



# Lyne and Longcross C of E (Aided) Primary School with Nursery

---

## Online Safety Policy

**Approved:**

**Review Due:**

Inspired by the relentlessly inclusive and loving example of Jesus Christ, our vision is to create a place of possibilities where children develop a lasting love of learning, where we recognise God has given us all special individual talents and strengths. Through working together as a community children will be encouraged and nurtured to fulfil their God given potential.

## Overview

Staff should be trained to recognise signs of mental health distress linked to online activity and respond appropriately.

The Staff and Governors of Lyne and Longcross C of E (Aided) Primary School with Nursery believe that online safety (online safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles. We know that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online. All staff believe that our school should provide a safe, caring and positive environment that promotes the social, physical and moral well-being of the individual child.

## Aims

- To clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Lyne and Longcross is a safe and secure environment.
- To safeguard and protect all members of the Lyne and Longcross community online.
- To raise awareness with all members of the Lyne and Longcross community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- To identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

## Procedures

Staff should be trained to recognise signs of mental health distress linked to online activity and respond appropriately.

The Headteacher retains, as per Keeping Children Safe in Education (KCSIE) 2025 and the Safeguarding policy overall responsibility for Online Safety. Curriculum content regarding online safety will be delegated to the responsibility of the Computing Leader.

All members of staff are provided with opportunities to receive online safety training, to develop their understanding of the risks to children. We recognise that staff working in the school who have become involved with a child who has suffered harm, or appears to be likely to suffer harm, may find the situation stressful and upsetting. We will support such

staff by providing an opportunity to talk through their anxieties with the DSL and to seek further support as appropriate.

### Allegations against staff

- All school staff should take care not to place themselves in a vulnerable position with a child. It is always advisable for interviews or work with individual children or parents to be conducted in view of other adults.
- All Staff should be aware of Surrey's Guidance on Behaviour Issues, and the school's own guidance in the Staff Handbook.
- We understand that a pupil may make an allegation against a member of staff. If such an allegation is made, the member of staff receiving the allegation will immediately inform the Head Teacher.
- Staff should be trained to recognise signs of mental health distress linked to online activity and respond appropriately.
- The correct procedure will be followed as per the Safeguarding Policy.

### Teaching and Learning

Why Internet and digital communications are important:

- The Internet is an essential element in 21st century life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, e.g. for research.
- Internet use will enhance learning
- Schools must regularly review filtering and monitoring systems using the DfE's 'Plan Technology for Your School' tool to ensure effectiveness and proportionality.
- The school Internet access is provided by JSPC Computer Services and includes filtering appropriate to the age of pupils.
- The school uses a proxy server to filter all internet access (see Technical Security Policy).

As part of the Computing Curriculum we will continue to ensure that:

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriate to a wider audience.
- Pupils will be taught how to evaluate Internet content.
- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

In line with KCSIE 2025, staff will be trained to identify and respond to online risks including misinformation, disinformation, fake news, and conspiracy theories. These risks are now part of the 4 Cs framework: content, contact, conduct, and commerce.

- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or other age-appropriate reporting tools.

### Managing Internet Access

#### Information system security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.
- Access to school networks will be controlled by personal passwords.

The school uses RM Safety Net as its monitoring system. Alerts generated from RM Safety Net are automatically sent to the Designated Safeguarding Lead (DSL) Team for review and action.

- Systems will be in place to ensure that Internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform online safety policy.
- The security of school IT systems will be reviewed regularly.

- Schools must regularly review filtering and monitoring systems using the DfE's 'Plan Technology for Your School' tool to ensure effectiveness and proportionality.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

### E-mail

As part of our curriculum, children will be taught about email use and given the opportunity to communicate with others in a safe and controlled environment.

- 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 pupil email communication must only take place via a school email address.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mails from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

### Published content and the school web site

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Pupils work will only be published with their permission or that of their parents/carers.
- Staff accounts for the school website will be safeguarded with an appropriately strong password.
- Staff should be trained to recognise signs of mental health distress linked to online activity and respond appropriately.

- The school will post information about safeguarding, including online safety on the school website.

#### Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children.
- Pupils' full names will be avoided on the Web site as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic sources.

#### Social media and personal publishing on Google Classroom

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Use of video services such as Skype, Google Meets, Zoom and Facetime will be monitored by staff. Pupils must ask permission from a member of staff before making or answering a video call, unless this is part of online learning provision and the session is being hosted by a member of school staff
- Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Staff should be trained to recognise signs of mental health distress linked to online activity and respond appropriately.
- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children. <http://www.surreycc.gov.uk/?a=168635>

Schools must regularly review filtering and monitoring systems using the DfE's 'Plan Technology for Your School' tool to ensure effectiveness and proportionality.

