Online Safety Policy

Review Due:	**September 2025**
Introduced:	September 2023
Applicable to:	All Trust Schools
Reviewed By:	NH
Approved By:	CEO
Date of Approval:	September 2024

Comments:

This is an updated statutory policy which reflects the changes to regulation within the government's 'Keeping Children Safe in Education 2024' document.

All staff working directly with children are expected to read at least part 1 of KCSIE (those who don't work directly with children can read the condensed version of part 1 in Annex A).

This policy sets out our approach to supporting online safety in schools across The Partnership Trust. This policy supersedes school level policies from October 2023. Schools are required to personalise this policy at Appendix 2 (contact details)

Contents

1	Aims	3
2	Legislation	3
3	Roles and Responsibilities	3
4	Educating pupils about online safety	6
5	Educating parents/carers about online safety	7
6	Cyber bullying	7
7	Acceptable use of the internet in school	8
8	Pupils using mobile devices in school	8
9	Staff using work devices outside school	8
10	How the school will respond to issues of misuse	9
11	Continuous professional development	9
12	Approval and monitoring	10
13	Links with other policies	10
	Appendix 1 – Bring your own device policy (BYOD)	11
	Appendix 2 – Key contacts	13

1. Aims

The Partnership Trust aims for all schools to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- 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/data 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 headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to:

- Education Act 1996 (as amended)
- Education and Inspections Act 2006
- Equality Act 2010
- Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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

3. Roles and responsibilities

3.1 The Board of Trustees and Local Governing Body (LGB)

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

Responsibility for ensuring that this policy is implemented is delegated to the CEO and school's Headteacher.

The monitoring of online safety will form part of the safeguarding governor's role and will form part of the monitoring meetings with the school's DSL. All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety[1], which includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring, 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
    - pupils with special educational needs and/or disabilities (SEND).

The Partnership Trust recognises that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

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

3.3 The designated safeguarding lead (DSL)

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, network manager (or equivalent), subject leader and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged 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 policy
- Updating and delivering staff training on online safety as part of safeguarding training (see paragraph 11 for additional information on continuing professional development)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher, LGB or Trust Board

This list is not intended to be exhaustive.

3.4 School Network manager

[1] Within this document all references to online safety can be taken to also include an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring

The School's Headteacher is responsible for ensuring that the School's IT network manager (this role may be fulfilled by an external support company) is aware of their following responsibilities under this policy:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, 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[2]
- 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 or incidents of cyber-bullying are reported to the school's Headteacher or DSL

This list is not intended to be exhaustive.

3.5 All staff[3]

All staff, 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 and ensuring that pupils follow the school's terms on acceptable use
- 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 behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents[4]

Parents are expected to:

- Notify a member of staff 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
- Support the school in managing the appropriate use of devices in schools – this may include supporting pupils being unable to bring devices to school

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

[2] including terrorist and extremist material
[3] including contractors, agency staff, and volunteers
[4] Including carers of families

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

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

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

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

Pupils in **KS3** will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **KS4 and KS5** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, 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
- 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)

5. Educating parents about online safety

The school will raise parents' awareness of online safety in newsletters or other communications home, and in information via school websites. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings and events to promote and encourage online safety at home.

The school will let parents know:

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

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

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes in an age appropriate manner.

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, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents 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 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. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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 may monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements can be found In Appendix 3

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons – unless directed by staff leading the lessons
- Clubs before or after school, or any other activities organised by the school

Pupils are required to hand in their phone to the class teacher/school office who will store them securely during the school day. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement and in agreement with the class teacher and the Senior Leadership Team (SLT). Any breach of the acceptable use agreement by a pupil may trigger sanctions in line with the school behaviour policy, which may result in the confiscation of their device. All agreed use of pupils' personal devices will be supervised by school staff and will adhere to the bring your own device policy (appendix 1).

