Esher Learning Trust

Online Safety and Mobile Phone Policy

Status: Approved
Date of Review: Statutory Policy – Annual Review
Responsibility: Student Wellbeing
Date of Approval: Student Wellbeing Committee: 5 October 2016
                         Provision Committee: 8 November 2016
                         Full Governors: 16 November 2016
                         ELT   5 December 2016 & 20 March 2017

This policy is based on the Surrey model policy and incorporating Mobile Policy, revised 2014

Online Safety is part of the Esher Learning Trust (ELT / The Trust) safeguarding responsibilities. This policy relates to other Trust policies including those for behaviour, safeguarding, anti-bullying, and staff Code of Conduct.

Using this policy

The school will form an Online Safety committee and will appoint an Online Safety Coordinator.

This policy covers the use of all technology which can access the school network and the Internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.

Managing access and security

The school will provide managed internet access to its staff and students in order to help students to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- The School will use a recognised and appropriate Internet service provider or regional broadband consortium.

- The School will ensure that all Internet access has age appropriate filtering provided by a recognised and appropriate filtering system, which is regularly checked to ensure that it is working, effective and reasonable.

- The School will ensure that its networks have virus and anti-spam protection.

- Access to school networks will be controlled by **personal** passwords.

- Systems will be in place to ensure that Internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform the Online Safety policy.

- The security of school IT systems will be reviewed regularly.

- **All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.**

- The School will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

Internet Use

- The school will provide an age-appropriate Online Safety curriculum that teaches students how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

- All communication between staff and students or families will take place using school equipment and/or school accounts.

- **Students will be advised not to give out personal details or information which may identify them or their location**

E-mail

- **Students and staff may only use approved e-mail accounts on the school IT systems.**

- Staff to student email communication must only take place via a school email address or from within the learning platform.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

- **The school will consider how e-mail from students to external bodies is presented and controlled.**

Published content e.g. school web site, school social media accounts

- The contact details will be the school address, email and telephone number. Staff or students' personal information will not be published.

- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing students' images and work

- Written permission will be obtained from parents or carers before photographs or names of students are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children

Use of social media including the School learning platform

- The School will control access to social networking sites, and consider how to educate students in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.

- Use of video services such as Skype, Google Hangouts and Facetime will be monitored by staff. Students must ask permission from a member of staff before making or answering a video call.

- Staff and students should use ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

Use of personal devices

- Personal equipment may be used by students to access the   school IT systems.

- Staff must not store images of students or student personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Protecting personal data

- Data handling is covered in ELT policies for example: the Staff Code of Conduct Policy, Data Protection and Retention of Records. These cover the use of biometrics in school, access to student and staff personal data on and off site, remote access to school systems.

Policy Decisions

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians, trustees and governors) must read and sign the 'Code of Conduct' before accessing the school IT systems.
- The School will maintain a current record of all staff and students who are granted access to school IT systems.
- People not employed by the school must read and sign the Code of Conduct before being given access to the Internet via school equipment.
- Parents will be asked to sign and return a consent form to allow use of technology and Internet access by their student.

Assessing risks

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

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt according to the ELT Behaviour/Code of Conduct policies.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of consequences and sanctions for students misusing the Internet and this will be in line with the schools' behaviour policy.

Community use of the internet

- Members of the community and other organisations using the school internet connection will have signed the Code of Conduct so it is expected that their use will be in accordance with the ELT Online Safety policy.

Communication of the Policy

To students and parents

- Students will be reminded about Acceptable Use as part of their Online Safety education and via Planners.

- The school will ask all new parents to sign the parent /student Home School agreement when they register their child with the school.

- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, and on the school web site.

- Parents will be offered Online Safety training annually.

To staff

- All staff will be shown where to access the Online Safety policy and its importance explained.

- All staff must sign and agree to comply with the Code of Conduct Policy in order to gain access to the school IT systems and to the internet

- All staff will receive Online Safety training on an annual basis.

Mobile Phone Usage

The school recognises that personal communication through mobile technologies is an accepted part of everyday life but that such technologies need to be used appropriately and safety.

Responsibility

It is the responsibility of students who bring mobile phones to school to abide by the guidelines outlined in this document.

The decision to provide a mobile phone to their children should be made by parents or carers. It is incumbent upon parents to understand the capabilities of the phone and the potential misuse of those capabilities.