#### Managing filtering

- The school will work in partnership with Surrey County Council 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.
- Schools must regularly review filtering and monitoring systems using the DfE's 'Plan Technology for Your School' tool to ensure effectiveness and proportionality.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

#### Managing videoconferencing

- Pupils should ask permission from the supervising teacher before making or answering a video conference call, unless this is part of online learning provision and the call is being hosted by a member of school staff
- Video conferencing will be appropriately supervised for the pupils' age.
- Staff must be aware of the risks associated with generative AI tools such as ChatGPT and Grok, and follow school guidance on their appropriate use.

#### Managing emerging technologies

- Staff must be aware of the risks associated with generative AI tools such as ChatGPT and Grok, and follow school guidance on their appropriate use.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Staff will use a school phone where contact with parents or pupils is required.

#### Use of personal devices

- Personal equipment may be used by staff and/or pupils to access the school IT systems provided their use complies with the contents of this policy and the relevant AUP.
- Personal devices must not be used to take or store images of pupils or pupil personal data. The school has purchased mobile phones and tablets to enable staff to take images for professional use (capturing moments outside of the classroom

e.g. on trips) for using when returning to school or for publishing to social media sites such as the school's Facebook account

- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Due to the significant advances in mobile technology, there is the potential for mobile phones, tablets, cameras and other portable devices to be used inappropriately and compromise the confidentiality of the children in our care.

We recognise that staff and volunteers may wish to have their personal mobile devices at work in case of emergency. However, the safeguarding of the children within the school is paramount at all times.

Parents/Carers are required to sign relevant documentation when their child starts at Lyne and Longcross C of E Primary School with Nursery, giving authorisation for our school to take photographs for assessment and observation. On occasion, with permission, these photos may be published on the school website or other publications. If parents do not give permission, we respect that decision.

#### Use of school mobile devices

Lyne and Longcross C of E Primary School with Nursery provides mobile devices for staff and volunteers to use to support their work with the children. To ensure the appropriate use of this equipment, and to ensure the safeguarding of all children, the following policy applies:

- Only the mobile devices belonging to Lyne and Longcross C of E Primary School and Nursery may be used to take appropriate and relevant images of children e.g. Observations or photographs/videos of events within school. Personal mobile devices must not be used.
- Staff should be trained to recognise signs of mental health distress linked to online activity and respond appropriately.
- Images or videos taken must be used in accordance with the UK GDPR and Data Protection Act 2018 and the schools own Safeguarding Policy.
- It is recognised that staff may be working around the school with small groups of children using mobile devices. In such cases staff should ensure that they are not in rooms alone with the door closed.
- Mobile devices belonging to the school will not be taken home by members of staff without permission by the Head Teacher.
- Under no circumstances must mobile devices be taken into the toilets without the permission of the Head Teacher. If photographs or videos need to be taken in the

toilet area e.g. of children washing their hands, then the Head Teacher will be informed and will ensure that more than one member of staff is present.

- Children may be given the opportunity to use the schools mobile devices within the school or on a school visit. Children will only use mobile devices belonging to the school.

#### Use of mobile devices by staff and volunteers

- Personal mobile devices should only be used outside of working hours and never whilst the children are present. Personal mobile devices should be stored in staff lockers or locked away during school hours.
- In very exceptional circumstances, such as a family emergency, staff and volunteers should seek permission from the Head Teacher to use their mobile devices during working hours. This should happen away from the children. The schools main telephone number can be used for emergencies by staff or volunteers or by people who need to contact them.
- In circumstances such as off site visits, staff will agree with the Head Teacher the appropriate use of personal mobile devices in the event of an emergency. This will be identified on the Risk Assessment for the visit. The school mobile will be used for emergency purposes only.
- Where there is suspicion that material on a mobile device may be unsuitable and may constitute evidence relating to a criminal offence the Head Teacher reserves the right to seize the device and assess the material saved on it. If the material is deemed unsuitable the Head Teacher will follow guidelines in the schools Safeguarding Policy.
- No electronic copies of photographs or videos will be passed to outside agencies without permission of the Parent/Carer, or unless there is a safeguarding issue.
- Staff and volunteers remain responsible for their own property and will bear the responsibility for any losses.
- Staff or volunteers who ignore this policy and use a mobile device without permission may face disciplinary action.