9. Staff using work devices outside school

All staff members will agree to the equipment loan agreement[5] and take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected
- Ensuring their hard drive is encrypted
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.
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 Headteacher/Network Manager.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, the school will follow the procedures set out in our policies on ICT, behaviour and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. 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.

11. Continuous Professional Development (CPD)

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).

[5] Appendix 4

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

The DSL 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.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Approval and Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

An incident report log can be found in appendix 6

This policy will be reviewed every year by the Director for Safeguarding in collaboration with Subject Leaders and the Trust Network Manager. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

This policy will be approved by the Chief Executive. by the Board of Trustees

At every review, the policy will be shared with all staff and the school's LGB.

Details for the monitoring of this policy by the school's Headteacher, Trust Network Manager, Trust Executive Trust Board and LGB are set out above.

13. Links with other policies

This policy links to the following Trust policies and procedures:

- Staff code of conduct
- Governor and Trustee code of conduct
- Complaints
- Exclusions
- Health and safety
- Equality

- GDPR Privacy notices
- GDPR and Data Protection
- Whistleblowing
- Acceptable use of ICT, Internet and Communications Systems
- Management of Contractors
- Safeguarding and Child Protection

and the following school policies:

- Behaviour and Anti-bullying
- Attendance
- Sex and relationship education
- First aid
- Curriculum documents

BRING YOUR OWN DEVICE POLICY

Rationale:

- The use of personal mobile devices at school deepens learning, is personalised and student-centred, and meets the expectations of teachers, students, parents and guardians
- At School students and staff are permitted to bring their own personal mobile electronic devices to school for the purpose of learning/teaching
- This policy applies to only those devices recommended by School as being relevant to student learning

Aims:

- To harness student and staff connectivity to personal mobile devices for the purpose of developing 21st century teaching and learning skills and for fostering digital literacy, fluency and social responsibility in a safe environment

Implementation:

- The increasing availability of personal mobile devices has accelerated the demand for new models of learning
- School has developed guidelines and procedures for BYOD will be communicated to staff, students, parents and guardians through the school website, newsletters, booklists and staff share drive

Technical Support will be provided:

- To access the school's wireless network during school hours
- Students may not use devices to record, transmit, or post photographic images or video of a person or persons during school hours or during school activities, unless otherwise allowed by a teacher.
- Devices may only be used to access computer files, internet sites and apps which are relevant to the classroom curriculum.
- School is not responsible for any possible device charges to your account that might be incurred during approved school-related use
- Students and parents should be aware that devices are subject to search by appropriate staff if the device is suspected of a violation of the school rules. If the device is locked or password protected the student will be required to unlock the device at the request of teaching or technical staff
- The school's network filters will be applied to a device's connection to the internet and any attempt to bypass the network filters is prohibited
- It is the responsibility of parents, guardians (for their child's device) and staff (for their own devices) to ensure that relevant up to date anti-virus software is installed on their device
- Students and staff are strongly encouraged to keep devices secured at all times when not in use. No students or staff shall be required to share their devices with others. To avoid loss, theft, and damage, sharing of devices with others is not recommended. Lock codes or device passwords are encouraged.
  Students and staff are solely responsible for the care of devices they choose to bring to school. School will not be held responsible (either financially or legally) for lost, stolen, or damaged devices nor for any malware viruses that they may inadvertently acquire via the School wireless network.

