Lyng Church of England Primary School E -Safety Policy

Review Body:	Governors
Responsibility:	Headteacher
Type of Policy:	Non Stat
Review Period:	Every 2 years
Reviewed:	Spring 2021
Next Review:	Spring 2023

This policy applies to all members of Lyng Church of England Primary School community (staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the school's IT systems, both in and out of school.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.

What is e safety?

- E safety encompasses not only internet technologies but also electronic communications such as mobile phones, wireless technology, and games consoles.
- The internet is an open communications network. Anyone can send messages, discuss ideas and publish materials with little restriction.
- It highlights the need to educate children about the benefits, risks and responsibilities of using ICT.
- It provides safeguards and raises awareness to enable users to safely manage their on line experiences.

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.
Internet use is a part of the curriculum and a necessary tool for staff and pupils and the school has a duty to provide students with quality Internet access as part of their learning experience.
The school Internet access is currently provided by Norfolk ICT Shared Services and includes filtering appropriate to the age of pupils.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

A planned online safety curriculum is provided as part of Computing and other lessons.

- Key online safety messages are regularly reinforced as part of a planned programme of activities
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Older pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils should be helped to understand the need for Acceptable Use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be recorded, with clear reasons for the need given to the headteacher.

At Lyng CE Primary School:

- 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
- Pupils will be shown how to publish and present information appropriately 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 will be taught to be critically aware of the materials they read~~
- Pupils will be taught research skills and the need to avoid plagiarism and uphold copyright regulations
- In lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Pupils will be taught how to report unpleasant Internet content e.g. When in school and at home using the CEOP Report Abuse icon or Hector Protector.

Managing Internet Access and Network Management

Information system security

- School ICT systems security will be reviewed and updated regularly by the school's technician
- Virus protection will be updated regularly by the school's technician
- Security strategies will be discussed with the IT provider
- The school makes use of encryption for staff equipment uses individual log-ins for all users
- The school has secure offsite daily back-up of school data (admin and curriculum).

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's E Safety Policy.
- Provides pupils with a password which gives them access to the Internet and other resources.
- Makes clear that no one should log on as another user.
- Makes clear that pupils should never be allowed to log-on using teacher and staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;

- Requires all users to log off when they have finished working or are leaving the computer unattended.
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used only to support their professional responsibilities.
- Ensures that access to the school's network from remote locations by staff is restricted.
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems
- Uses secure data transfer; this includes DfE secure website for all CTF files sent to other schools
- Has wireless network secured to appropriate standards suitable for educational use
- Has IT and communications systems installed professionally.
- Maintains equipment to ensure Health and Safety is followed

Managing filtering

- The school will work in partnership with Norfolk Children's Services 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 ~~nominated member of staff~~. school's IT technician
- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
-

Passwords

- Internet and network access is through a unique username and password.
- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others.
- If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems.
- Staff are responsible for keeping their password(s) private.

E-mail

- The school provides staff with an NCC email account for their professional use
- Staff may only use their Norfolk Schools email for any school related communication. Personal emails must not be used.
- Pupils may only use approved e-mail accounts on the school system.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Pupils must immediately tell a teacher if they receive offensive e-mail
- Pupils will be taught not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission, and of the dangers associated with such behaviour.
- Staff to pupil email communication is through approved school email systems (class email/ pupil school email online system such a) when it is required, such as for remote learning.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.

Published content and the school web site

- The contact details on the Website should 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 and ensure that content is accurate and appropriate.

Digital images and video

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school and annually thereafter. This includes publication on the school website, prospectus or other high profile use, such as media publications.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials.
- Only school resources are to be used for recording / photographs of pupils. Mobile phones/personal equipment should not be used.
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose.

Social networking and personal publishing

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff
- School staff should not be online friends with any pupil.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Pupils are required to sign and follow our pupil Acceptable Use Agreement.
- Pupils do not currently have access to social networking sites at school, but are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- They will be advised never to give out personal information of any kind which may identify them, anybody else or their location.
- Pupils and their parents/ carers will be advised on the safe use of social network spaces, including age limits for such sites

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

Managing videoconferencing

- Any videoconferencing will take place in the structured context of lessons at this school.
- Videoconferencing will be appropriately supervised for the pupils' age.

Mobile devices

- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

- No pupil should bring his/ her mobile phone or personally-owned device into school. Any device brought into school will be kept in the school office until the end of the school day. The parent/ carer will be informed.
- If a pupil needs to contact his or her parents /carers, they will be allowed to use a school phone. Parents are to contact their child via the school office.
- All visitors are requested to keep mobile devices switched off/on silent.
- The recording of images, video and audio on any personal mobile device by parents or visitors is not permitted, except where it has been explicitly agreed in advance by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- When parents/ carers wish to use a device to record their own child at an event, this is acceptable providing: the Headteacher has given permission *and* no other person/ people are included in the images.
- Staff members are discouraged from using mobile phones during school hours. However, if necessary, they may use their phones during school break times when there are no pupils present. If a staff member is expecting an urgent personal call they may seek specific permission from the Headteacher to use their phone at other than their break times or to take the call on the office phone.
- Staff are not to use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- Staff are not to use personal devices for professional purposes, such as contacting parents. All contact should be through the school's communication systems via the office.
- Staff will be issued with a school phone where contact with pupils, parents/carers is required during off-site activities. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and contact the school
- School mobile phones and associated cameras will only be used during lessons or formal school time as part of curriculum activity.
- Pupils will be provided with school mobile devices to use in specific learning activities under the supervision of a member of staff.
- The sending of abusive, offensive or inappropriate material is not permitted.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the GDPR regulations 2018

Policy Decisions

Authorising Internet access

- All staff must read and sign the relevant 'Acceptable Use Agreement' before using school IT resources.
- Parents will be asked to sign and return a consent form.
- Pupils must agree to comply with the Responsible Internet Use statement before being granted Internet access**.**
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school IT resources' form before being allowed to access the Internet on the school site.
- The school will maintain a current record of any staff and pupils who are refused granted access to school IT systems.

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 referred to the Designated Safeguarding Lead and dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Community use of the Internet

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

Communications Policy

Introducing the E-safety policy to pupils

- Appropriate elements of the E-safety policy will be shared with pupils
- E-safety information will be placed in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

Staff and the E-safety policy

- All staff will be given the School E-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.
- Staff who manage filtering systems or monitor ICT use by the school will have clear procedures for reporting issues**.**

Enlisting parents' support

- Parents/carers' attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- The school will ask all new parents and pupils to sign the parent /pupil Acceptable Use Agreement when they register their child with the school. A master copy of the Agreement will be available on the school website for reference.
- Parents and carers will from time to time be provided with additional information on E-safety.

Associated Documents : Social Media Policy ; GDPR ; Safeguarding Policy ; Staff Code of Conduct ; Acceptable Use Agreements

22/2/19