#### Use of mobile devices by visitors

We recognise that visitors may wish to have their personal mobile devices with them for use in case of emergency. However, safeguarding the children within the school is paramount and it is recognised that personal mobile devices have the potential to be used inappropriately and therefore the school has implemented the following policy:

- Mobile devices should be switched off during visits into school and signs will be placed around the school to make this clear to all visitors.

- Parent/Carers are permitted to take pictures and videos of their own child and only their child during class assemblies or other school performances. Parent/carers will be made aware of this before each event and will be asked to sign a declaration form agreeing to this and stating that these images will not be placed on any form of social media.
- Where there is suspicion that material on a mobile device may be unsuitable and may constitute evidence relating to a criminal offence the Head Teacher reserves the right to seize the device and assess the material saved on it. If the material is deemed unsuitable the Head Teacher will follow guidelines in the schools Safeguarding Policy.
- The Head Teacher reserves the right to refuse visitors the opportunity to use mobile devices to take photographs or make recordings on Safeguarding grounds.
- In exceptional circumstances, such as a family emergency, visitors will seek permission from the Head Teacher to use their mobile devices, and this should happen away from the children.
- School Photographers will be treated as any other visitor and appropriate levels of supervision will be in place at all times.
- Visitors remain responsible for their own property and will bear the responsibility of any losses.
- Visitors who ignore this policy and use a mobile device without permission may face criminal charges

### Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the UK GDPR and Data Protection Act 2018.

### Authorising Internet access

- All staff must read and sign the AUP before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved, on-line materials.
- All Pupils are asked to sign their own 'Acceptable Use Agreement' before they are allowed access. This can be in the form of a whole class poster which the Pupils are expected to sign, after a whole class discussion about the SMART poster.
- Any person not directly employed by the school will be asked to sign an 'acceptable use policy' before being allowed to access the internet from the school site.

### Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

#### Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

#### Community use of the Internet

All use of the school Internet connection by community and other organisations shall be in accordance with the school e-safety policy.

#### Introducing the online safety policy to pupils

- Appropriate elements of the online safety policy will be shared with pupils
- Online Safety rules will be posted in all classrooms.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of online safety issues and how best to deal with them will be provided for pupils.

#### Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Schools must regularly review filtering and monitoring systems using the DfE's 'Plan Technology for Your School' tool to ensure effectiveness and proportionality.
- Staff that manage filtering systems or monitor ICT use, will be supervised by senior management and have clear procedures for reporting issues.

Parents and carers will be invited to participate in termly online safety workshops and will receive regular updates and resources to support safe online practices at home.

#### Enlisting parents' support

- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will receive annual updates on online safety, via a presentation from the online safety leader. They will also be provided with additional information on online safety as appropriate.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- All parent/careers will be required to grant permission for photos of their children to be sent via Marvellous Me. This permissions list will be shared with all members of staff.

#### Whistleblowing

- We recognise that children cannot be expected to raise concerns in an environment where staff fail to do so.
- All staff should be aware of their duty to raise concerns, where they exist, about the management of Child Protection, which may include the attitude or actions of colleagues.
- All staff are aware of the whistleblowing policy.

#### Responding to concerns regarding radicalisation or extremism online

- Schools must regularly review filtering and monitoring systems using the DfE's 'Plan Technology for Your School' tool to ensure effectiveness and proportionality.

The school retains full safeguarding responsibility for pupils placed in alternative provision. Regular communication and monitoring arrangements will be maintained to ensure effective safeguarding oversight.

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the Internet in schools and that suitable filtering is in place which takes into account the needs of pupils. Schools will need to highlight specifically how internet use will be monitored either here or within subsequent sections.

- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy.

### Prevention

We recognise that the school plays a significant part in the prevention of harm to our pupils by providing pupils with good lines of communication with trusted adults, supportive friends and an ethos of protection.

The school community will therefore:

- Establish and maintain an ethos where children feel secure and are encouraged to talk and are always listened to.
- Ensure that all children know there is an adult in the school whom they can approach if they are worried or in difficulty.
- Provide half-termly lessons to all pupils, strictly devoted to e-safety.
- Include across the curriculum opportunities which equip children with the skills they need to stay safe from harm and to know to whom they should turn for help.
- Promote the school's own e-safety rules and ensure that children are aware of them and that they are displayed throughout the school.
- Parents will be informed of the policy and its practices and a copy of the policy made available for inspection.