Stepping Stones
E-Safety and Online Safety Policy 2017 -2018

Approved by – Standards and Effectiveness Committee

Date – 24th January 2018

(Reviewed in line with Governor monitoring of Online Checklist)

Completed by Alison Dodd

Contents

Introduction

At Stepping Stones we strive to provide all our children with an outstanding, creative and stimulating learning environment. We recognise that our children are growing up in a world increasingly influenced and dependent on technology. We aim to ensure all our children are able to use technologies safely, responsibly and effectively. We strive to teach our children how to keep safe in a digital world, ensuring they are aware of the precautions needed to keep themselves safe and what they can do to report any concerns they may have to a trusted adult.

At Stepping Stones we aim to provide our parents and carers with up to date and relevant information and support to ensure they have a good understanding of their critical role in their child's e-safety abilities. We aim to offer regular training and support to keep the aware of potential risks new technologies can pose.

Aims

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

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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.

Our E-Safety Vision -

E-safety continues to influence and encompass all aspects of modern life. At Stepping Stones we recognise the need for our children to use technologies responsibly under the guidance of our teaching. E-safety includes the use of new technologies, internet and electronic communications such as mobile phones, online platforms and personal publishing. We recognise the profound effect that E-safety has on the future opportunities and prospects of our children and staff, and therefore are committed to educating and equipping them with a solid understanding of online dangers and precautions.

Our school's E-Safety policy will operate in conjunction with other policies including those for Positive behaviour, Anti-Bullying, Safe guarding, Curriculum Policies and Data Protection.

Roles and Responsibilites including the E-Safety Champion

Every staff member at Stepping Stones has a responsibility to our children to promote and uphold our E-Safety expectations and vision. Our E-Safety Champion is to be the main point of contact for e-Safety related issues and incidents .Our E-Safety champion is Alison Dodd (Headteacher) working with Michaela Armstrong (family support) and Kirstie Hunter (Computing Leader).

The governing body (Committee of Stepping Stones)

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is **Sandra Thornberry**.

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 2)

The headteacher

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

The designated safeguarding lead

Alison Dodd (Headteacher)

Jane Meacham (Deputy Headteacher)

Micaela Armstrong (Family Support Worker)

The above staff are the designated safeguarding lead(s) for the school.

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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 (appendix 3 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 governing board

This list is not intended to be exhaustive.

The ICT manager (This is contracted to Ed-IT and BTLS through service level agreements and overseen by the Computing Leader and Headteacher)

The ICT 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 on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) 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.

All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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

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 (appendix 1)

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

The role of the E-Safety Champion team includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's E-Safety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an E-Safety incident occur.
- Ensuring an E-Safety Incident Log is appropriately maintained and regularly reviewed.

• Keeping personally up-to-date with E-Safety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).

• Providing or arranging E- safety advice/training for staff, parents/carers and governors.

• Ensuring the Head teacher, SLT, staff, children and governors are updated as necessary.

• Liaising closely with the school's Designated Senior Person / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

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 (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

The school uses LCC Acceptable User Policy. All staff sign and have a copy of this each September or when joining the school.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

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

Security and data management

Security is of paramount importance in our school as we recognise the vulnerability and complexity of our children. The following principles need to be upheld by all staff:

- Secure log in details to access private information on the school server.
- Responsible access to the school server when accessed off site. It is the teacher's responsibility to use secure internet connections to access pupil data files with a password requirement for access. ***(See appendix agreement)***
- Personal data is to be stored on a secure, password protected network within the school secure server.
- Staff with access to personal data are to be informed and updated of their legal responsibilities to uphold privacy and security by a member of the E-Safety team.
- All staff to be aware of how to access, store and dispose of confidential data both inside and outside the school premises. ***(see appendix agreement)***
- E-Safety champions to be aware of the use of 'cloud' storage facilities to manage pupil files and other sensitive data, ensuring its secure use in guidance the Data Protection Act and remote access responsibilities outlined above.
- Mobile devices such as ipads and staff laptops to be securely password protected. All staff to ensure they are logged off at the end of each session. All pictures and pupil information to remain on password protected devices and logged off securely when off site.
- All personal devices such as smart phones and tablets to remain securely locked in staff lockers when on sight. All access to staff email containing confidential content

should be only be accessed through secure, password protected wifi on password protected school devices only. ***(see appendix smartphone agreement)***

- All confidential and school data is to backed up on the online server each night. This is to be managed by our ICT technician on his weekly visits and monitoring.

Use of mobile devices

Stepping Stones recognises the benefits that mobile devices offer to enable our children's learning experiences to be captured and shared. Stepping Stones ensures these collected images are securely stored and deleted when appropriate, in line with the above principles outlined in our security and data management section.

Only school, password protected mobile devices can be used to capture images and recording of our children both on and off site.

