OXTED SCHOOL
ICT ACCEPTABLE USE POLICY

Purpose: The School is committed to the development of effective teaching and learning strategies that use ICT in a responsible and socially acceptable fashion to enhance learning. The purpose of this policy is to define the acceptable use of ICT within the School, with particular reference to the use of the internet and email.

Date created: May 2015
Created/implemented: May 2015
Review period: 3 years
Last reviewed: May 2015
Last re-written: June 2013
Next due for review: May 2018

Policy statement
At Oxted School, we believe that Information Communications Technology is an essential tool for learning. The aim of this policy is to outline how we endeavour to create a safe learning environment for all users of the computer system.

A safe ICT learning environment includes:

- An infrastructure of whole School awareness, designated responsibilities and procedures
- An effective range of technological tools
- A comprehensive internet safety education programme for the whole school community

Responsibilities and Procedures

E-safety is a child safety (not an ICT) issue. Safeguarding children and young people in both the real and virtual world is everyone’s responsibility. The policy is cross referenced to the child protection and safeguarding policy, the anti-bullying policy and the use of photographic images policy.

Implementing e-safety policies demands the involvement of a wide range of all interest groups:
Head of School
Governors
Senior leadership
Classroom teachers
Support staff
Young people and parents or carers

All staff, students and parents have to agree to and sign an internet and email use agreement which clearly outlines the responsibilities of the users of the computer system. (See Appendix 1)

In the event of an e-safety incident the procedure for responding to the incident is shown in Appendix 2.

Technological Tools

In order to protect responsible users, electronic methods will be used to:

- help prevent access to unsuitable material
- monitor and record the use of ICT by users (including internet sites visited and the content of electronic mail messages)

Software is a key ICT Tool made available by the school for users. It is licensed exclusively for use by staff and students. Usage outside these parameters may lead to disciplinary action.

Internet safety education programme

As recommended by the Byron Review all students will be taught about online safety through a combination of the ICT, Citizenship and PSHE curriculum. The School also undertakes to educate parents and carers through meetings and literature. Staff will be informed about e-safety strategies at induction and as developments take place.

APPENDIX 1
OXTED SCHOOL STAFF ACCEPTABLE USE POLICY

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in School. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the IT Services Team.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school’s email / internet / intranet / learning platform and any related technologies for professional purposes, or for uses deemed ‘reasonable’ by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the School or other related authorities. I will change my passwords termly.
- I understand that I am responsible for all activity carried out under my username.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any School business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in School, taken off the School premises or accessed remotely. Personal data can only be taken out of School or accessed remotely when authorised by the Head of School or Governing Body.
- I will not install any hardware or software without the permission of the IT Services Team.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/or staff will only be taken, stored and used for professional purposes in line with School policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the School network/learning platform without the permission of the parent/carer, member of staff or Head of School.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head of School.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in School and outside School, will not bring my professional role into disrepute.
- I will use the Secure Gateway to access data and will ensure that this information is not accessed by others on my personal computer / device.
- I will use an encrypted memory stick if I have need to store data for mobile use.
- I will not leave confidential information available for the use of others in public spaces.
- I will shred using School procedures all documents which contain data.
- I will report any incidents of concern regarding children’s safety to the DCPO.
- I will ensure that electronic communications with students including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will support the school’s E-safety policy and help students to be safe and responsible in their use of ICT and related technologies. I will promote E-safety with students in my...
care and will help them to develop a responsible attitude to system use, communications and publishing
STUDENT ‘RESPONSIBLE COMPUTER AND INTERNET USE’ STATEMENT

UPDATED: 13 February 2015

These E-safety Rules help to protect students and the School by describing acceptable and unacceptable computer use.