APPENDIX 1 – Bring Your Own Device (BYOD) Policy

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	☒	☐	☐	☐	☒	☐	☐	☐
Use of mobile phones in lessons	☐	☒	☐	☐	☐	☐	☒	☐
Use of mobile phones in social time	☒	☐	☐	☐	☐	☒	☐	☐
Use of smart phones in a professional capacity	☒	☐	☐	☐	Not Applicable			
Taking photos on mobile phones or other camera devices	☐	☒	☐	☐	☐	☐	☐	☒
Use of hand held devices e.g. PDAs, PSPs	☒	☐	☐	☐	☐	☒	☐	☐
Use of personal email addresses in school, or on school network	☐	☒	☐	☐	☐	☐	☒	☐
Use of school email for personal emails	☐	☒	☐	☐	☐	☐	☒	☐
Use of chat rooms / facilities	☐	☒	☐	☐	☐	☐	☒	☐
Use of instant messaging	☒	☐	☐	☐	☐	☐	☒	☐
Use of social networking sites	☐	☒	☐	☐	☐	☐	☒	☐
Use of blogs	☐	☒	☐	☐	☐	☐	☒	☐
Use of Games Console in school time	☐	☒	☐	☐	☐	☐	☒	☐
Use of Smart Watches	☐	☒	☐	☐	☐	☐	☒	☐

The above is a guide and may be personalised as appropriate for individuals

APPENDIX 2 – Key Contacts

ROLE/ORGANISATION	NAME	CONTACT DETAILS
Designated safeguarding lead (DSL[6])	Sinead MacPhee	smacphee@themendipschool.com 01749 838040
Deputy DSL (DDSL)	Carly Pollock	cpollock@themendipschool.com
Headteacher	Natalie Hanna	nhanna@themendipschool.com 01749 838040
Network Manager	Jodie Edgall	Jedgall1@thepartnershiptrust.com
ICT Subject Leader	Sheona Glass	sglass@themendipschool.com
Chief Executive Officer (CEO)	Emily Massey	Email: emassey@thepartnershiptrust.com
Safeguarding Governor	Melinda Baker	MBakerGov@themendipschool.com
Safeguarding Trustee	Dawn Wilde	Email: dwildetrustee@thepartnershiptrust.com
Senior Mental Health Lead[7]	Sinead MacPhee	smacphee@themendipschool.com
Designated teacher	Alisa Creaser	acreaser@themendipschool.com

[6] Within this document all references to the DSL should be taken to represent the DSL/DDSL and/or the wider safeguarding team

[7] All schools must have this by 2025 – delete is not appropriate

APPENDIX 3 – Acceptable Use Agreements

Learner Acceptable Use of Internet and ICT Intent

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using 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

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS EYFS AND KS1	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I 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 computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
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 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 3 – Acceptable Use Agreements

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS KS2/3/4/5	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **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 Agreements

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school or Trust's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that school devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed:	**Date:**

ICT Equipment Loan Agreement

Where necessary the School will provide equipment to Staff to assist in the delivery of the School curriculum. This equipment is loaned to Staff members. Whilst the equipment is in your care the following items should be noted.

- Equipment should only be used as is set out in the 'ICT Acceptable Use Policy'.
- Loaned equipment remains the property of the School and is only for use of the member of Staff that it is issued to. It is however, that member of staff's responsibility to look after the equipment whilst it is in their possession.
- Insurance cover is not provided. You are responsible for replacement if equipment is stolen whilst in your personal possession through your insurance policy (please check the details of these). Many insurance policies do not cover theft from an unattended car or accidental damage.
- Under no circumstance should Staff attempt to fix suspected hardware faults with the equipment. This must be assessed by the Network Manager before repair.
- Equipment must be returned on the termination of your employment.
- Equipment must be returned to the Network Manager/ School when requested. Appropriate notice will be given.
- Equipment damaged may not be immediately replaced. If the cost of repair is greater than the value of the equipment it will not be repaired.
- Training in the appropriate use of the equipment will be offered as part of the induction program when necessary. Refresher sessions will take place when required.
- Any charge incurred by Staff using school equipment is not chargeable back to the school.
- Failure to comply with any or all of the above may result in action in line with the disciplinary being taken and the withdrawal of the equipment.

I have read the above conditions and agree to abide by them. I am aware of the implications of insurance and recognise my responsibilities in the event of loss or damage.	
Item Serial Number	
Item Asset Tag	
Item type	
Staff Name	
Signed	
Date	

APPENDIX 5 – Online Safety Training Needs Audit

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

APPENDIX 6 – Online Safety Incident Log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**