Cameras, Videos and Photographs:

THESE RULES MUST BE FOLLOWED BY ALL STAFF MEMBERS EMPLOYED BY STEPPING STONES, LANCASHIRE COUNTY COUNCIL AND ALL SUPPLY AGENCIES –

- Photographs and videos of children, staff and other employees or school visitors are only to be taken using a school owned camera/devices.
- The images/videos must be uploaded on the school computers only and stored on school computers only.
- If staff choose to use these images/videos for their lessons, making displays or for interactive displays (such as Powerpoints) then the preparation of such must be done on secure password protected school computers only.
- No personal cameras/mobile phones/tablets can be used to take images/videos of staff, pupils, visitors and other school employees. Refer here to the Safeguarding policy and the children in school who have not got permission to be photographed/videoed.
- Also, only school-owned device such as a camera or iPad can be used for taking ANY photographs/videos out of school.

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 2.

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. Any USB devices containing data relating to the school must be encrypted.

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

Work devices must be used solely for work activities.

Staff Mobile devices (Phones)

Staff should not use their mobile phones during the school day. Staff should ensure their mobile phones are stored in the staff room and not in class with them (unless in exceptional circumstances which need to be agreed with SLT)

Staff should make calls from the designated staff areas and not class bases.

Parents taking photographs and videos

- Under the Data Protection Act (1998) parents are entitled to take photographs of **their own children on the provision that the images are for their own use**. E.g. at a school production. Including other children or other purposes could constitute as a potential breach of the Data Protection Act.
- Parents are informed at all events that they should only take photographs of their own children and they need permission to include other children/adults.
- Parents are reminded to be respectful when taking images and not obstructing the view of other parents / carers etc.
- Parents are reminded at events in the form of a written poster that they should not be posting pictures of other children /adults on social networking sites without obtaining permission from the parents.

Storage of photographs and videos

All images should be transferred regularly from mobile devices e.g. camera's and ipads and placed on the teachers drive (L) or Pupil drive if they are using them for their work. Photographs will be stored and used from this location only and should not be taken out of school on devices such as pen drives etc.

Images are not stored on any cloud devices of drop box.

Images should be deleted regularly – Every 6 months or when a child leaves the school.

Communication Technologies

Communication technologies contribute hugely to modern life and therefore are embraced and encouraged responsibly within our school. We aim to equip all our children with a secure and comprehensive understanding of the positive use of social platforms. Through an open and modelled approach, Stepping Stones aims to ensure our children area aware of the potential dangers and lasting impact of social communication technologies.

Internet access

Children's access

- Pupils must be supervised at all times when accessing school equipment and online materials.
- Pupils should use individual log on details and not be logged on in a staff account. These are available in classes near the computers.
- Pupils will be taught how to evaluate Internet content and should sign an a agreement to use the internet in a safe appropriate manner. (Think then Click)
- Pupils are restricted to use the pupil drive.
- School will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught, to be critically aware of the materials they read and the importance of cross checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. telling a responsible adult.
- Pupils will have individual logs for any learning resources used such as purple mash / active learn.

Adult access:

- All staff have individual log on details to the computers.
- Access to the office and headteachers drive is restricted. Staff have access to the teachers drive (t:), teachers planning, pupil data and public drive (p:).
- Staff are asked to data cleanse regularly – deleting old file, past pupil images etc.
- Staff should store their passwords in an envelope sealed in the school safe. This is in case of long term absence etc.

Social Networks

Twitter

Our school twitter account is only to be accessed by designated staff, who are regularly updated and aware of children with permission for online posts, gathered from parents each half term by the E-Safety champion.

Class Dojo App

Class Dojo online app is to be used by all class based staff in conjunction with above permissions gathered from parents/ carers, to share regularly schools events and children's work. Parents are provided with log in details on admission to the school. Parents can download the app and see their child's work and celebration. Some posts are made to the School page which can be seen by all parents. Permissions are sought through our permission letters in order to posts to go to other parents which may include more than one child.

Email

Each class a password secured email account to enhance learning opportunities. These are monitored by classroom adults when in use and checked half termly by e-Safety champion. (willow@steppingstones.lancs.sch.uk, maple@steppingstones.lancs.sch.uk, oak@steppingstones.lancs.sch.uk)

Staff E-mails are to be accessed on secure, password protected internet connections only. These accounts are password protected and passwords regularly updated.

Staff email accounts are to be accessed on school devices only and any confidential materials to be securely deleted and emptied from the trash folder immediately.

School Website

The school website content is in line with Lancashire guidelines and is managed by secure ICT support services. All children's identities and locations are protected, and only images of children with recent permissions are published. All content is approved by the head teacher before publication.

The school website offers support an advice to parents and carers regarding E-Safety issues and developments.

Software / hardware

- The software purchased in school is all documented with appropriate licensing.
- APPS are downloaded using the class accounts.
- A central management system is in place and managed by the IT technician.
- The school bursar monitors and documentation is in place to prove purchasing.
- Regular audits of software and hardware are carried out.

