Online Safety Policy

Formby High School
Determined To Achieve

Policy Approved: 21 November 2017 (Governing Body)
Scheduled Review: November 2020

The Formby High School Online Safety Policy, and the procedures contained therein, reflect the philosophy set out in the School's Mission Statement, particularly with reference to the provision of a 'safe and pleasant environment for effective learning' and 'to foster self-esteem, mutual respect and good behaviour'.

The purpose of internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the School's management information and business administration systems.

This policy provides a framework to help staff and students remain safe online and develop their knowledge and understanding. Those whose behaviour is unacceptable are dealt with in a firm, fair and reasonable way so as to support the staff and students as individuals, yet demonstrate clearly that certain patterns of behaviour are unacceptable.

This policy forms part of the overall arrangements for safeguarding as set out in the Safeguarding Policy. Formby High School fully recognises its responsibilities for online safety.

All staff and students must agree to abide by the School ICT Acceptable Usage Policy prior to using any School ICT facilities.

Development, Monitoring and Review of this Policy

This Online Safety Policy has been developed by a working group made up of:

- Designated Senior Person for Safeguarding
- Members of the School Leadership Team
- ICT Network Manager
- Teaching and support staff
- Governors

The Governing Body will monitor the implementation of the policy, receiving regular updates from the Headteacher. The policy will be reviewed by the Governing Body on a three yearly basis.

Definition of Key Terms

- **The School** – Formby High School
- **School system users** – all individuals who may have cause to use the school's ICT network and / or hardware, including staff, students, trainee teachers, staff employed by third party contractors/lettings , parents, Governors and visitors.

Scope of the Policy

This policy applies to all school system users who have access to and are users of the School ICT systems, both in and out of the School.

The Education and Inspections Act (2006) empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of School hours, but is linked to membership of the School.

The School will deal with such incidents within this policy and associated Behaviour and Discipline, Mobile Phone and Anti-Bullying policies, and may inform parents/carers of incidents of inappropriate online safety behaviour that take place inside and outside of the School.

Context

Technology is playing an ever increasing part in our day to day activities, both inside and outside of school, and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, students and parents/carers associated with the School are able to use technology in a safe and responsible manner.

Some of the potential dangers of using technology may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom contact is made on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the offline world but it is important that as a School we have a planned and coordinated approach to ensuring that all those who use School technology do so in a safe and responsible way. As with all risks, it is impossible to eliminate them completely but with a

planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

Policies and practices

The Online Safety Policy outlines the importance of ICT within and outside of education. It provides guidance on the School's approach to online safety and, along with the ICT Acceptable Usage Policies, details a code of conduct for school system users. The policy aims to provide an agreed, coordinated and consistent approach to online safety. This code of conduct forms the basis of the School's expected behaviours regarding the use of technology and any infringements of the code of conduct may lead to disciplinary action against the perpetrator(s).

Infrastructure and technology

The School ICT systems are compliant with current statutory guidance/requirements. They are reviewed and actioned upon as and when required. This incorporates a combination of content filtering, monitoring and real time alerting. The ICT Network Manager will carry out checks to ensure that the filtering methods selected are appropriate, effective and reasonable as instructed by the Designated Safeguarding Lead (DSL). Virus protection will be installed and updated on a regular basis. Executable files (files that can be run as a program on a computer) will not be allowed to be saved in students' work areas.

Education and training

As the use of technology and the potential risks associated with the use of technology change rapidly, it is essential to ensure that the School community know how to use technology safely and responsibly. Staff will undertake annual training on online safety in order to raise awareness and keep up to date with new technologies. An online safety curriculum that meets the needs of all students and ensures their safety and well-being is delivered through Computing and PSHEE lessons. The topic is also frequently addressed in assemblies. The curriculum is reviewed and revised on a regular basis to ensure that it remains current.

Standards and inspection

The School reviews its approach to online safety on a regular basis. Reference is also made to online safety in the annual Safeguarding audit (S175) and through Ofsted inspections.

Policy Statements

As part of the Online Safety Policy the School will manage:

- Internet access by students
- The use of digital images and video
- Data protection
- Digital communications
- The handling of inappropriate online use

Internet access

The Internet is an essential element of 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 means through which the curriculum can be delivered and enriched and is a necessary tool for staff and students.

- All school system users must read and conform to the ICT Acceptable Usage Policy, as well as accepting the system disclaimer message upon log-in, before using any School ICT resource or facilities.
- School internet access is designed expressly for student use and will include filtering appropriate to the age of students.
- The School will take all reasonable precautions to ensure that only appropriate material

is accessed by all users. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never be accessed via the School computer system.

