Leek High School

Online Safety Policy

Contents

Signed by:

_____ Headteacher Date: _____

_____ Chair of governors Date: _____

Introduction

At Leek High School, we understand that computer technology is an essential resource for supporting teaching and learning. The Internet, and other digital and information technologies, open up opportunities for students and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe Internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the Internet and other digital technology devices by all students and staff.

The school is committed to providing a safe learning and teaching environment for all students and staff and has implemented important controls to prevent any harmful risks.

1. Legal framework

1.1. This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997

1.2. This policy also has regard to the statutory DfE (2018) guidance 'Keeping children safe in education'.

2. Use of the Internet

2.1. The school understands that using the Internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all students, though there are a number of controls the school is required to implement to minimise harmful risks.

2.3. When accessing the Internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to students or staff due to inappropriate Internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

3.2. The **Local Governing Body (LGB)** is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard students when they are using school systems to access e-mail or use the Internet.

3.3. The **Online Safety Coordinator**, **Mr Phillip Evans**, is responsible for ensuring the day-to-day online safety in the school and managing any issues that may arise.

3.4. The **Systems Manager**, **Mr Matthew Wheeldon**, is responsible for the day-to-day management of access to school computer systems, online filtering and monitoring users.

3.5. The **Headteacher** is responsible for ensuring that the **Online Safety Coordinator** and any other relevant staff receive appropriate training to allow them to fulfil their role.

3.6. The **Online Safety Coordinator** will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach students about online safety.

3.7. The **Headteacher** will ensure there is a system in place which monitors and supports the **Online Safety Coordinator**, whose role is to carry out the monitoring of online safety in the school, keeping in mind data protection requirements.

3.8. The **Online Safety Coordinator** will regularly monitor the provision of online safety in the school and will provide periodic feedback to the senior leadership team.

3.9. The **Online Safety Coordinator** will ensure that online safety incidents are logged in the school behaviour recording and, where appropriate, safeguarding reporting/tracking systems.

3.10. The **Online Safety Coordinator** will ensure that all members of staff are aware of the procedure when reporting online safety incidents.

3.11. Cyberbullying incidents will be reported and dealt with in accordance with the school's **Anti-Bullying Policy**.

3.12. The **Headteacher** will review and amend this policy with the **Online Safety Coordinator**, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.

3.13. Teachers are responsible for ensuring that online safety issues are embedded in the curriculum and safe Internet access is promoted at all times.

3.14. All staff must ensure they are up-to-date with current online safety issues and this Online safety Policy.

3.15. All staff and students will ensure they understand and adhere to our **Acceptable Use Agreement**, which they must sign and return to the Headteacher.

3.16. Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

3.17. The **Online Safety Coordinator** is responsible for communicating with parents/carers regularly and updating them on current online safety issues and control measures.

3.18. All students are aware of their responsibilities regarding the use of school computer systems, including their expected behaviour when using e-mail or the Internet.

4. Online safety education

4.1. Educating students:

- An online safety programme will be established and taught across the curriculum on a regular basis, ensuring that students are aware of the safe use of new technology both inside and outside of the school.
- Students will be taught about the importance of online safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.
- Students will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of Internet use will be presented in all computer rooms.
- Students are instructed to report any suspicious use of the Internet and personal digital devices.
- PSHE sessions will be used to educate students about cyber bullying, including how to report cyberbullying, the social effects of spending too much time online and where to access help.
- The school will hold online safety events, such as Safer Internet Day and Anti-Bullying Week, to promote online safety.

4.2. Educating staff:

- All staff will undergo regular online safety training to ensure they are aware of current online safety issues and any changes to the provision of online safety, as well as current developments in social media and the Internet as a whole.
- The **Online Safety Coordinator** will audit staff regularly order to identify areas of training need.
- All staff will employ methods of good practice and act as role models for students when using the Internet and other digital devices.

- All staff will be regularly updated on websites that are deemed inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- New staff are required to undergo online safety training as part of their induction programme, ensuring they fully understand this policy.
- The **Online Safety Coordinator** will act as the first point of contact for staff requiring online safety advice.

4.3. Educating parents/carers:

- Online safety information will be directly delivered to parents/carers through a variety of formats, including the school website and social media.
- Parents/carers' evenings, meetings and other similar occasions will be utilised to inform parents/carers of any online safety related concerns.

5. Online safety control measures

5.1. Internet access:

- Internet access will be authorised once parents/carers and students have returned the signed consent form in line with our **Acceptable Use Agreement**.
- A record will be kept of all students who have been granted Internet access.
- All users will be provided with **usernames** and **passwords** and must keep these confidential to avoid any other user using their login details.
- User passwords must be changed on a regular basis and their activity is continuously monitored by the **Systems Manager**.
- Effective filtering systems will be established to eradicate any potential risks to students through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- Filtering systems will be used which are relevant to students' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- The **Online Safety Coordinator** and **Systems Manager** will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions to the online resources students can access.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the **Online Safety Coordinator** or **Systems Manager**.
- All school systems will be protected by up-to-date virus software.