Management of software and hardware

- All servers, wireless systems and cabling are securely located. The server room will be up and running by Feburary half term. This is only to be accessed by designated IT staff.
- All wireless devises are security enabled.
- Access for downloading apps has been distributed to classes, in order to ensure each class has relevant apps for their curriculum and teaching.
- The IT support team are responsible for managing the security of the school network.
- Computers are regularly updated as is the system by the IT technicians.

- All staff, pupils have individual log on details to access the computer systems and should be taught to lock/ log out the computer when leaving it unattended.
- The school IT Technicians are responsible for installing software.
- Any breaches or concerns should be raised with the Head teacher.
- Staff should not use removable storage devices that are not encrypted. Where possible my ngfl should be used or remote access. All teachers have access to remote access from home therefore reducing the need to be transferring files onto pen drives and data storage devices.
- The Computing Leader / Head teacher and business support manager are all responsible for liaising with the IT technicians and support.

Educating pupils about online safety

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

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

The safe use of social media and the internet will also be covered in other subjects where relevant.(PSHCE, Esafety days and computing curriculum)

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.

Educating parents about online safety

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

Online safety will also be covered during parent open afternoon sessions.

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.

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. All class teachers will discuss cyber-bullying with their groups, and the issue will be addressed in theme weeks / circle time / daily meeting.

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 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.

Illegal Offences

Any suspected illegal material or activity must be brought to the immediate attention of the headteacher who would refer to the appropriate authorities outlined above.

Never personally investigate, interfere with or share evidence as you may be inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those involved investigating the incident. Always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk)

This includes searching devices without permission. If staff suspect a device may have evidence / illegal content on then it should be reported to the headteacher, the headteacher will make the decision on what course of action to take. It is not appropriate for staff to search the device. This may be seen as incriminating or tampering with evidence.

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

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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. **Headteacher / appropriate SLT member only.**

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

Examples of Illegal Offences

- Accessing sexual abuse images.
- Accessing non – photographic child sexual abuse images.
- Accessing criminally obscene adult content.
- Incitement to racial hatred.

Inappropriate Use – Incidents and Sanctions Procedure:

Incident	**Procedure/Sanctions**
Accidental access to inappropriate materials (materials which might get through the filter).	Adult/pupil to minimise webpage/turn off monitor; Tell a trusted adult or adult might have already seen; Adult to enter details into the incident log and report to LGfL filtering services if necessary; Persistent 'accidental' offenders will have their actions responded to by the school behaviour policy.
Using other people's log in details; Deliberate searching for inappropriate materials; Bringing inappropriate electronic files from home; Using chats and forums in an inappropriate way.	Inform SLT member; or designated E-Safety Champion; Enter details on incident log; Additional awareness raising of E-Safety issues with the pupils and class; Behaviour policy for persistent offenders and possible banning from ICT equipment for period of time; Parent/carer involvement as needed.

- The headteacher is responsible for dealing with E-Safety incidents.
- All staff are made aware through the policy and training about the different types of incidents and hot to respond to them. E.g. illegal or inappropriate.
- The headteacher records incidents using an E-Safety incident log form.
- Incidents would be monitored on an annual basis and reported to the committee.
- The head teacher would make contact with parents where appropriate and other agencies if required.
- The head teacher would seek advice from HR/ police immediately if concerns were raised about staff which may result in suspension pending investigation.
- These procedures are in place to protect staff and pupils.

Education and training

Stepping Stones keeps staff up to date with appropriate online training via the school portal. This is monitored by head teacher in line with Lancashire guideline concerning child protection. E-Safety champions keep themselves aware of updates and developments in line with Lancashire guidelines.

Dealing with Incidents:

Any of the incidents that have been mentioned within this policy are to be reported to the Head Teacher (in some cases it may need to be reported to the Senior Designated Person for Child Protection.) The Head Teacher will then refer to external authorities as required – Police, CEOP, IWF (Internet Watch Foundation). These authorities are licensed to investigate while schools are not.

Appendix 4 is used to log details of E Safety concerns. For serious concerns the safeguarding policy and procedures will be used and the same systems would be in place.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL(s) will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

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

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

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

Student / Pupil Acceptable Use Policy Agreement

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / IPad.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will only visit websites that have been agreed.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer / tablet.
- When I use tablet/ computers at home I will follow the same rules and tell adults if something is not right / someone is talking to me online.
- I will never share my personal information with anyone I do not know. (Online)

Signed (child): .....

(The school will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children the signature of a parent / carer should be sufficient)

Signed (parent): .....

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.*

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

All staff, volunteers, visitors and governors need to read and agree to the LA policy for use of social media.

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • 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 • Share my password with others or log in to the school's network using someone else's details	
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. 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/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Adapt this audit form to suit your needs.

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
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? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**