- The School will block/filter access to social networking sites on School computers. Students may be given access to social media sites if it is deemed a necessary part of their current curriculum. Students will not be allowed access to public or unregulated chat rooms.
- The School will ensure that the use of internet derived materials, both by staff and students, complies with copyright law and that staff and students adhere to the School's Data Protection Policy.
- School system users should report any breaches, or suspected breaches, of the ICT Acceptable Usage Policy to a member of staff immediately.
- Any student failing to adhere to the ICT Acceptable Usage Policy will be sanctioned according to the School's Behaviour and Discipline Policy.
- The School will keep a record of any student who is restricted from the internet.
- Through the Computing curriculum, students will be taught what internet use is/is not acceptable and given clear objectives for internet use.
- Students will be educated in the effective use of internet research, including the skills of knowledge location, retrieval and evaluation.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Through the PSHEE programme, Anti-Bullying and annual Safer Internet Day and the Computing curriculum, students will be taught never to give out personal details of any kind which may identify them or their location.
- The School will provide information and awareness to parents and carers through letters, newsletters, school website, and signposting parents to relevant websites, parents' information evenings and online safety workshops.
- Students will be shown how to report any inappropriate use or material.
- Staff will be provided with regular updates and training on online safety and use of the School's ICT resources.
- Any form of bullying or harassment is strictly forbidden and any student undertaking such behaviour will be sanctioned in accordance with the Anti-Bullying Policy and the Behaviour and Policy.

The use of digital images and video

The development of digital imaging technologies has created significant benefits to learning, allowing School staff and students instant use of images they have recorded themselves or downloaded from the internet. School staff and students are made aware of the potential risks associated with storing, sharing and posting images on the internet and must follow the good practice detailed below:

- When using digital images, staff will inform and educate students about the risks associated with the taking, using, sharing, publishing and the distribution of images. In particular, students will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are permitted to take digital images and video to support educational aims, but must follow School policies concerning the sharing, distribution and publication of those images. A school camera is available to borrow from the Administration department. Images that are taken by staff using a personal device should be destroyed or transferred to the School network where they may be stored appropriately and used for work purposes.
- Care will be taken when capturing digital images and video that students are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.

- Images and videos published on the School website or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- In order to safeguard all students, the School will avoid using full names in association with their photograph on the School website. Please refer to the Child Protection Policy for further information.
- Permission from parents or carers will be obtained before photographs of students are published on the School website or in any other promotional material.

Data Security and Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

All School Staff and students will follow the guidelines set out in the Data Protection Policy.

- Care is taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Personal data is used or processed on only secure password protected computers and other devices and that these devices are properly "logged-off" at the end of any session in which they are using personal data.
- Staff must adhere to the content of the Data Protection Act 1998 and the School's Data Protection Policy, particularly in relation to staff or student personal data and pictures.
- Staff must ensure that personal data or images relating to students (or staff) are processed in line with the Data Protection Act 1998.
- Personal data or images relating to students must not be sent via external email, over the internet or via other messaging systems.
- Personal data or images relating to students (or staff) may only be held on the School network and must not be saved to an external drive without prior permission from the Designated Senior Person. The Designated Senior Person should be consulted prior to commencing any activity or process relating to student personal data or images.
- Where it is necessary for personal data or images relating to students (or staff) to be removed from the School premises, due regard should be given to ensure its safety and security and the member of staff in possession of such information is responsible for ensuring it is stored appropriately using encryption and password protection.
- Where school system users access the School's ICT systems remotely all of the above policy statements apply.

Digital Communication

Digital communication is an area that is developing rapidly with new and emerging technologies, devices are becoming more mobile and information sharing/communication is becoming more sophisticated.

When using communication technologies the School ensures the following good practice:

- The official School email service is regarded as safe and secure and is monitored. Staff should therefore use only school email facilities when communicating on a school related matter.

- Users need to be aware that email communications may be monitored.
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, students or parents/carers must be professional in tone and content. These communications may only take place on official school accounts and be in line with all applicable school policies. Personal email addresses and /or text messaging using personal phones should not be used. Social networking may be used for work purposes.
- Students will also be taught strategies to deal with inappropriate emails and digital communication, and be reminded of the need to communicate clearly and correctly and not include any unsuitable or abusive material.
- Personal information will not be posted on the School website and only official email addresses should be used to identify members of staff.
- All students will be made aware of the School's Mobile Phone Policy and will be expected to adhere to it at all times.
- Students will be instructed about safe and appropriate use of mobile telephones and other handheld electronic devices, both on and off the site, in accordance with the School's Acceptable Usage Policy and Mobile Telephone Policy.
- Emerging technologies will be examined for educational benefit before being considered for use in the School.

Handling inappropriate online use

In the event of an online safety incident it is important that there is a considered, coordinated and consistent approach. Incidents will be managed using the incident flowchart. Any breach, or suspected breach, of the School's ICT Acceptable Usage Policy by a student will be investigated by the Climate for Learning Leader and, if required, will be referred to a member of the DSL. Complaints of a Child Protection nature must be dealt with in accordance with the School's Child Protection Policy. Any breach, or suspected breach, of the School's ICT Acceptable Usage Policy by a member of staff will be referred to the Headteacher.

INCIDENT FLOW CHART