The
Ongar
Academy

Affectare ad Optimum

Policy Title	ICT and E-Safety
Version	1
Author(s)	David Grant, Headteacher
Committee Responsible	Education
Governor Link	Blane Judd
Date approved by Committee	24 Feb 2015
Date approved by Full Governing Body	15 April 2015
Review Date	As required

ICT and E-Safety Policy

Enquiries & comments
Any enquiries and comments about this publication may be made to:

e-mail: admin@theongaracademy.org

Aim

The school, through this policy, wishes to provide guidelines under which staff and students should feel confident about the use of ICT and related technologies in the delivery and enhancement of teaching and learning.

Objectives

- To ensure that students and staff use ICT and related technologies safely and securely.
- To ensure that students' learning is enhanced to maximum extent.
- To safeguard students' rights for equal opportunity to participate and use ICT.
- To ensure that responsibilities for staff are clear and that required formalities and agreements are adhered to.

Introduction

ICT is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of 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.

ICT 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. All users need to be aware of the range of risks associated with the use of ICT related technologies.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and students) include both fixed and mobile internet; technologies provided by the school (such as PCs, portable devices, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies privately owned by students and staff, but brought onto school premises.

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose e-mails, instant messaging, internet/intranet use and any other electronic communications involving its employees or contractors, without consent, to the extent permitted by law.

This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using school ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised HCC staff.

Breaches

A breach or suspected breach of policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school disciplinary procedure. In extreme cases, policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the designated member of SLT with responsibility for ICT and E-Safety.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. memory stick, CD) must be checked for any viruses using school provided anti-virus software before using them. Training on how to do this is available from the network support team.

- Staff should never interfere with any anti-virus software installed on any school ICT equipment that they use.

- If staff suspect there may be a virus on any school ICT equipment, they should stop using the equipment and contact the ICT network support team immediately.

Data Security

The handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. In extreme cases, failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

- The school gives relevant staff access to its Management Information

System and Network, with a unique ID and password. It is the responsibility of everyone to keep these passwords secure.(See password section below)

- All staff should keep all school related data secure. This includes all personal, sensitive, confidential or classified data.

- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, staff should keep it locked.

- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under their control at all times.

- It is the responsibility of individual staff to ensure the security of any personal, sensitive and confidential information contained in documents faxed, copied, scanned, emailed or printed.

- Anyone expecting a confidential/sensitive fax or email should have warned the sender to notify before it is sent.

Passwords

- Staff should change passwords whenever there is any indication of possible system or password compromise.

- Staff should not record passwords or encryption keys on paper or in an unprotected file.

- Staff should disclose their personal password to the ICT network support staff when necessary, and never to anyone else.

- User ID and passwords for staff and students who have left the school will always be removed from the system.

Strategic Overview

The senior member of staff with designated responsibility for ICT should be familiar with information risks and the school's response.

It is this person's responsibility to minimise any risks present.

It is also this person's responsibility to understand:

- what information is held, and for what purposes.
- what information needs to be protected. (e.g. any data that can be linked to an individual, student or staff etc)
- how information will be amended or added to over time.
- who has access to the data and why.
- how information is retained and disposed of.

These responsibilities can be delegated as appropriate to suitably appointed staff.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency or authority.

- All redundant ICT equipment that may have held personal data will have the storage media wiped to ensure the data is irretrievably destroyed or be physically destroyed. (By the network support team)

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

- Any redundant ICT equipment being considered for sale/gift will hold a valid PAT certificate.

E-Mail

The use of e-mail should be in line with the school's communications policy.

E-mailing Personal, Sensitive, Confidential or Classified Information

- Staff should assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible.
- Where staff conclude that e-mail must be used to transmit such data:

  – They should exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

  ○ Staff should verify the details, including accurate e-mail address, of any intended recipient of the information.
  ○ Staff should verify (by phoning) the details of a requestor before responding to e-mail requests for information.
  ○ Staff should not copy or forward the e-mail to any more recipients than is absolutely necessary.

  – Staff should not send the information to any person whose details they have been unable to separately verify (usually by phone).
  – Staff should not identify such information in the subject line of any e-mail.
  – Staff should request confirmation of safe receipt.

E-Safety - Roles and Responsibilities

It is the role of the designated member of SLT with responsibility for E-Safety and ICT to keep abreast of current issues and guidance through organisations such as the LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/E-Safety Co-ordinator and all governors have an understanding of the issues and strategies at the school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following school policies: child protection, health and safety, home–school agreements, and behaviour/student discipline (including the anti-bullying) policy and PSHEE.

E-Safety in the Curriculum

ICT and online resources are used across the curriculum. It is essential for E-Safety guidance to be given to the students on a regular and meaningful basis.

- The school has a framework for teaching internet skills in relevant computing lessons.
- The school provides opportunities within PSHEE to teach about E-Safety.
- Educating students on the dangers of technologies that may be encountered outside school is done formally in an annual assembly and informally when opportunities arise.
- Students are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Students are aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying i.e. parent/carer, teacher/trusted staff member, an organisation such as Childline or CEOP report abuse button.

