Online Safety Policy

'Building a lifelong love of learning in a safe and happy school'

Reviewed by:	Laura Harvey & Daniela Thompson	**Date:** September 2024
Agreed by staff	October 2024	
Adopted by Governing Board:	November 2024	
Date of next review:	October 2025	

Philosophy

The internet is an extremely rich resource and communication tool both for learning and for recreation. If used effectively it can have a positive impact upon raising educational standards through the teacher's ability to plan and resource lessons and also to increase their own subject knowledge prior to teaching.

Children use the internet widely inside and outside of school because it is part of the statutory curriculum. Children need to develop the appropriate skills and understanding that will enable them to use these tools and resources well and safely, as well as the ability to analyse and evaluate the resources they find. As a result, online safety is a major focus in our curriculum.

Staff, Governors and Pupils have a responsibility to ensure that they use the internet appropriately and in accordance with the guidelines outlined in this policy.

Governors have a responsibility for reviewing the internet policy on a regular basis and ensuring that it is fit for purpose.
Governors must ensure that filters are in place to safeguard children, staff and the school. The filters must be able to pick up on inappropriate content but should also not be so strict that they do not allow children to undertake appropriate research. This is a balancing act and needs to be reviewed regularly.

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, including mobile and smart technology (which we refer to as 'mobile phones')
- 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 (DfE) statutory safeguarding guidance, Keeping Children Safe in Education.

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

Roles and responsibilities

The governing board

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

The safeguarding governor 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 understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure appropriate filters are in place.

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

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy.

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 Computing Subject Leader and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection and safeguarding policy
- Ensuring that any online safety incidents are logged (see appendix 5) 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 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary

The Computing Subject Leader

The Computing Subject Leader ensures that the technician is:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, 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 regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Providing a reliable, secure and safe filtered broadband internet connection (through E2BN) for use within school

All staff and volunteers

All staff and volunteers are responsible for:

- Reading and understanding 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 the Online Safety Agreement (Appendix 1).
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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'
- Staff will preview any recommended sites before use.
- Staff will ensure that only age-appropriate materials are used.
- Any websites to be accessed by children must be checked by staff before being recommended. Raw image searches are discouraged when working with pupils.
- Good practice is that if internet research is set for homework, specific sites will be suggested that have previously been checked thoroughly by the teacher. Furthermore, it is advised that parents recheck these sites and supervise this work. Ideally, parents will be advised to supervise any further research.
- All staff, volunteers and governors must comply with the social media Policy regarding the posting of any information or images relating to the school.
- All staff are aware that deliberate or inadvertent access to inappropriate material must be reported to IT lead asap.
- Staff will try and keep up to date with any online risks regarding apps, social media and issues.
- Any inappropriate content discovered must be reported to the IT lead asap.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy or concerns about online safety.
- Ensure their child has read, understood and agreed to the Online Safety Agreement (Appendix 2)

The school will raise parents' awareness of internet safety in letters or other communications, and in information via our website. This policy will also be shared with parents. Online safety will also be covered during an annual parent workshop.

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

- www.internetmatters.org
- www.childnet.com/parents-and-carers
- www.vodafone.co.uk/mobile/digital-parenting
- www.net-aware.org.uk/

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. .

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

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

Teachers will:

- Help to prevent children from accidentally accessing unsuitable material, the school's internet access is through a recognised educational service provider offering a filtered service.

- Ensure that use of the internet in school by pupils, will only be permitted whilst they are supervised by an adult.

- Foster a responsible attitude in our pupils towards the Internet in partnership with parents. Parents will be asked to share the 'Online Safety Agreement' (appendix 1) with their child and will not be allowed access to the internet until this has been signed.

- Educate pupils in the effective use of the internet by displaying and referring to the 'SAFE' document (see appendix 1)

- Teach pupils about safe and considerate internet use, including the importance of safeguarding their personal details when using email and the internet.

- Teach children to tell a trusted adult if they come across anything on the internet that makes them feel uncomfortable or unsafe.

- Inform parents if pupils have misused the internet.

- Refer complaints of misuse to the Designated Safeguarding Lead.

- Ensure that complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.

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.

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.

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.
- Ensuring their hard drive is encrypted
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – 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, as set out in appendix 3.

Work devices must be used solely for work activities.

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

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, their parents will be informed depending upon the individual circumstances, nature and seriousness of the specific incident.

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 Policy. 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.

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.

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

Website Guidelines

At Loughton Manor we maintain our own website in accordance with statutory guidance. Pupils whose work appears on the school website will be identified only by their first names. If a photograph is used, we will not name the pupil(s) and we will only use images of children whose parents have given written consent. Should any parent or guardian particularly wish their child's name, photograph or work not to appear on the school's website, their wishes will be respected.

Staff and governors' home information and e-mail identities will not be included – only the point of contact to the school i.e. phone number, school address and e-mail.

Home Learning Online

The school subscribes to two online home learning resources: Espresso and Purple Mash. Parents and pupils are notified annually of their passwords and usernames and reminded of the importance of not sharing these details. In the event of home learning, lessons will either be pre-recorded or taught using a secure link. For further information, please see our Remote Education Provision document for parents.

Remote Learning

There may be occasions where the school may need to rely on virtual learning. (for example, during the lockdown period of the pandemic or due to inclement weather)

Any virtual learning must be undertaken whilst ensuring that the safety of children has been considered.

Teachers must be aware that the level of filters that children have in a home environment may differ from the filters provided by school.

To facilitate a safe environment, teachers must consider the following requirements;

All virtual sessions should be timetabled and approved by the SLT.

