LINCOLN ANGLICAN ACADEMY TRUST
DIOCESE OF LINCOLN

Wrawby St Mary's CE Primary

E-Safety Policy - Including Internet use

Created: May 2024
Review date: May 2027

E-Safety Policy – including Internet Use

E-Safety or online safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible IT / Computing use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of internet filtering.

1 Writing and reviewing the e-Safety Policy

The e-safety Policy relates to other policies including those for Computing, bullying and for child protection, including Preventing Radicalisation and Extremism. This policy has been written by the school, building on the Kent e-Safety Policy and government guidance. The policy and its implementation will be reviewed annually and where necessary in cases of reported misconduct or risks.

2 Teaching and learning

2.1 Why Internet use is 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. A framework of e-safety training has been developed and embedded within the computing scheme of work. This includes educating pupils on what is acceptable internet use and how to conduct effect effective research including skills of information location, retrieval and evaluation.

2.2 Internet content

Pupils should be taught:

- Skills of **Information Literacy,** that is, to be critically aware of the materials they read and the importance of cross-checking information before accepting its accuracy.
- How to report unpleasant internet content.

2.3 Email and other cloud applications (Office 365)

Pupils should be taught:

- About the risks of ‘spam’ and ‘spoofing’ and how to report it.
- About the risks of opening attachments from unknown senders.
- How to identify and report cases of grooming.
- About the seriousness of e-bullying / online bullying when partaking in discussions, emails and instant messages.
- How to correctly reference materials they have found from other sources so as not to infringe copyright or the intellectually property of others.
- How to communicate and collaborate appropriately by becoming increasingly aware of Netiquette.

2.4 Portable Devices

Pupils should be taught:

- That due to portable devices always being accessible, there are dangers of overuse (and therefore social exclusion) of and unsolicited contact by text and picture message through mobile phones.

2.5 Videoconferencing/Webcams

Pupils should be taught:

- The appropriate behaviours/conduct to adopt when using a webcam.
- The dangers of using a webcam outside of school.

3 Managing Internet Access and Other Technologies

3.1 Information system security

- School IT systems capacity and security will be reviewed regularly.
- All staff possess individual logins and passwords to the school network with appropriate access rights and privileges. When needed pupils will be provided with an individual login and password.
- Virus protection is installed on all school computers and updated regularly in light of new **viruses** and **Trojan horses** that weaken the school's security.
- Staff must ask permission from the Executive Headteacher before installing software on any school machines.

3.2 Internet

- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils are forbidden from downloading games or other programmes from the Internet.
- Staff must ask the permission of the ICT coordinator before downloading programmes from the internet.
- Public **chat-rooms** and **instant messaging** are not allowed and are blocked using the school internet filter.
- Access to **peer-to-peer** networks is forbidden in school.
- Children must adhere to the Internet Use agreement which has been signed by parents and themselves.
- Securly web filtering will alert the Executive Headteacher should any member of staff or pupil be found to be searching for inappropriate content online.

3.3 Email

Pupils may only use approved Office 365 email accounts on the school system.

- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Staff should never use personal email addresses to communicate with pupils. All staff have an official school email address.

3.4 Portable Devices

- Only school mobile phones will be used during lessons or formal school time, unless agreed by the Head of School. The sending of abusive or inappropriate text messages is forbidden.
- Staff should be aware that technologies such as portable Laptops, tablets and mobile phones may access the internet by bypassing filtering systems and present a new route to undesirable material and communications.
- Staff should not use their personal mobile phones to contact pupils or capture photographs of children. Alternative equipment will be provided by the school.

3.5 Learning Platform (Office 365)

- A secure username and password will be used on Office 365 by both staff and pupils. The correct levels of privilege are applied the correct users.
- Activity on the Learning Platform will be monitored to ensure that the content posted by users is valid and does not infringe the intellectual property rights of others.
- Children are to be encouraged to use an 'avatar' rather than their own photo.

3.6 Published content and the school web site

- The contact details on the school website should be the school address, email and telephone number. Staff or pupils personal information will not be published.
- The school's office staff will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.7 Publishing and storing pupils' images and work

- Pupils' full names will not be used anywhere on the website or blog, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil image file names will not refer to the pupil by name.
- Pupil image files should be securely stored on the school network.

3.8 Social networking, personal publishing and blogging

- School will block/filter access to social networking sites.
- 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.

3.9 Managing filtering

- The school will work in partnership with their IT technicians, to ensure systems to protect pupils are reviewed and improved. The current filtering for the internet is Securly.
- If pupils discover unsuitable material, it must be reported to their teacher or TA. Office staff will then contact Securly/Computeam who will ensure the material is blocked with immediate effect.
- Suitable material which is blocked by filtering can be unblocked by Securly/Computeam
- The filtering system will be reviewed with advice from Computeam

3.10 Managing videoconferencing

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised.

3.11 Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.12 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4 Policy Decisions

4.1 Authorising Internet access

- All staff must read and sign the Staff Code of Conduct and the IT User and Social Media Policy before using any school IT resource.
- Reception pupils and Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign an agreement on entry to school to pertain to the schools Code of Conduct regarding internet access.
- The school's wireless access points are encrypted to prevent outside access.

4.2 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 device. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- It is the responsibility of all staff to be aware of pupils' use of the internet, email and messaging services.

4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with according to the school's complaints policy should it be deemed necessary.
- Any complaint about staff misuse must be referred to the Head of School.
- 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 possible consequences for pupils misusing the Internet.
- The Police will be consulted to establish procedures for handling potentially illegal issues.

5 Communications Policy

5.1 Introducing the e-Safety Policy to pupils

- There is a code of conduct for pupils explaining their responsibilities.
- Pupils will be informed that network and Internet use will be monitored.

5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff will read and sign a code of conduct regarding internet and technology use. This is to ensure the safety of pupils and themselves.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school web site.
- Parents/carers will read and sign an e-safety agreement which consents to their children using internet services in school and states that they understand the school safety procedures.
- The school will ask all new parents to sign the parent/pupil code of conduct when they register their child with the school.

Glossary

Acceptable Use Policy A policy that a user must agree to abide by in order to gain access to a network or the internet. In the schools context, it may also cover how other communications services, such as mobile phones and camera phones, can be used on the school premises.

Avatar A graphic identity selected by a user to represent him/herself to the other parties in a **chat-room** or when using **instant messaging**.

Chat-room An area on the internet or other computer network where users can communicate in real time, often about a specific topic.

Filtering A method used to prevent or block users' access to unsuitable material on the internet.

Information Literacy The ability to locate pertinent information, evaluate its reliability, analyse and synthesise it to construct personal meaning and apply it to informed decision making.

Instant messaging(IM) A type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet, analogous to a telephone conversation but using text-based, not voice-based, communication.

Peer-to-peer (P2P) A peer-to-peer network allows other users to directly access files and folders on each others computer. File sharing networks such as 'Lime Wire' create weaknesses in networks security by allowing outside users access to the schools resources.

Spam Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

Spoofing Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Trojan Horses A virus which infects a computer by masquerading as a normal program.

Video Conferencing The process of conducting a conference between two or more participants over a network, involving audio and often text as well as video.

Virus A computer program which enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.

Webcam A webcam is a camera connected to a computer that is connected to the internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.