E-Safety Policy

Introduction:
ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- iPad /Tablet / Portable IT devices
- Websites & Social Media
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Layfield, we understand the responsibility to educate our students on e-safety (online) issues; teaching them the appropriate behaviours to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for our school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, trustees, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, iPads, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by students and staff, but brought onto school premises (such as laptops, netbooks, mobile phones, camera phones, PDAs and portable media players, etc.).

The school works collaboratively with other Trust schools that have access to our systems.

Mobile Apps play an increasing role in how students work together using mobile technology.

E-Safety Policy

E-safety (Online) - Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-safety co-ordinator in this school is the Computing Co-ordinator. It is the role of the e-safety co-ordinator to keep abreast of current issues and guidance through organisations such as Stockton LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

The Executive Team, Trustees and Governors are updated by the Headteacher/ E-safety co-ordinator. All have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice. This policy, supported by the school's acceptable use agreements for staff, trustees, governors, visitors and pupils, is to protect the interests and safety of the whole school community.

E-safety (Online) in the Curriculum

ICT and online resources are used significantly across the curriculum. We believe it is essential for e-safety (online) guidance to be given to the pupils on a regular and meaningful basis. E-safety (online) is embedded within our curriculum and we continually look for new opportunities to promote e-safety (online). We also dedicate assembly time to discuss current e-safety (online) trends and concerns. In addition to this, we actively involve third parties (e.g. Police Community Support Officers) to discuss physical safety of devices, moving between home and school.

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Internet use is a part of the statutory curriculum and is a necessary learning tool for staff and pupils.

- Staff will preview any web sites, Apps or other digital resources before their use in school.
- Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues, or if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline.
- All IT systems have report abuse systems integrated within them. This includes school platforms, tablets and email systems. E-Safety (Online) co-ordinators are alerted of reports, where appropriate action is taken.
- As a school, we encourage responsible use over a 'block all' approach. We encourage pupils to use all digital systems and technology ethically, morally and responsibly; making mature choices when working digitally.

Virgin Media (Aspire) and Northern Grid provide filtering. The school has a Smoothwall filtering solution and all access is logged. The logs are randomly but regularly monitored and whenever any inappropriate use is detected it is investigated. Pattern matching technologies are used to detect unsafe activity under the PREVENT agenda. Upon triggering of an alert, the relevant year manager(s) are informed.

Managing ICT Systems and Access

The school is responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.

- The school uses management control tools for controlling and monitoring workstations.
- The school uses a mobile device management system to maintain tablet access to school systems.
- Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access.

- Servers, workstations and other hardware and software are kept updated as appropriate; in line with teaching and learning demands.
- Virus protection is installed on all appropriate hardware, and it is kept active and up-to-date.
- The school decides the appropriate level of access and supervision pupils should receive when using the internet.
- All users will sign an end-user Acceptable Use Policy (AUP), appropriate to their age and access.
- Users are made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity is monitored and checked.
- Whether supervised by a member of staff, or working independently, pupils will abide by the school AUPs at all times.
- Staff will abide by the school AUPs at all times.
- Out of the interests of child protection, staff will be subject to routine safeguarding checks of school tablets.
- Administrator or master passwords for school ICT systems are kept secure.
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur. The school will provide relevant access to new platforms, where a responsible approach will be taken in their use.
- The school will regularly audit ICT use to establish if the e-safety (online) policy is adequate and that the implementation of the e-safety (online) policy is appropriate.

By using IT facilities or by connecting tablets to school systems Layfield will use filtering and monitoring software (whilst on site) to ensure effective learning and for child/staff protection purposes.

Layfield will install device management software to provide school specific configurations such as connectivity settings, application delivery and restrictions (on the school site). This software will be active both on and off site for all school equipment.

Email & Digital Communications (Please see appropriate staff/student acceptable use policies).

The use of e-mail and digital communications (e.g. instant messaging) within most schools is an essential means of communication for both staff and students. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. Pupils are introduced to email as part of the ICT Scheme of Work.

- Staff and pupils should use approved e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system will be monitored and checked.
- Pupils are allocated an individual e-mail account for their use in school / classes
- Pupils are taught when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening email from an unknown sender, or viewing/opening attachments.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- Each email provides a method to report abuse in the event of inappropriate content received – this will be dealt with by the E-Safety (Online) Co-ordinator.