E-Safety Skills Development for Staff

- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart).
- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas.

Managing the School E-Safety Messages

- The school endeavours to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used.

Incident Reporting, E-Safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the designated member of SLT with responsibility for ICT and E-Safety. Incidents should be logged and the Flowchart for Managing an E-Safety Incident should be followed. (See below)

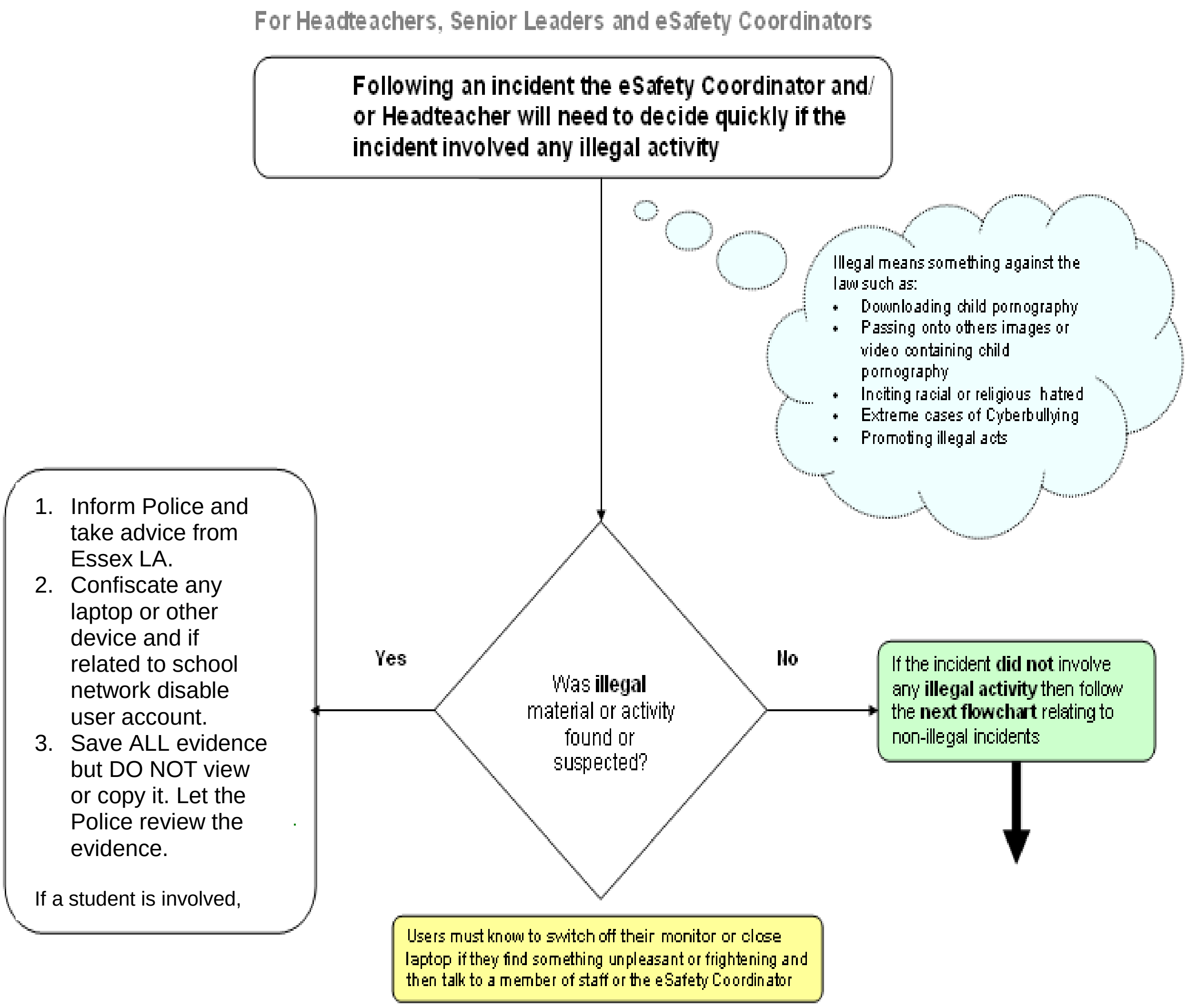
E-Safety Incident Log

Some incidents may need to be recorded in other places, such as Solero, if they relate to a bullying or racist incident. When in doubt, please consult with the senior member of staff with designated responsibility for E-Safety and ICT.

