Online safety policy

Reviewed Mar 2020

Document Control

Description	By Whom	Date
Established (from previous data protection and e-safety policy)	WM	Mar 2020
Approved by Trustees		27/4/2020
Next Full Review due		Apr 2022

Contents

1 Introduction

Computer technology in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

Websites

Learning Platforms and Virtual Learning Environments

E-mail and Instant Messaging

Chat Rooms and Social Networking

Blogs and Wikis

Podcasting

Video Broadcasting

Music Downloading

Gaming

Mobile/ Smart phones with text, video and/ or web functionality

Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At the Harmony Trust, we understand the responsibility to educate our children on Online Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

2 Aims

Our Trust aims to:

Allow staff and pupils to embrace the benefits of the online world in a safe manner. To do this we will:

- 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

3 Legislation and guidance

This policy is based on the Department for Education's (DfE) 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 Department'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 is in line with the Relationships education curriculum from Sep 2020

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

4 Roles and responsibilities

The Board of Trustees

- overall responsibility for monitoring this policy and holding the Trustees to account for its implementation.
- ensure regular meetings are held with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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)

The Executive Principal / Principal

- responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. This is delegated to the Head of Academy in schools for which this post exists.

The designated safeguarding lead

The DSL takes lead responsibility for overall safeguarding in school, in particular:

- Supporting the Executive Principal / Principal / Head of Academy in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Executive Principal / Principal / Head of Academy, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see academy online system – CPOMS / My Concern) 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 providing staff training on online safety (appendix 4 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 Head of Safeguarding and /or Board of Trustees

This list is not intended to be exhaustive.

Academy ICT Co-ordinator / Computing Lead

The ICT Co-ordinator / Computing Lead takes lead responsibility for online safety in school, in particular:

- Supporting the Executive Principal / Principal / Head of Academy in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Senior leadership, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Updating and providing staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Providing regular reports on online safety in school to the DSL or Senior Leadership
- Keep abreast of current issues and guidance through organisations such as the LA, CEOP (Child Exploitation and Online Protection) and Childnet.

The Senior network manager

The Senior network manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 (leading the contract with the 3rd Party contractor who undertakes these tasks and receiving regular reports on the system to ensure it is working correctly)
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

Data Protection Officer (DPO)

The DPO takes responsibility for :

- Supporting the Executive Principal / Principal / Head of Academy in establishing safe online data practices (transferring, sharing, deleting and forwarding)
- Updating staff on data related matters
- Working in partnership with the Trust's Data Lead to ensure compliance with statutory guidance related to data online
- Assessing the suitability of contractors to deliver online services to the Trust
- Working with relevant / appropriate staff to address online data breaches or losses
- Acting as a link between the Information Commissioners Office (ICO) and the Trust when a serious data incident occurs
- Liaising with other (external) agencies and services
- Ensuring all stakeholders (parents and staff) are regularly notified of data matters that affect them and how the Trust manages any data held online (internally and externally)
- Recording (and reporting where appropriate) any data issues resulting from online systems used by the Trust and its academies
- Providing regular training to staff (and more frequently to those with key roles) which includes safe online management of data
- Work with the Senior Network Manager to ensure that processes meet (or exceed) the GDPR and Data Protection Act (2018) expectations and requirements

This list is not intended to be exhaustive.

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 DSL to ensure that any online safety incidents are logged (see online system) 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

This list is not intended to be exhaustive.

Parents / Carers

Parents/ Carers are expected to:

- Notify a member of staff or the Principal / Head of Academy 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 and 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 / Carer factsheet - Childnet International

Visitors and members of the community

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

4 Educating pupils about online safety

ICT and online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to the children on a regular and meaningful basis. Online Safety is embedded within our curriculum and we continually look for new opportunities to promote Online Safety.

Each academy has a framework for teaching internet skills in ICT lessons.

Each academy provides opportunities within a range of curriculum areas to teach about Online Safety

Educating children on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the curriculum

Children become aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

Children are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities

Children are taught about keeping their personal data safe and secure

Children are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Children are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

Children are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the computing curriculum

The teaching of online safety will link to the National Curriculum and SRE legislation (from Sep 2020)

Pupils will be taught about online safety as part of the curriculum and as discrete ICT sessions:

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

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 social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Safer internet day is also used as a vehicle to promote online safety.

5 Educating parents and 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 or text messaging service. This policy will also be shared with parents via the academy website.

Online safety will also be covered during parents' evenings and specific sessions as required by individual academies.

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

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

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting online safety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss Online Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.

Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website).

Parents/ carers are expected to sign a Home School agreement

The Trust disseminates information to parents relating to online Safety where appropriate in the form of;

Information and celebration evenings

Posters

Website postings

Newsletter items

Special online safety events

6 Cyber-bullying

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 behaviour policy.)

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. This will be discussed in class and within assemblies.

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 detail).

The school also sends information/leaflets 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 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 consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

Cause harm, and/or

Disrupt teaching, and/or

Break any of the school rules or there could be suspicion it has been used for illegal purposes

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

Delete that material, or

Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

Report it to the police (taking into account the age of the child)

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7 Acceptable and safe use of Online technologies

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 1-3). 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 and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported to the DSL.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the DSL, depending on the seriousness of the offence; investigation by the Head of Academy / Principal, and involvement of police for very serious offences. For staff, deliberate access to inappropriate materials will lead to disciplinary action.

