SAWLEY INFANT & NURSERY SCHOOL

E-Safety Policy (including online safety)

Approved by:	Academy Governing Body
Date:	14.03.22
Minute no:	19.10.2
Version:	v2
Review cycle:	Annual
Publication:	Internal & public

VERSION CONTROL			
VERSION	DATE	AUTHOR	CHANGES
v1.0	Oct 2016	DD Based on the latest Derbyshire LA Model Policy - Sept 2015	
DRAFT v2	Feb 22	DD Updated based on previous policy & 'The Key' model policy	Reflects latest KCSiE requirements. Acceptable Use Agreement & Loan Agreement removed (covered by Acceptable Use Policy & IT provider documents).

Contents

Appendices

1. Introduction

The school must ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as are applied to the school's physical buildings. E-Safety is recognised as an essential aspect of strategic leadership in this school and the headteacher, with the support of governors, aims to embed safe practices into the culture of the school.

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, 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 scam

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 DfE's guidance on protecting children from radicalisation.

It reflects legislation at the time when it was last reviewed. 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. Any changes in legislation will take precedence over anything printed in the policy.

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

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

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-bullying and Cyberbullying Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

- Acceptable Use of IT policy
- Staff Code of Conduct

2. Aims

The Online and E-Safety Policy aims to ensure that we:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which enables 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

3. Roles and responsibilities

3.1 The academy governing body

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

The governing body 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).

All governors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The 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)

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions. Currently, the headteacher has the role of being the DSL.

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

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the ICT manager 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 *(see Appendix 2)* 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 1 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 governing board

This list is not intended to be exhaustive.

3.4 The ICT provider and ICT Coordinator

ICT provision and management is outsourced to an external provider. As part of their contractual responsibilities, the ICT provider is responsible for:

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

The ICT Coordinator is a staff role. The ICT Coordinator is responsible for:

- Ensuring that any online safety incidents are logged (see Appendix 2) 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.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- 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 (see Appendix 2) 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'

Teachers are responsible for:

- Ensuring that pupils are aware of the e-Safety rules, introducing them at the beginning of each new school year.

- Promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a ‘No Blame’ culture so pupils feel able to report any bullying, abuse or inappropriate materials

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

- Ensure they and their child understand the terms on acceptable use of the school’s ICT systems, internet and any loaned equipment. Parents are given information about the school’s e-safety policy at the Induction Day for new pupils.

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

- What are the issues? -UK Safer Internet Centre
- Hot topics - Childnet International
- Parent resource sheet - Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the school’s ICT systems or the 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. Technical and hardware guidance

4.1 School Internet provision

The school uses an external Internet Service Provider and IT Technical Support Provider as part of Willows Academy Trust.

4.2 Content filter

Our Internet Provider uses a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

All pupils and staff have been issued with clear guidelines on what to do if this happens, and parents/carers will be informed where necessary.

Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

4.3 Downloading files and applications

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.

4.4 Portable storage media

Staff and authorised students are allowed to use their own portable media storage (USB Keys etc). If use of such a device results in an anti-virus message they should remove the device and immediately report to the ICT Coordinator.

4.5 Security and virus protection

The school IT service provider also provides all anti-virus software. The software is monitored and updated regularly by the technical support staff

Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the school ICT Coordinator who will coordinate reports to the external provider.

5. E-Safety for pupils

Sawley Infant and Nursery School believe it is our responsibility to prepare pupils for their lives in the modern world, and ICT is an integral part of that world. At our school, we are committed to teaching pupils to use ICT effectively and appropriately in all aspects of their education.

5.1 Internet access at school

Internet access is carefully controlled by teaching staff according to the age and experience of the pupils, and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the internet, and computers with internet access are carefully located so that screens can be seen at all times by all who pass by.

5.2 Using the Internet for learning

The internet is now an invaluable resource for learning for all our pupils, and Sawley Infant and Nursery School use it across the curriculum both for researching information and as a source of digital learning materials.

Sawley Infant and Nursery School teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

Teachers carefully plan all Internet-based teaching to ensure that pupils are focused and using appropriate and relevant materials.

Children are taught how to use search engines and how to evaluate Internet-based information as part of the ICT curriculum, and in other curriculum areas where necessary. They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music and that this must be taken into consideration when using them.

5.3 Teaching safe use of the Internet and ICT

Sawley Infant and Nursery School think it is crucial to teach pupils how to use the internet safely, both at school and home.   We do this through units of work, assemblies, projects and events such as internet safety day which are tailored to be age-appropriate.

5.4 Suitable material

Sawley Infant and Nursery School encourage pupils to see the internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

5.5 Non-Educational materials

Sawley Infant and Nursery School believe it is better to support children in finding their way around the Internet with guidance and positive role modelling rather than restrict internet use to strict curriculum-based research. As well as researching internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time, at out-of-school-hours provision, and home. There is a selection of links to such resources available on the school website.

5.6 Unsuitable material

Despite the best efforts of the school staff, occasionally pupils may come across something on the internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur so that action can be taken. The action will include:

a. Making a note of the website and any other websites linked to it.

b. Informing the ICT Coordinator who will record the incident and take action to prevent a repetition.

c. Discussion with the pupil about the incident, and how to avoid similar experiences in future

d. Discussion with the child's parents/carers to advise them of what has happened.

