Lightmoor Village Primary School

Online Safety Policy

2025 2026

Online safety policy Lightmoor Village Primary School

This policy should be read alongside; ICT/Computing; Child Protection and Safeguarding; Acceptable Use and Social Media and Mobile and Smart Technology Policy.

The purpose of this policy statement is to:

• Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices.
• Provide staff and volunteers with the overarching principles that guide our approach to online safety.
• Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in Lightmoor Village Primary School.

Teaching and Learning

Here at Lightmoor we currently use 'Natter Hub' to support the teaching of online safety across the whole school years 1-6.

'Natterhub is a ready-to-go solution with animated lessons covering everything from managing secure passwords to highlighting the need for self-protection when photo sharing and taking part in group chats. With a 350+ curriculum-aligned lesson library and the ability for teachers to plan and assess a whole year.'

We keep online safety at the forefront of our minds, not just during internet safety weeks. Each class right across school takes part in a focussed and well planned activity using the resources from Natter Hub year 1-6 every week.

To keep communication open with the wider community and to support and inform our parents and carers we also share different online safety posters from the National Online Safety group, each week in our newsletters.

We believe it is essential that children are safeguarded from potentially harmful and inappropriate online material. We will take an effective whole setting approach to online safety to empower us to protect and educate our pupils, students, and staff in their use of technology.

Keeping Children Safe in Education 2025 shared key updates around online safety see below:

- changes to the list of content risks under online safety, adding in disinformation, misinformation and conspiracy theories

- more information on the DfE guidance on generative artificial intelligence (AI)
- DfE's filtering and monitoring self-assessment tool

Using Natter Hub and advice and support from Telford and Wrekin, our ICT service providers, we are able to support staff and children with using AI and our computing lead and online safety lead, along with our safeguarding governor on the monitoring and filtering processes in place

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism. **Including disinformation, misinformation and conspiracy theories**
- **Contact:** being subjected to harmful online interaction with other users; for example: 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; for example, 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. If we feel our pupils, students or staff are at risk, we will report it to the Anti-Phishing Working Group (https://apwg.org/).

Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children.

We believe that:

• Children and young people should never experience abuse of any kind.
• Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

• The online world provides everyone with many opportunities; however it can also present risks and challenges.
• We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online.
• We have a responsibility to help keep children and young people safe online, whether or not they are using [name of organisation]'s network and devices.

• Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.
• All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

We will seek to keep children and young people safe by:

• Appointing an online safety coordinator: Our Headteacher Lucy Cowan is our online safety coordinator and Lead DSL. Supported by Charley Lampitt our computing lead and Helen Oldham our safeguarding Governor.
• Providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults.
• Supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
• Supporting and encouraging parents and carers to do what they can to keep their children safe online.
• Developing an online safety agreement for use with young people and their parents or carers.
• Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person
• Reviewing and updating the security of our information systems regularly.
• Ensuring that user names, logins, email accounts and passwords are used effectively
• Ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
• Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
• Providing supervision, support and training for staff and volunteers about online safety.
• Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

Information system security

- School ICT systems security will be reviewed regularly by the ICT technician from T&W
- Service Provider (T&W) filters information using Smoothwall (filtering system).
- WiFi access is password protected. Information is monitored using SENSo.
- Staff must use Senso to monitor and control what pupils are typing/accessing during use of computers/laptops to meet safeguarding responsibilities.
- InTune management solution is used to control what pupils are accessing on the school iPads maintains the safe use of technology.

Managing filtering

- The school will work in partnership with T&W to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator and/or the ICT Technician.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- A log of any incidents on CPOMS will be used to identify patterns and behaviours of the pupils.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to parent email (including Parent Mail texting service) communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as possibly suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

If online abuse occurs, we will respond to it by:

• Having clear and robust safeguarding procedures in place for responding to abuse (including online abuse).

• Any complaint about staff misuse must be referred to the Headteacher. Complaints of internet misuse will be overseen by a senior member of staff. Pupils and parents will be informed of incidents.

• Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.

• Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account.

• Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Enlisting parents' support

- Parents and Carers attention will be drawn to the school's Online Safety Policy, in newsletters and on the school website and updates will be given.
- Parents are offered online safety training annually, with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust.

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

• Child protection.
• Procedures for responding to concerns about a child or young person's wellbeing.
• Dealing with allegations of abuse made against a child or young person.
• Managing allegations against staff and volunteer.
• Code of conduct for staff and volunteers.
• Anti-bullying policy and procedures.
• Photography and image sharing guidance.

Authorising internet access

- All staff, governors and visitors must read this online safety policy and sign appendix 1, alongside reading staff code of conduct and reading and signing the SISP – Schools Information Security Policy. Visitors" before using any school ICT resource.
- Pupils must sign an acceptable user policy agreement before accessing the school network independently at the start of KS2. It is the responsibility of the class teacher to ensure this is adhered to.

Contact details

Online safety co-ordinator
Name: Lucy Cowan
Phone/email: 01952 387620

Senior lead for safeguarding and child protection
Name: Lucy Cowan
Phone/email: 01952 387620

This policy was last reviewed: November 2025

Appendix 1

Acceptable Use Agreement / Code of Conduct Staff, Governor and Visitor

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with John Newton (school online safety coordinator.)

- Permission will be sought from students and parents before any photographs are published on a web site, blog or social media outlet.
- Images of children must not be published where it is possible to identify their names.
- Access must only be made via the authorised account and password, which must not be made available to any other person
- All Internet use should be appropriate to staff professional activity or student's education.
  Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed.
- No hardware of software will be installed without the permission of the ICT coordinator.
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden
- Copyright of materials and intellectual property rights must be respected
- All electronic communications with pupils/parents and staff must remain professional
- Own personal details, such as mobile phone number and personal email address must not be given out to pupils.
- Personal data must be kept secure and used appropriately, whether in school, taken off school premises or accessed remotely
- Any material that could be considered offensive, illegal or discriminatory must not be browsed, downloaded, uploaded or distributed.
- Internet access can be monitored and logged which can be made available, on request, to a line manager or Headteacher.
- Support of the school to online safety must be respected by not deliberately uploading or adding any images, video, sounds or text that could upset or offend any member of the school community.
- Online activity, both in school and outside, will not bring the professional role into disrepute.
- Support and promote the school's Online.
  Safety policy and help pupils to be safe and responsible in their use of computing and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the

School

Signature ……..……..……

Full Name …….....(printed)

Job title . . . . Date……..

Parents and Carers, in order to support the safe use of the internet and give ownership to our pupils we have been doing lots of work around using the internet responsibly in school.

Please could you read and discuss this agreement with your child and then sign it, ask your child to sign it, and return it to the class teacher. If you have any questions or concerns please speak to Mrs Cowan or Mr Newton.

Young person's agreement

 I will be responsible for my behaviour when using the internet, including social media

platforms, games and apps. This includes the resources I access and the language I use.

 I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to the group leader.

 I will not send anyone material that could be considered threatening, bullying, offensive or illegal.

 I will not give out any personal information online, such as my name, phone number or address.

 I will not reveal my passwords to anyone.

 I will not arrange a face-to-face meeting with someone I meet online unless I have discusses this with my parents and/or group leader and am accompanied by a trusted adult.

 If I am concerned or upset about anything I see on the internet or any messages that I receive,

I know I can talk to Mrs Cowan, Mr Newton, or my class teacher.

I understand that my internet use at [Name of group/organisation] will be monitored and logged and can be made available to the group leader. I understand that these rules are designed to keep me safe and that if I choose not to follow them, [Name of group/organisation] may contact my parents/carers.

Signatures:

We have discussed this online safety agreement and [ ] agrees to follow the rules set out above.

Parent/carer signature…… Date

Young person's signature…….....Date