images of:

- any other pupil unless they and their parents/carers have given agreement in advance
- any member of staff
- any part of the school building.

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.

Smart Watches:

Pupils can wear smart watches during the school day providing they are only being used as a normal watch and for no other function beyond telling the time. Any camera, messaging, telephone call services and internet connectivity must be disabled whilst in school.

Tracking Devices:

Tracking devices, such as Air Tags or equivalent, are permitted in school each day only for pupils in Years 5 or 6 who are independent travellers e.g., attached to a child's bag. However, audible alerts are not permitted during the school day.

Tracking devices are NOT permitted on residential trips. If a child is sent with one and a staff member becomes aware, they will remove the tracking device and store it in their room for the duration of the trip. The staff member will then return the device to the parent/carer of the child on return from the trip.

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)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates
- Ensuring they fully shut down and re-open their devices a minimum of once a week to ensure any necessary updates are installed.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

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 Finance & Business Manager, who can refer them onto the external service provider.

11) 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 Behaviour & Discipline 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 Code of Conduct Policy in the first instance. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

12) Training:

All new staff members will receive Online Safety training as part of their induction, as well as Child Protection and Prevent.

All staff members will receive Online Safety refresher training at least annually as part of their safeguarding training, as well as relevant updates as and when required for example through emails, briefings 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, 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.

Our DSLs will complete Designated Safeguarding Lead training when taking up the post and then refresher training at least every 2 years. They will also complete annual Online Safety training and Safeguarding training. They will also update their knowledge and skills on the subject of Online Safety and Safeguarding at regular intervals in addition.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training annually.

Volunteers will receive appropriate training and updates as part of our school's annual Volunteer Meeting.

More information about safeguarding training is set out in our Child Protection policy.

13) Monitoring arrangements:

At Applecroft School, we have deployed (via SITSS) monitoring software called Senso on all staff and pupil Window and Chromebook devices. This software monitors all keystrokes, software used and website visited and immediately alerts all DSLs of any violation. These alerts are monitored by the DSL team and followed up as necessary with children, parents, staff and lettings and recorded on CPOMS for pupils and StaffSafe for staff, where relevant.

This policy will be reviewed annually by the Lead DSL. This is important because technology, and the risks and harms related to it, evolve and change rapidly. At every review, the policy will be shared with the trustees.

14) Links with other policies:

This Online Safety policy is linked to our:

- Anti-Bullying policy
- Behaviour and Discipline policy
- Child Protection policy
- Complaints procedure
- Computing policy
- Data Protection policy and privacy notices
- Home-school agreement
- Safeguarding policy
- Staff disciplinary policy and procedures
- Staff Code of Conduct Policy

Appendix 1:

EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the school's IT systems (e.g., Chromebooks, tablets and computers) and access the Internet in school I will: ● Ask a teacher or adult if I can do so before using any device ● Only use websites that a teacher or adult has told me to 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 accounts (e.g., Google documents) and devices for schoolwork only ● Be kind to others and not upset or be rude and/or disrespectful ● Look after the school's IT equipment and tell a teacher straight away if something is broken or not working properly ● Only use the username and password I have been given ● Try my hardest to remember my username and password ● Never share my password with anyone, including my friends ● Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer ● Save my work on the school network ● Check with my teacher before I print anything ● Log off or shut down a computer when I have finished using it **I agree that the school will monitor what I input into devices, the software I use and the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's IT systems, devices and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above and, in the school's, Online Safety policy for pupils using the school's IT systems and internet and will make sure my child understands these. I understand that the school's Senso software will monitor what my child inputs into devices, the software they use and the websites they visit. If we/I permit my child to wear a Smart Watch to school, we will ensure that 'school mode' is activated or all functions except the clock function will be disabled for the duration of the school day. We/I understand that tracking devices e.g., Air Tags are not permitted on any school trip including residential trips and that a staff member will remove these from a pupil if they are found.	
Signed (parent/carer):	**Date:**

Appendix 2:

KS2 acceptable use agreement (pupils and parents/carers)

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

I will read and follow the rules in this acceptable use agreement policy.

When I use the school's IT systems (e.g., Chromebooks, tablets and computers) and access the internet in school I will:

- Always use the school's IT systems and the internet responsibly and for educational purposes only
- Only use them when a staff member is present, or with a staff member's permission
- Use school accounts (e.g., Google documents) and devices for schoolwork only
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Check with my teacher before I print anything
- Always log off or shut down a computer when I've finished working on it
- If bringing a Smartwatch to school, I will ensure it is only used as a watch and for no other function beyond telling the time. Any camera, messaging, telephone call services and internet connectivity will be disabled whilst in school and/or 'school mode' activated.

For children who are independent travellers in Years 5 and 6 only:

- If bringing a mobile device from home into school e.g., mobile phone, I will ensure this is switched off at all times when on school premises and will follow the school rules regarding this

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 posts on Google Classroom
- Create, link to, or post any material that is offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Access/use anyone else's files, account, device without a teacher's or staff member's permission
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Download and use any social networking sites with an age rating above my chronological age
- Bring a tracking device on any daily school trips including residential trips

I agree that the school will monitor what I input into devices, the software I use and the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Parent/carer's agreement: I agree that my child can use the school's IT 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 IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. I will supervise my child's use of the internet and ensure that they do not download and use any social networking sites with an age rating above their chronological age. I understand that the school's Senso software will monitor what my child inputs into devices, the software they use and the websites they visit. We/I understand that tracking devices e.g., Air Tags are not permitted on any school trip including residential trips and that a staff member will remove these from a pupil if they are found. If we/I permit my child to wear a Smart Watch to school, we will ensure that 'school mode' is activated or all functions except the clock function will be disabled for the duration of the school day.	
Signed (parent/carer):	**Date:**

