**Federation of Liphook Infant School and Liphook CofE Junior School**

# Safe Internet Use Policy

## 1. Aims

- To have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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

### 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, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user 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 scams

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety
- Meeting digital and technology standards
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education

It also refers to the DfE'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.

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

## 3. Roles and responsibilities

### 3.1 The governing board

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

- The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- The governing board will discuss online safety and requirements for training during Governor Safeguarding Monitoring Team meetings and monitor incidents of cyber bullying by looking at the bullying log.
- The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.
- The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:
    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
    - Reviewing filtering and monitoring provisions at least annually
    - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
    - Having effective monitoring strategies in place that meet the school's safeguarding needs

The governor who oversees online safety is **Steve Saycell.**

All governors will:

- Make sure 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)
- Make sure that online safety is a running and interrelated theme when devising and implementing The Federation's approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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 Executive Headteacher

The Executive Headteacher (who is also the DSL) is responsible for making sure 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 designated safeguarding lead (DSL) and deputy safeguarding leads (DDSLs) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

- Making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly

- Together with the IT technician and Infant Head of School, take the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the IT technician and Infant Head of School to make sure the appropriate systems and processes are in place
- Working with the IT technician, Infant Head of School 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's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are recorded on CPOMS and on the bullying log and dealt with appropriately in line with the school anti-bullying policy
- Working with the IT technician, Infant Head of School and Computing Leads to update and deliver 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 governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

### 3.4 The IT Technician

The IT Technician is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's IT 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 IT systems on a half termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Making sure 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 (appendix 3), and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)

- Knowing that the DSL is ultimately responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by speaking to the ICT technician or a member of SLT
- Following the correct procedures ie: speaking to the ICT technician or a member of SLT if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

### 3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or a member of SLT of any concerns or queries regarding this policy
- Make sure that 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
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

### 3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy 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

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

**All** primary schools must teach: Relationships education and health education

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
- Be discerning in evaluating digital content

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

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- 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, 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 are shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- 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 benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

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.

**Pupils will be taught practical cyber security skills**

This section is based on the DfE's non-statutory cyber security standards for schools and colleges.

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that are used to trick people into disclosing personal information
- Password security
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

## 5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in newsletters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parent workshops.

The school will let parents/carers know:

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

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Executive Headteacher or Heads of School.

Concerns or queries about this policy should be raised with the IT technician or a member of SLT.

## 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 Anti-bullying 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 encourage them to do so, including where they are a witness rather than the victim.

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

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 the computing curriculum.

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 on cyber-bullying to parents/carers so 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 Anti-bullying policy.

### Artificial intelligence (AI)

Pupils are not permitted to use generative AI tools at school; however we know that generative AI tools, such as Microsoft Copilot, Gemini and Chat GPT, are widespread and easy to access at home.

Liphook Federation recognises that AI may have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. Liphook Federation will treat any use of AI to bully pupils very seriously, in line with our anti-bullying policy.

Staff should be aware of the risks of using AI tools while they are still being developed. Any use of artificial intelligence should be carried out in accordance with our AI policy.

## 7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix) 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, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

## 8. Mobile phones

From September 2026, pupils may only bring brick phones into school, and these must be handed straight to their class teacher or office staff

## 9. Staff use

- School staff must take care to protect their privacy and protect themselves from risk of allegations in relation to inappropriate relationships and cyberbullying.
- school related issues must not, at any time, be discussed on the internet through social networking sites, e.g. Facebook
- staff and governors must not under any circumstances make links with any pupils via the internet through social networking sites (e.g. Facebook) until the child is over the age of 18

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

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- 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 it 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
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

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

Work devices must be used solely for work activities.

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

## 10. 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 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 code of conduct and low level concerns policy. 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 and/or LADO.

## 11. Training for staff, governors and volunteers

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, staff updates, staff briefings 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, threatening, harassing and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL 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.

## 12. Monitoring arrangements

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

This policy will be reviewed every year by the Executive Headteacher with the Digital Transformation Team. 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.

## 13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Low level concerns policy
- Behaviour policy
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable use of ICT policy

This policy was formulated by the Executive Head teacher and Governors of The Federation of Liphook Infant School and Liphook C of E Junior School and is to be reviewed annually.

Signed: ..... Signed: .....

Executive Head teacher Chair of Governors

Date: May 2026

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

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:<br>AGREEMENT FOR PUPILS AND PARENTS/CARERS | |
|---|---|
| **Name of pupil:** | |
| **When I use the school's ICT systems (like iPads and computers) and get onto the internet in school I will:**<br>• Only use school computers and iPads for schoolwork and homework.<br>• Only use SeeSaw and/or Microsoft Teams appropriately for my learning.<br>• Keep my login information secret- I will never share my password with anyone, including my friends.<br>• Never bring files into school without permission or upload inappropriate material to my workspace.<br>• Only edit or delete my own files and not look at, or change, other people's files without their permission.<br>• Only use websites that a teacher or adult has told me or allowed me to use.<br>• Tell my teacher immediately if:<br>  ○ I select a website by mistake<br>  ○ I receive messages from people I don't know<br>  ○ I find anything that may upset or harm me or my friends<br>• Never give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends.<br>• Never arrange to meet someone I have only ever previously met on the Internet.<br>• Only message people I know, or a responsible adult has approved. Be kind to others and not upset or be rude to them.<br>• Never share photos or videos of anyone without their permission.<br>• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly<br><br>**I understand that only brick phones can be brought to school and that smart watches, that connect to the internet, cannot be brought to school. I know that brick phones need to be put straight into the class phone box or handed to a member of the office staff.**<br>**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.** | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer agreement**: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these. | |
| **Signed (parent/carer):** | **Date:** |

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:<br>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:**<br>• 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)<br>• Use them in any way that could harm the school's reputation<br>• Access social networking sites or chat rooms<br>• Use any improper language when communicating online, including in emails or other messaging services<br>• Install any unauthorised software, or connect unauthorised hardware or devices to the school's network<br>• Share my password with others or log in to the school's network using someone else's details<br>• Take photographs of pupils without checking with teachers first<br>• Share confidential information about the school, its pupils or staff, or other members of the community<br>• Access, modify or share data I'm not authorised to access, modify or share<br>• 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.<br>I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.<br>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.<br>I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.<br>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 4: online safety training needs – self-audit for staff (as part of September INSET)

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