• I understand the School owns the computer network and learning platform and can set rules for its use. I understand it is a criminal offence to use a computer or network for a purpose not permitted by the School

• I will only use ICT systems in School, including the internet, email, digital video, mobile technologies, etc, for school purposes. I will not use ICT systems at school for private purposes, unless the Head of School has given specific permission

• I will not use ICT systems at School for personal financial gain, gambling, political activity, advertising or illegal purposes

• I will treat all ICT equipment with respect and understand that it may incur replacement or repair fees if deliberately damaged or stolen

• I will only log on to the School network/learning platform with my own user name and password

• I accept that I am responsible for all activity carried out under my username

• I will follow the School’s ICT security system and not reveal my passwords to anyone and change them regularly

• I will make sure that all ICT communications with students, teachers or others is responsible and sensible, particularly as email could be forwarded to unintended readers

• I know that partaking in any online communication could be subject to School scrutiny and possible sanctions

• I am aware that the sending of explicit images is not only illegal, but puts myself and others at risk

• I will use the discussion forums on the School’s learning platform for exchanging information and will share my ideas constructively

• I will not give out any personal information such as name, phone number or address through email, personal publishing, blogs, messaging or when using the School’s learning platform. I will not arrange to meet someone unless this is part of a School project approved by my teacher

• I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher
• I will not download or install software on School technologies
• I will not attempt to attach any personal computer or mobile device to the School’s Network or wireless systems, without prior consent from the IT Services Team
• I will ensure that my online activity, both in School and outside School, will not cause my School, the staff, students or others distress or bring the School into disrepute. This may result in serious sanctions from the School or the police.
• I will respect the privacy & ownership of others’ work online at all times.
• I understand the School can exercise its right to monitor the use of the School’s computer systems and learning platform, including access to websites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the School’s computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
• I understand that all my use of the Internet, School’s learning platform and other related technologies can therefore be monitored and logged and can be made available to my teacher.

I understand that these rules are designed to keep me safe and that if they are not followed, School sanctions will be applied and my parent/ carer or the police may be contacted. I understand that irresponsible use may result in the loss of my network or Internet access.
OXTED SCHOOL STUDENT LAPTOP LOAN POLICY

Oxted School Device Loan Acceptable Use Policy

The following rules are designed to keep you safe and ensure that equipment provided by the School is looked after appropriately.

If you fail to follow these rules, the School may restrict your account usage or temporarily or permanently withdraw your access to the device.

The Device

- Is to be used only by named and agreed person
- May not be loaned or given to any other person without prior agreement from the School
- Is for School based work only
- Is pre-loaded with a full version of Microsoft Office, which is valid until such time the student leaves the School
- Must not be loaded with any other applications without prior agreement from the School
- Software, utilities and restrictions put in place by the School must not be removed

Your responsibility

- You are responsible for all activity carried out on the device
- All communications with students, teachers and others will be sensible and represent the School in a positive manner
- You must not browse, download, upload or forward material that could be considered offensive or illegal. If you come across any such material then you must report it to the School at the earliest opportunity
- Windows Updates and other software updates should be installed as soon as possible after release. Windows or other applications will display a prompt when updates are ready or required
- A virus checker must be installed and be kept up-to-date at all times
- Connection to the internet outside of School is your responsibility. The School does restrict Wi-Fi settings on the device and therefore it is for the named person to add the device to a home Wi-Fi connection
- Parents/guardians are responsible for monitoring internet usage on the device when used outside of School
- Any faults or damage must be reported to the School at the earliest opportunity.
- Repair or replacement due to damage or loss, caused through a deliberate action, or by leaving the device unattended in a public place

Our responsibility

- The School will aim to fix any faults with the device as soon as possible, this may be delayed should new parts be required
- The School reserves the right to recall the device temporarily or permanently for any reason at any time
appendix B

flowchart for responding to e-safety incidents

E-safety incident

- Unsuitable materials
  - Report to local e-safety lead and/or LSCB e-safety officer
  - If child or young person: review incident and decide on appropriate course of action, applying sanctions as necessary
  - Debrief on e-safety incident

- Illegal material or activity found or suspected
  - Illegal activity
    - Report to police
    - If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
    - Debrief on e-safety incident
  - Illegal content
    - Report to IWF and/or police
  - Child or young person at risk
    - Report to CEOP (but police if risk of immediate danger)

- Secure and preserve evidence
- Await police/IWF/CEOP response
- If no illegal material or activity is confirmed, revert to internal disciplinary procedures for staff
- If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LA/LSCB on treatment of offender/victim

Review policies and technical tools, and share experience and practice as required

Monitor situation

Note: this flowchart originally appeared in Flowchart for responding to Internet safety incidents in school in the Becta publication E-safety: Developing whole-school policies to support effective practice. We have revised and updated it to include additional lines of reporting to CEOP [http://www.ceop.gov.uk] and the Internet Watch Foundation [http://www.iwf.org.uk].