- An agreed procedure will be in place for the provision of temporary users, e.g. guest students and adult volunteers.
- Staff are able to use the Internet for personal use out-of-school hours, as well as at break and during lunch.
- Personal staff use will only be monitored by the Online Safety Coordinator for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.
- Inappropriate Internet access by staff will be dealt in accordance with the **Staff Code of Conduct**.

5.2. Email:

- Students and staff will be given approved email accounts and are only able to use these accounts.
- The use of personal email accounts is prohibited.
- No sensitive and/or personal data shall be sent to any other students, staff or third parties using email.
- Students are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
- Staff members are aware that their email messages are not monitored.
- Any emails sent by students to external organisations will be overseen by a member of staff and must be authorised before they are sent.
- Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

5.3. Social media and networking:

- Use of social media on behalf of the school will be conducted following only with the prior approval of the **Headteacher**.
- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Online Safety Coordinator.
- Students are regularly educated on the implications of posting photos or personal information online outside of the school.
- Students are not permitted to take or publish photographs/video of other students or staff.

- Staff are regularly educated on posting inappropriate photos or information online, which may adversely affect them and/or the school.
- Staff are not permitted to communicate with students over social networking sites and must keep ensure that their privacy settings prevent students from communicating with them.
- Staff are not permitted to publish comments about the school which may adversely affect its reputation.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the **Online Safety Coordinator** prior to accessing the social media site.

5.4. Published content on the school website:

- The **Headteacher** will be responsible for the overall content of the website and will ensure that this is appropriate, accurate and up-to-date.
- Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or students will be published.
- Photographs and full names of students, or any content that may easily identify a student, will be selected carefully, and will not be posted if consent from parents/carers has not been given.
- Staff are able to take photographs, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take pictures using personal digital devices.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

5.5. Personal digital devices (mobile devices and hand-held computers):

- Staff may authorise the use of a personal digital device by a student where it is seen to be for safety or precautionary use.
- Students are permitted to access the school's Wi-Fi system at any times using their own personal digital devices.
- Mobile phones must not be used during teaching hours by students or staff unless it actively supports learning.
- Staff are permitted to use hand-held computers which have been provided by the school, though Internet access will be monitored for any inappropriate use.

- The sending of inappropriate messages or images from mobile phones is prohibited.
- Personal digital devices will not be used to take photographs or videos of students or staff.
- The school will be especially alert to instances of cyberbullying and will treat such instances as a matter of high priority.

5.6. Network security:

- Network profiles for each student and staff member are created, in which the individual must enter a username and personal password when accessing the computer systems within school.
- Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.
- Passwords will expire after 90 days to ensure maximum security for student and staff accounts.
- Passwords are stored using non-reversible encryption.

5.7. Virus management:

- Technical security features, such as virus software, are kept up-to-date and managed by the **Systems Manager**.
- The **Systems Manager** will ensure that the filtering of websites and downloads is up-to-date and monitored.

6. Cyberbullying

6.1. For the purpose of this policy, cyberbullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

6.2. The school recognises that both staff and students may experience cyberbullying and will commit to preventing any instances that should occur.

6.3. The school will regularly educate staff, students and parents/carers on the importance of staying safe online, as well as being considerate to what they post online.

6.4. Students will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE sessions.

6.5. The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and students.

6.6. The school has zero tolerance for cyberbullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our **Anti-Bullying Policy**.

6.7. The **Online Safety Coordinator** will decide whether it is appropriate to notify the police of the action taken against a student.

7. Reporting misuse

7.1. Leek High School will clearly define what is classed as inappropriate behaviour in the **Acceptable Use Agreement**, ensuring all students and staff members are aware of what behaviour is expected of them.

7.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to online safety are explained to students as part of the curriculum in order to promote responsible Internet use.

7.3. Misuse by students:

- Teachers have the power to discipline students who engage in misbehaviour with regards to Internet use.
- Any instances of misuse should be immediately reported to a **pastoral leader** or the **Student and Welfare Support Officer**, who will then report this to the **Online Safety Coordinator**.
- Any student who does not adhere to the rules outlined in the **Acceptable Use Agreement** and is found to be wilfully misusing the Internet, will have a letter sent to their parents/carers explaining the reason for suspending their Internet use.
- Other forms of disciplinary action to a student upon the misuse of the Internet. This will be discussed and agreed with the **Online Safety Coordinator**.
- Complaints of a child protection nature, such as when a student is found to be accessing extremist material, will be dealt with in accordance with our **Child Protection and Safeguarding Policy**.

7.4. Misuse by staff:

- Any misuse of the Internet by a member of staff should be immediately reported to the **Online Safety Coordinator**.
- The **Online Safety Coordinator** will deal with such incidents in accordance with the **Allegations of Abuse Against Staff Policy** and may decide to recommend that the **Headteacher** takes disciplinary action against the member of staff.

- The **Online Safety Coordinator** will decide whether it is appropriate to notify the police or LADO of the action taken against a member of staff.

7.5. Use of illegal material:

- In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
- If a child protection incident is suspected, the school's child protection procedure will be followed.

8. Monitoring and review

8.1. The Online Safety Coordinator will regularly evaluate and review this policy taking into account the latest developments in technology and feedback from staff/students.

8.2. This policy will be reviewed in full by the Local Governing Body on an annual basis; any changes made to this policy will be communicated to all members of staff.