Internet Management

Staff will preview any recommended sites before use

Raw image searches are discouraged when working with children

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents / carers recheck these sites and supervise this work. Parents / carers will be advised to supervise any further research.

All users must observe software copyright at all times. It is illegal to copy or distribute Trust software or illegal software from other sources.

All users must observe copyright of materials from electronic resources.

Internet Use

Staff, pupils and the wider community must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended audience.

Don't reveal names of colleagues, pupils or other community members or share any other confidential information acquired through your job on any social networking site or blog.

Online gambling or gaming is not allowed on Trust owned equipment or through the LA internet services.

It is at the Principal's discretion on what internet activities are permissible for staff and children and how this is disseminated.

Infrastructure

Academy internet access is controlled through Virtue Technologies web filtering systems.

The ICT team have access to and monitor at random intervals the web logs for all Harmony Trust academies' Internet traffic.

The Harmony Trust is aware of its responsibility when monitoring staff communication under current legislation and takes into account; General Data Protection Register (2018), The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

Staff and children are aware that Trust-based email and internet activity can be monitored and explored further if required.

The Trust does not allow children access to Internet logs.

If staff or children discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the online safety coordinator or teacher as appropriate.

It is the responsibility of the academy, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up to date on all Trust machines.

Children and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the Trust's responsibility nor the ICT team's to install or maintain virus protection on personal systems. If children wish to bring in work on removable media it must be given to the ICT Technician for a safety check first.

The Trust does not allow the use of portable data devices in its academies. They should instead seek to use Office 365 and One-drive services.

Children and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the ICT Technician.

If there are any issues related to viruses or anti-virus software, the ICT team should be informed.

Managing Other Web 2 Technologies (including social media, blogs and other interacting sites online)

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our children to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

All children are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

Children are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

Children are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).

Our children are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

Children are encouraged to be wary about publishing specific and detailed private thoughts online.

Our children are asked to report any incidents of bullying to the school.

Staff may only create blogs, wikis or other web 2 spaces in order to communicate with children using systems approved by the Principal.

Passwords and Password Security

Passwords

Always use your own personal passwords to access computer-based services

Make sure you enter your personal passwords each time you logon

Do not include passwords in any automated logon procedures

Staff should change temporary passwords at first logon

Change passwords whenever there is any indication of possible system or password compromise

Do not record passwords or encryption keys on paper or in an unprotected file

Never disclose your personal password

Ensure that all personal passwords that have been disclosed are changed once the requirement is finished

Password complexity rules are applied, and passwords must contain a minimum of seven characters with a capitol letter and a special character

User ID and passwords for staff and children who have left the Trust are removed from the system within one week

If you think your password may have been compromised or someone else has become aware of your password report this to the ICT team.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The children are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and children are regularly reminded of the need for password security.

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood this policy.

Users are provided with an individual network, e-mail and Management Information System (where appropriate) log-in username.

Children are not allowed to deliberately access on-line materials or files on the Trust network, of their peers, teachers or others

Staff are aware of their individual responsibilities to protect the security and confidentiality of Trust networks, MIS systems including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

The ICT team apply a policy to lock down admin devices after 10 minutes of inactivity with teacher devices applying after 45 minutes.

In each school, all ICT password policies are the responsibility of the Principal and all staff and children are expected to comply with the policies at all times.

Pupils using mobile devices in school

We discourage pupils from bringing mobile devices into school. However, where parents feel it is necessary for the journey to and from school, pupils may bring them into school, but they must be handed into the office.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Staff are discouraged from using USB sticks and must not have any personal data on any USB stick or external hard drive.

If staff have any concerns over the security of their device, they must seek advice from the ICT team.

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 policies on [behaviour and ICT 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, (taking into account the age of the alleged perpetrator.)

Complaints

Complaints and/ or issues relating to Online Safety should be made to the Head of Academy or Principal. Incidents should be logged and where necessary / appropriate referred to the relevant agency in accordance with personnel or safeguarding procedures.

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. New staff receive information on the Trust's acceptable use policy and the management of data as part of their induction.

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).

The DSL [and deputy/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.

Trustees 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.

Monitoring arrangements

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

This policy will be reviewed every two years by the Trust Head of Safeguarding. At every review, the policy will be shared with the Board of Trustees

7 Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

ICT and internet acceptable use policy

8 Data Protection Statement

The procedures and practice created by this policy have been reviewed in the light of our Data Protection Policy.

All data will be handled in accordance with the school's Data Protection Policy.

Data Audit For This Policy					
What?	**Probable Content**	**Why?**	**Who?**	**Where?**	**When?**
Online Safety policy	**Name, address, personal information related to any online safety issues**	**Required to be retained as part of safeguarding process**	**Principal / SLT, Trust central team, staff or other representative as required as part of the safeguarding process**	**Kept on file at academy (and Trust central where appropriate)**	**Held on file until child leaves school and then passed onto new school**

As such, our assessment is that this policy:

Has Few / No Data Compliance Requirements	Has A Moderate Level of Data Compliance Requirements	Has a High Level Of Data Compliance Requirements
	✓	

9. Review Procedure

There will be an on-going opportunity for staff to discuss with the online Safety coordinator any issue of online Safety that concerns them.

This policy will be reviewed every 2 years and consideration given to the implications for future whole Trust development planning.

The policy will be amended if new technologies are adopted, or there are changes to legislation / guidance.

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

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

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
• I will 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 for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in 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 username 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'm 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 • 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 agreement (staff, Trustees, volunteers and visitors)

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

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
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?	
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?	