Parents/carers should be aware if their child takes a mobile phone to school it is assumed household insurance will provide the required cover in the event of loss or damage. The school cannot accept responsibility for any loss, damage or costs incurred due to its use.

Students are responsible for their own mobile phone.

Parents/carers are requested that in cases of emergency, they contact the school office who can ensure their child is reached quickly and assisted in any relevant way. Passing messages through school reception also reduces the likelihood of disrupting lessons inadvertently.

Acceptable Uses

Mobile phones will be switched off (not just put on silent mode) and will be kept out of sight during classroom lessons, school assemblies, whilst moving through corridors and when in the library.

During break and lunch times only, and whilst in designated areas, students are permitted to use soundless features such as text messaging, answering services, call diversion and vibration alert to receive important calls.

Mobile phones should not be used in any manner or in any location that could cause disruption to the normal routine of the school.

Students should protect their phone numbers by giving them only to close friends and family. This will help protect the student's number from falling into the wrong hands and guard against insulting, threatening or unpleasant communications.

The school recognises the importance of emerging technologies present in modern mobile phones e.g. camera and video recording, internet access, MP3 and MP4 playback, blogging etc. Teachers may wish to utilise these functions to aid teaching and learning and students may have the opportunity to use their mobile phones in the classroom. On these occasions, express permission will be given by the teacher. Students may then use their mobile phones in the classroom for that lesson only. The use of personal mobile phones in one lesson for a specific purpose does not mean further usage is then acceptable.

If asked to do so, students will show the content requested or hand their phone to a teacher or other designated adult such as the police.

Theft or damage

The responsibility of keeping a students' mobile phone safe lies with the student; the school accepts no responsibility for replacing lost, stolen or damaged mobile phones.

The school accepts no responsibility for students who lose or have their mobile phones stolen while travelling to and from school.

Students should mark their mobile phone clearly with their full name.

Students who bring a mobile phone to school should leave it in their bag when they arrive.

To reduce the risk of theft during school hours, students who carry mobile phones are advised to keep them well concealed and not 'advertise' that they have them.

When a mobile phone is found on the school premises and the owner cannot be located, it should be handed into the front office reception.

It is strongly advised that students use passwords and/or pin numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Mobile phones and/or passwords may not be shared.

Inappropriate conduct

Using mobile phones to bully or threaten students or staff is unacceptable. Cyberbullying will not be tolerated. In some cases it could constitute criminal behaviour. Using technology to humiliate, embarrass or cause offence will not be tolerated; regardless of whether 'consent' was given.

It is forbidden for students to use their own or other students' mobile phones to take videos and pictures of acts to denigrate or humiliate others. This also includes using mobile phones to photograph or film any student or member of staff without their consent. It is a criminal offence to use a mobile phone to menace, harass or offend another person and almost all calls, text messages and emails can be traced.

Mobile phones are not to be used or taken into changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow students, staff or visitors to the school.

Should there be more than one disruption to lessons caused by a mobile phone, the responsible student may face disciplinary actions as sanctioned by the Headteacher. This may include a mobile phone ban in school.

It is unacceptable to take a picture of a member of staff without their permission. In the event that this happens the student will be asked and expected to delete those images.

Mobile phones are banned from all examinations. Students MUST hand phones to invigilators before entering the exam hall. Any student found in possession of a mobile phone during an examination may have that paper disqualified. Such an incident may result in all other exam papers being disqualified.

Any student who uses vulgar, derogatory, or obscene language while using a mobile phone will face disciplinary action.

Students may not engage in personal attacks, harass another person, or post private information using SMS messaging, taking/sending photos or objectionable images, and phone calls. Students using mobile phones to bully other students will face disciplinary action. [It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. As such, the school may consider it appropriate to involve the police.]

Students must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. The transmission of such images is a criminal offence. Similarly, 'sexting' – which is the sending of personal sexual imagery - is also a criminal offence.

Sanctions

Students who infringe the rules set out in this document could face having their phones confiscated by teachers. If the phone is being used inappropriately the student must give it to a teacher if requested.

On any infringement of this policy the mobile phone would be confiscated by the teacher and taken to a secure place within the school office. The student will be able to collect the mobile phone at the end of the school day and a record will be made of the incident.

If the incident involves students under the age of 13 or is deemed illegal or inappropriate, then the school has a duty to inform the Local Area Designated Officer for safeguarding (LADO) and may refer the incident to the police.