5.7 E-Mail

E-Mail is a valuable method of communication that plays an important role in many aspects of our lives today. Sawley Infant and Nursery School believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively.

- The use of e-mail is taught as part of the ICT curriculum.
- Pupils are not allowed to access personal e-mail using school internet facilities

5.8 Chat, discussion and social networking sites

Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people. We teach children personal safety and privacy as part of teaching children the safe use of the Internet.

All commercial Instant Messaging and Social Networking sites are filtered as part of the internet provision service.

Pupils may take part in discussion forums or post messages on bulletin boards that teachers have evaluated as part of specific lesson activities. Individual pupil names or identifying information will never be used.

5.9 Cyberbullying - Online bullying and harassment

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy and the anti-bullying and anti-cyberbullying policy. These include:

- No access to public chat rooms, Instant Messaging services and bulletin boards.
- Pupils are taught how to use the Internet safely and responsibly and are given access to guidance and support resources from a variety of sources.
- We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff and have a range of materials available to support pupils and their families.
- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

5.10 Contact details and privacy

Pupil's personal details, identifying information, images or other sensitive details will never be used for any public internet-based activity unless written permission has been obtained from a parent or legal guardian. Pupils are taught that sharing this information with others can be dangerous.

5.11 Deliberate misuse of the internet facilities

All pupils have discussed the rules for using the internet safely and appropriately. Where a pupil is found to be using the internet inappropriately then sanctions will be applied according to the nature of the misuse, and the school behaviour policy.

6. Use of the internet and ICT resources by school staff

6.1 The internet

Our school understands that the internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion. Sawley Infant and Nursery School are committed to encouraging and supporting our school staff to make the best use of the internet and all the opportunities it offers to enhance our teaching and support learning.

6.2 Internet availability

To enable staff to make full use of these important resources, the Internet is available in school to all staff for professional use.

6.3 ICT equipment and resources

The school also offers staff access to appropriate ICT equipment and resources, including computers, laptops, tablets, interactive whiteboards, data projectors, digital cameras, video camcorders, sound recorders, and a range of professional and curriculum software

6.4 Professional use

Staff are expected to model appropriate ICT and internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and internet use by our pupils both in school and at home.

Staff are also careful to consider inclusion and equalities issues when using ICT and the internet, and to provide pupils with appropriate models to support the school's Inclusion and Equal Opportunities policies.

Staff who need support or INSET in using ICT as part of their professional practice can ask for support from the ICT Coordinator.

6.5 Personal use of the internet and ICT resources

Some equipment (including laptops) is available for loan to staff, with permission from the ICT coordinator and headteacher. The appropriate forms and agreements must be signed. All staff must be aware of the school policy on using school Internet and ICT resources for personal use explained in the Acceptable Use of IT policy.

6.6 E-mail

Sawley Infant and Nursery School recognise that e-mail is a useful and efficient professional communication tool. To facilitate this, staff members will be given a school e-mail address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups. Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this. E-mail accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.

6.7 Online discussion groups, bulletin boards and forums, online chat and messaging

Sawley Infant and Nursery School realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin boards to share good practice and disseminate information and resources. The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.

6.8 Social networking

The school appreciates that many staff will use social networking sites and tools. The use of social networking tools and how it relates to the professional life of school staff is covered in the Staff Code of Conduct expectations and agreement and the Acceptable Use of IT policy.

7. Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools

- Relationships and sex education and health education in secondary schools

At our infant school **(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** (junior school or primary school) will be taught to:

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

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

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

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

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

8. 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 and virtual learning environment (VLE). This policy will also be shared with parents.

Online safety will also be covered during the induction process for new pupils.

If parents have any queries or concerns about 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.

9. Cyber-bullying

9.1 Definition

Cyberbullying 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.)

9.2 Preventing and addressing cyber-bullying

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

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

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

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 15 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 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.

9.3 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*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

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

10. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to follow the Acceptable Use of IT policy. This is covered at induction for staff and governors and refreshed annually thereafter as a minimum. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

11. Pupils using mobile devices in school

Pupils are not permitted to bring mobile devices into school.

Pupils are taught the importance of safe and appropriate use of mobile phones and similar devices as part of teaching internet safety.

12. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching them to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date – always install the latest updates

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

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

13. 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 acceptable use of IT. 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 by the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

14. Complaints regarding E-Safety

The school takes e-safety very seriously and takes all reasonable precautions to ensure that pupils are kept safe when accessing the internet in school. However, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for the material accessed or any consequences of internet access. The IT Coordinator acts as the first point of contact for any complaint. If the complaint cannot be resolved by the IT Co-ordinator, it should be raised with the headteacher and will be handled in accordance with the school Complaints Procedure.

15. Training

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

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

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, 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 the risks up
- 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 and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

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

16. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found at Appendix 2.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. 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.

Appendix 1

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?	
Are you aware of the ways in which 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 policy?	
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 2

Online Safety Incident Report 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**