Online Safety Policy

Mayfair school of English is committed to ensuring online safety. The Online Safety policy covers the use of the computing systems, equipment and software in school. It also includes issues such as social networking, online-bullying, data protection, passwords, filtering, digital and video images and use of mobile devices. The policy clearly states the school's commitment to act on online safety incidents outside the school that affect the well-being of staff and students.

1 Roles and Responsibilities

1.1 The Designated Safety Lead (DSL) person and Deputy Designated Safeguarding Leads are responsible for monitoring incidents and handling sensitive issues should they arise. It is, however, the responsibility of all staff to be vigilant with regard to the use of school technology.

1.2 Access to the Network

The school IT Manager is responsible for technical security. Devices and network equipment are secured and managed by the network manager who also ensures that antivirus software is in place for all school systems.

2 Acceptable use of technology

Guidance on the acceptable use of technology is provided for all users on the school site. These expectations are clearly communicated to new students in the school induction. It is clear to staff that acceptable use forms part of their contract.

3 Safeguarding

There are clear links between the school online safety policy and sections of other policies such as Equal Opportunities, Admissions, Prevent and the Safeguarding Policy.

Students are aware of online safety issues and acceptable use. Students have access to a student Wifi which has restricted access.

4 Unacceptable use of technology

Wireless Internet access for students and visitors is filtered for all users and regularly updated. The school may take action and intervene where there is a breach of the acceptable use guidelines. This may apply inside or outside school.

All users are encouraged to be responsible and risk-aware when using the internet and social media, both in school and beyond.

Unacceptable use includes but is not limited to:

- Illegal content such as sexually explicit content, radicalisation, terrorism, racism
- Bullying and harassment
- Footage of real or simulated violence, criminal activity or accidents from video clips, games or films

- Content instructing or promoting crime or violence.
- Posting anyone else's personal information over networks

Procedures for reporting abuse or incidents must be followed as outlined below:

- All users (staff or students) have a responsibility to report online safety incidents to the DSL.
- Incidents are recorded and handled with discretion and may involve other support agencies (eg local authority and regional broadband grid) if necessary.
- Any breach of standards as outlined in the school Equal Opportunities Policy may result in sanctions such as a warning or exclusion from school.

5 Use of Digital Images

Parental permission for Under 18s is needed when publishing personal images on the website or other publications. All members of the school understand their rights and responsibilities in the taking, use, sharing, publication and distribution of images. Digital images are securely stored in accordance with the Data Protection Act.

6 Communication between Staff and Pupils

The school has in place protocols for communication between the staff and students. Staff understand that communication with young people and parents / guardians should take place only through official school systems (eg school email) and must be professional in nature.

6 Security and Data

Passwords protect the security of systems and data and are required by all staff to access networks and devices. Technology resources and all digital equipment are school property. The IT Manager may review files at any time in order to maintain the integrity of the system and to ensure responsible use of the technology. Users are prohibited from obtaining copies of files, or modifying the files, data or passwords of others and also from installing software on school computers.

7 Network access

Devices and network equipment are secure and managed. Antivirus & malware prevention is applied and regularly updated. System backups are an integral component of system recovery routines.

8 Data Protection

The school has a Data Protection Policy. All staff understand their statutory obligations under the Data Protection Act to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

9 Staff training

Online safety training is given in the staff induction and is also a component of Safeguarding training.

10 Reporting Incidents

Monitoring of online safety incidents takes place and records are kept in line with child protection procedures. Where monitoring identifies safeguarding issues, intervention takes place and will be referred to external agencies where appropriate. Parents are informed of online safety incidents, as relevant.

September 2017