WESTLEIGH HIGH SCHOOL
Aspiring & Achieving Together

E-SAFETY POLICY

The aim of this policy is to outline the procedures to ensure that students use technology safely. It is also useful to read the Acceptable Use Policy in conjunction with this e-Safety Policy.

The eSafety Lead in school is Mrs J Coleman. This e-Safety policy has been written in conjunction with the Wigan Safeguarding Children Board (WSCB) e-Safety strategy and government guidance. It has been approved by the Senior Leadership Team and Governors.

1. Learning

1.1 Why the Internet and digital communication are important

Technology, including the Internet, is an essential element in 21st century life for education, business and social interaction. As a school, we have a duty to provide our students with high-quality access to technology as part of their learning experience. The school computer network and Internet access is designed expressly for student use and includes age-appropriate filtering and monitoring.

1.2 Internet use will enhance and extend learning

Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students. Staff are made aware of and students are educated in the safe use of the Internet, which includes setting and discussing clear boundaries for the appropriate use of the Internet and digital communications.

1.3 Students will be taught how to evaluate Internet content

Students are also educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. The use of Internet derived materials by our users will comply with copyright law. Please also refer to the schools Acceptable Use Policy which further outlines acceptable use.

2. Managing Internet Access

2.1 Information system security

The security of our school computer network is reviewed regularly and anti-virus software is installed and updated.

2.2 Email

- Students and staff should only use the approved email accounts at westleigh.wigan.sch.uk.
- During ICT and PSHE lessons, students are made aware of how to stay safe online and how to report abuse, including email. Students must report if they receive offensive or inappropriate email.
- Students are taught that they must not reveal their personal details or those of others, or arrange to meet anyone without specific permission; this is via social media, email communication or any other platform.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

- Students can report abuse to members of school staff who will then inform the e-Safety Lead. The Report Abuse icon (eye on legs) is also available on the school homepage; students are made aware that this is another way they can report abuse.

2.3 Published content

Personal contact information for both staff and students will not be published on the school website or Virtual Learning Environment (Moodle). The contact details given online will be the main office.

2.4 Publishing student' images

Photographs that include students are carefully selected so that images of students cannot be misused. Students' full names will not be used anywhere on the school website or Moodle, particularly in association with photographs. Written permission, using the approved permission form, from parents or carers will be obtained before photographs of students are published on the school website or Moodle. An updated list is maintained on SIMs and managed by staff in the Pupil Office.

2.5 Social networking and personal publishing

The school educate staff and students in the safe use of social networking sites and educate students' in their safe use. This is carried out via ICT lesson, PSHE lessons, assemblies and for staff in particular, through online training provided by Wigan Safeguarding Children's Board

Students are advised never to give out their personal details of any kind that could identify them, their friends or their location. Students can report abuse to members of school staff who will then inform the e-Safety Lead. The Report Abuse icon (eye on legs) is also available on the school homepage; students are made aware that this is another way they can report abuse.

Students are taught the reasons why personal photographs or videos should not be posted online without considering how the media can be used in now or in the future. Where cyberbullying is suspected, this will be considered as unacceptable and will trigger an investigation. Please refer to the Acceptable Use Policy for further information relating to cyberbullying.

Students are also advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others. Please also refer to our Social Media Policy.

2.6 Managing monitoring and filtering

Our school work in partnership with Wigan Council to ensure that systems to protect our students are reviewed and improved. The computer network is also monitored by **e-safe Systems** who provide an integrated and comprehensive approach to e-Safety, alerting us to any potential concerns. **e-safe Systems** deliver a suite of leading edge forensic monitoring software that provides the ability to:

- detect inappropriate and illegal images;
- identify grooming, cyber bullying, radicalisation, suicide and self-harm through text and website detection;
- improve productivity through the control of general internet and ICT misuse
- secure confidential data & monitor user activity to identify internal threats
- encourage more responsible use of ICT and the Internet.

In support of the Prevent Duty, **e-safe systems** monitors online radicalised and extremist actions in all languages and scripts.

If staff or students discover an unsuitable site, it must be reported to the eSafety Lead or the Network Manager.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.7 Managing videoconferencing

Videoconferencing should use the Wigan Video Conferencing Network to ensure quality of service and security rather that the Internet. Students should ask permission from the supervising teacher before making or answering a videoconference call. Videoconferencing will be appropriately supervised for the students' age.

2.8 Managing emerging technologies

Emerging technologies are examined for their educational benefit and risk assessed before use in school is allowed. The Senior Leadership Team are aware that technologies such as mobile phones with wireless Internet access can bypass our school filtering systems and present a new route to undesirable material and communications. Please refer to our Mobile Phone Policy which outlines responsible use and consequences.

Where contact with students is required to facilitate their learning staff will be issued with a school phone.

2.9 Protecting personal data

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

3. Policy Decisions

3.1 Authorising Internet access

All staff must read and sign the 'Staff Acceptable Use Policy and Code of Conduct for ICT' before using any school ICT resource, including any laptop issued for professional use. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Our students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement contained within the school's Acceptable User policy.

Parents/carers will be asked to sign and return a consent form.

3.2 Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Wigan Council can accept liability for any material accessed, or any consequences of Internet access.

Our school 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.

Our school ensures monitoring software and appropriate procedures are in place to highlight when action needs to be taken by the school.

3.3 Handling e-Safety complaints

Complaints of Internet misuse will be reported to the e-Safety Lead and action in line with the Wigan Safeguarding Children Board e-Safety policy will be taken.

Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children will be reported to the LADO within one working day in accordance with Wigan Safeguarding Board policies.

Any complaint about staff misuse must be referred to the head teacher and if the misuse is by the head teacher it must be referred to the chair of governors in line with Wigan Safeguarding Board Child Protection procedures.

Students, parents and staff will be informed of the complaints procedure

4. Communicating e-Safety

4.1 Introducing the e-safety policy to pupils

E-Safety rules are posted in all rooms where computers are used.

All system users are informed that network and Internet is monitored.

A programme of e-Safety training and awareness raising has been put in place in line with the Wigan Safeguarding Children Board's e-Safety Strategy.

4.2 Staff and the e-Safety policy

All staff are given access to the School e-Safety Policy and its importance explained.

Staff are informed that network and Internet traffic is monitored and traced to the individual user, including staff laptops.

Staff that manage filtering systems or monitor ICT use will be supervised by senior leadership and work to clear procedures for reporting issues.

Staff should understand that phone or online communications with students can lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

4.3. Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school magazine and on the school website.

Adopted by the Board of Governors and recorded in the Minutes of the meeting held on:	**J Holland** **Chair of Governors** **14/09/2015**
Review Date	September 2016
Headteacher	**C Bramwell**