Appendix 3:

Acceptable Use Agreement (staff, trustees, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET:
AGREEMENT FOR STAFF, TRUSTEES, VOLUNTEERS AND VISITORS

Name of staff member/trustee/volunteer/visitor:

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety. When using the school's IT systems and accessing the Internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms for personal use on any device during the school day or whilst on the school site
- 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
- Give out my personal details such as mobile phone number, email address and social media account details to pupils
- Use school equipment to access the internet for non-school purposes outside of the school building without the prior approval from my Headteacher
- Use the internet to free surf in front of pupils
- Share my password with others or log in to the school's network using someone else's details
- I will not take images, sound recordings or videos of pupils or wider school activities on any personal device
- I will not take images, sound recordings or video of pupils or wider school activities on a school device without permission from the Headteacher
- I understand I may only use my personal mobile phone and other devices, with camera functions in designated areas. When not in a designated are, phones must be on silent or switched off and out of sight. Any exception must be pre-arranged with the Headteacher
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I am 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 IT 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 IT 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
- If working in a classroom, I will pre-check for appropriateness all internet sites I intend to use including the acceptability of other material visible on the site. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school
- I will let the designated safeguarding lead (DSL) and Headteacher 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 raise any safeguarding concerns from my visit immediately with the Lead DSL or Headteacher
- I will always use the school's IT systems and internet responsibly and ensure that pupils in my care do so too
- I understand that the school's Senso software is installed on all Windows and Chromebook devices and that this will monitor all keystrokes I input, all software I use and all websites I visit and will alert all DSLs should a violation occur. I understand this monitoring extends to my emails, online training, and documents
- If wearing a smart watch, I will ensure this is on silent and that I only use the clock/watch facility when on site i.e., not use the message, camera, phone facilities unless in a designated area.

Signed (staff member/trustee/volunteer/visitor):	**Date:**

Appendix 4:

Acceptable Use Agreement (Peripatetic Teachers, Coaches and Supply Teachers)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET:

AGREEMENT FOR PERIPATETIC TEACHERS, COACHES AND SUPPLY TEACHERS

Name of Peripatetic Teacher, Coach, Supply Teacher:

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record. Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff/adults are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the Headteacher. Breaches will be investigated, recorded and where appropriate, disciplinary procedures will apply, and police involvement will be sought.

The school's Online Safety policy and Child Protection policy will provide further detailed information as required.

When using the school's IT systems and accessing the Internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms for personal use on any device during the school day or whilst on the school site
- 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
- Use school equipment to access the internet outside of school without the prior approval from my Headteacher
- Use the internet to free surf in front of pupils
- Share my password with others or log in to the school's network using someone else's details
- I will not take images, sound recordings or videos of pupils or wider school activities on any personal device
- I will not take images, sound recordings or video of pupils or wider school activities on a school device without permission from the Headteacher
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I am not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school
- I will not give out my personal contact and online account information such as phone numbers, email address, and social media account to pupils and/or parents/carers. Should I need to share my professional details, such as mobile number or email address, with parent/carers, this must be agreed in advance as acceptable approach with the Headteacher or Deputy Headteacher
- In my professional role in school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites
- I will not upload any material about or references to the school or its community on my personal social networks
- I will not use my professional email address for personal matters
- I understand I may only use my personal mobile phone and other devices, with camera functions in designated areas. When not in a designated are, phones must be on silent or switched off and out of sight. Any exception must be pre-arranged with the Headteacher
- If wearing a smart watch, I will ensure this is on silent and that I only use the clock/watch facility when on site i.e., not use the message, camera, phone facilities unless in a designated area.
- I will not use personal devices in front of pupils and will only use approved personal devices in designated areas

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET:

AGREEMENT FOR PERIPATETIC TEACHERS, COACHES AND SUPPLY TEACHERS

- I will only use the school's IT 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) 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 IT systems and internet responsibly, and ensure that pupils in my care do so too
- I will report an accidental access to or receipt of inappropriate materials or filtering breach to the Lead DSL or Headteacher
- My private account postings will never undermine or disparage the school, its staff, trustees, parents/carers or pupils. Privileged information known as a result of my work in the school I will keep confidential
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.
- I will only upload images or videos of staff, pupils or parent/carers onto school approved sites where specific permission has been granted
- I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices
- I will only use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act
- I understand that online safety is part of my responsibility, and I will promote positive online safety messages at all times, including when setting home learning, rehearsal or skill practice or when providing pastoral support
- I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, trustees, visitors, pupils or parent/carers) which I believe may be inappropriate or concerning in any way to the Headteacher
- If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the Headteacher. I will pre-check for appropriateness all internet sites used in the classroom ahead of accessing this in front of children, this will include the acceptability of other material visible, however briefly on the site
- I understand that the school's Senso software is installed on all Windows and Chromebook devices and that this will monitor all keystrokes I input, all software I use and all websites I visit and will alert all DSLs should a violation occur. I understand this monitoring extends to my emails, training and documents.

Signed (Peripatetic Teacher, Coach, Supply Teacher):	**Date:**

Appendix 5:

Online Safety Training Needs Self-Audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of Staff Member:	**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, trustees and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Do you regularly change your password for accessing the school's IT 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?	