Senior staff or DSL must be able to drop in on any online sessions, to undertake a random check.

A clear agreement of behaviour for student and staff must be in place and should cover the following elements.

- Teacher must act as a role model and be aware of their conduct at all times
- Consider suitability of the background; photos, artwork, identifying features, mirrors – ideally the backing should be nondescript or consist of the school logo.
- staff and pupils must be in living / communal areas – no bedrooms
- staff and pupils must be appropriately dressed (as they would in a face-to-face session).
- resources / videos must be age appropriate.
- the child may not have support immediately to hand at home if they feel distressed or anxious about content.
- Sessions should not be recorded without permission of parent, child and teacher, if teacher discovers the session is being recorded, then the session should be ended immediately.
- Any recorded sessions are subject to data protection guidance and should be stored appropriately.

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 5.

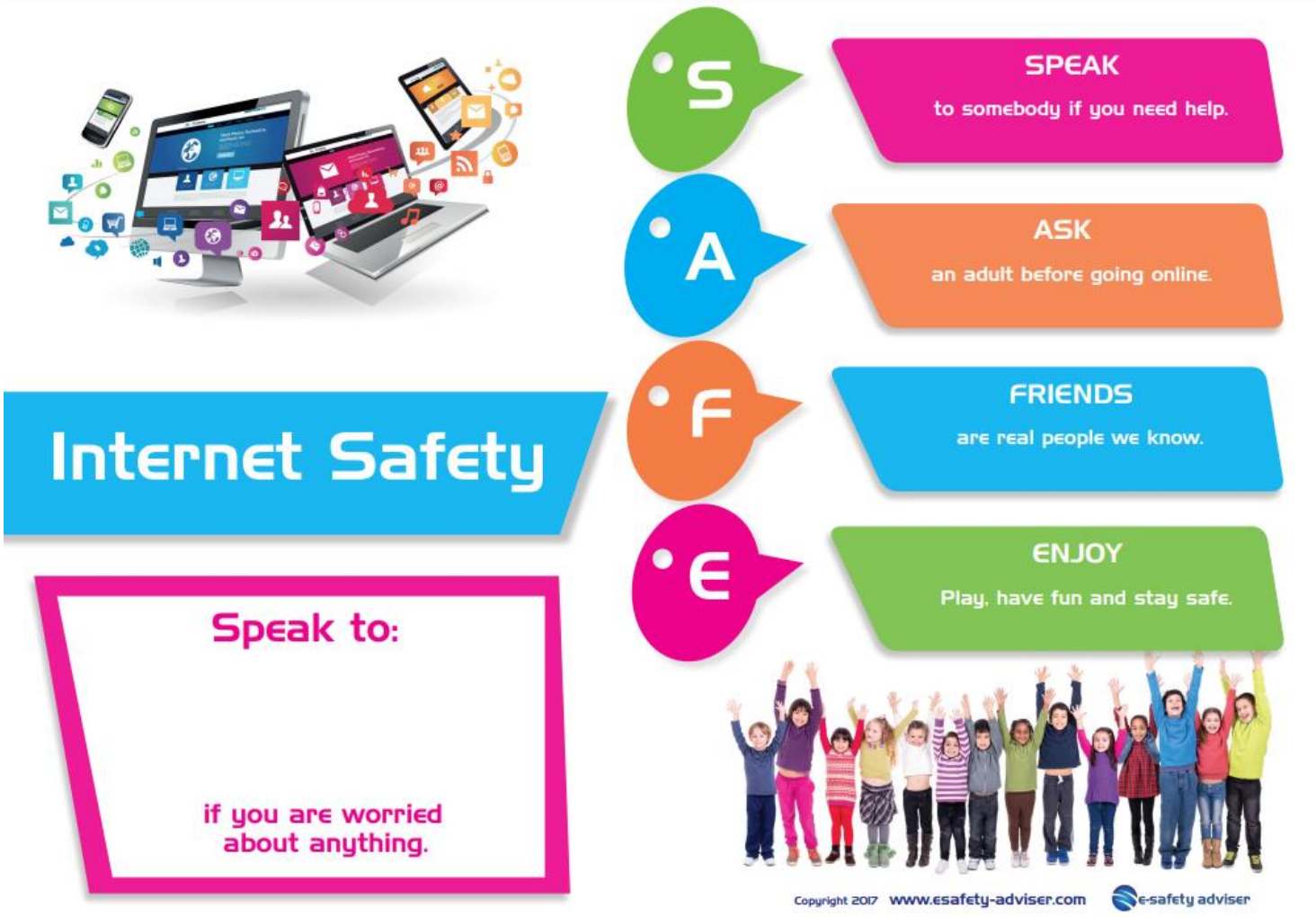
This policy will be reviewed annually by the DSL and Computing Subject Leader. At every review, the policy will be ratified by the governing board.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Relationships policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints policy
- Computing policy

Appendix 1 – Teaching resource



Appendix 2 – Online safety agreement

I will speak to somebody if I need help or if I feel worried or unhappy when using the internet.

I will always ask an adult before going online.

I will only speak to friends online and never speak to strangers.

I will enjoy using the internet whilst keeping myself safe.

Child's Name: _____

Date: _____

I have shared and discussed this with my child

Name: _____

Signed: _____

Date: _____

Appendix 3 – Staff's acceptable use agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND 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 (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 only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that 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 only use school iPads and not my phone or camera to take photographs of children in school. I will let the Designated Safeguarding Lead (DSL) and Computing Subject Leader 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):	**Date:**

Appendix 4 – Online safety training needs audit

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff and governors?	
Are you familiar with the Online Safety 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?	

Appendix 5: 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**