Inappropriate Material

- Accidental access to inappropriate materials must be immediately reported to the ICT Network Support Team.
- Deliberate access to inappropriate materials by any user will be logged; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)

Flowcharts for Managing an E-Safety Incident



Following an incident the eSafety Coordinator and/ or Headteacher will need to decide quickly if the incident involved any illegal activity

Illegal means something against the law such as:

- Downloading child pornography
- Passing onto others images or video containing child pornography
- Inciting racial or religious hatred
- Extreme cases of Cyberbullying
- Promoting illegal acts

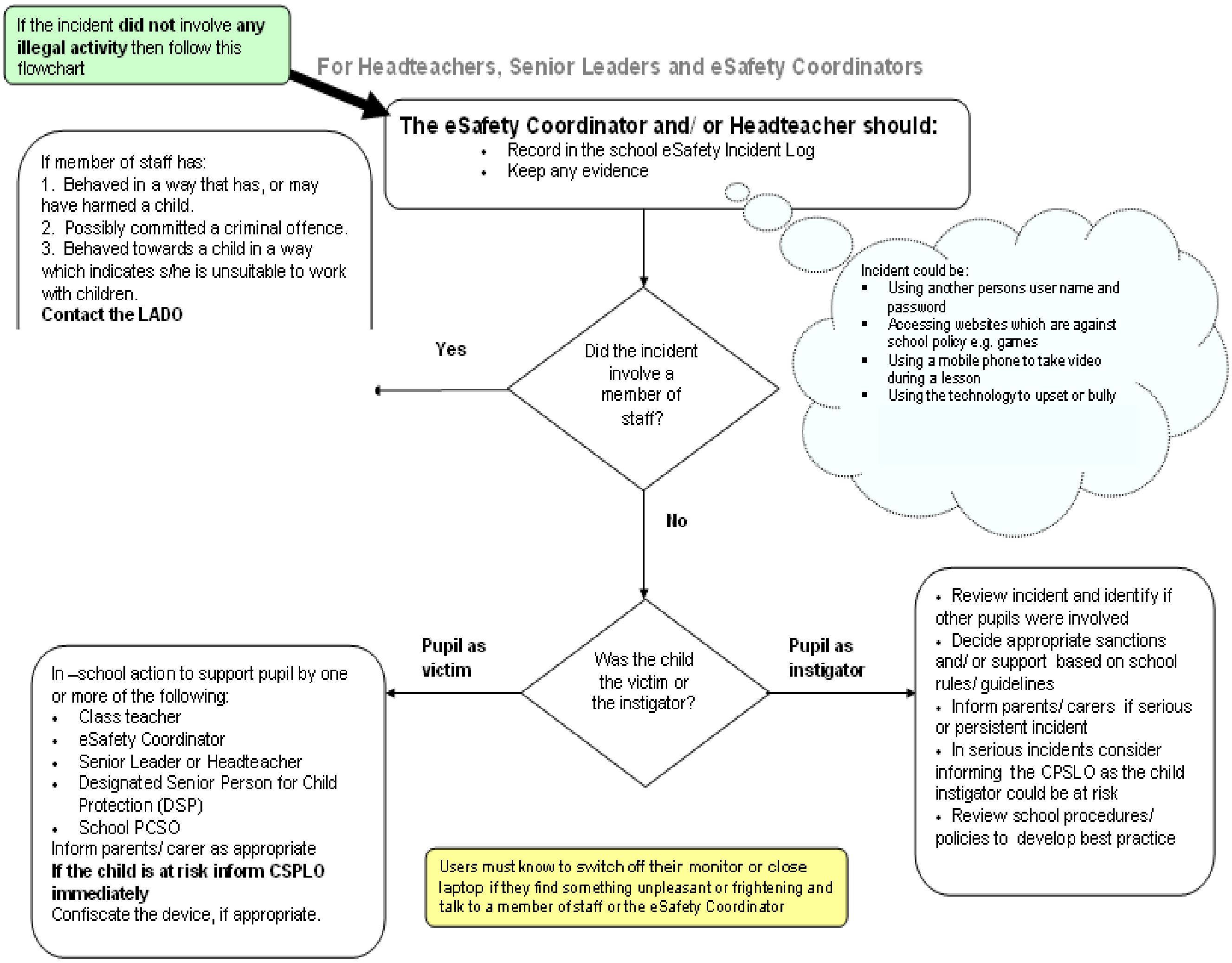
Was **illegal** material or activity found or suspected?

1. Inform Police and take advice from Essex LA.
2. Confiscate any laptop or other device and if related to school network disable user account.
3. Save ALL evidence but DO NOT view or copy it. Let the Police review the evidence.

If a student is involved,

If the incident **did not** involve any **illegal activity** then follow the **next flowchart** relating to non-illegal incidents

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator



If the incident **did not** involve **any illegal activity** then follow this flowchart

For Headteachers, Senior Leaders and eSafety Coordinators

The eSafety Coordinator and/ or Headteacher should:

- Record in the school eSafety Incident Log
- Keep any evidence

Incident could be:

- Using another persons user name and password
- Accessing websites which are against school policy e.g. games
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully

Did the incident involve a member of staff?

Yes

If member of staff has:
1. Behaved in a way that has, or may have harmed a child.
2. Possibly committed a criminal offence.
3. Behaved towards a child in a way which indicates s/he is unsuitable to work with children.
Contact the LADO

No

Was the child the victim or the instigator?

Pupil as victim

In –school action to support pupil by one or more of the following:

- Class teacher
- eSafety Coordinator
- Senior Leader or Headteacher
- Designated Senior Person for Child Protection (DSP)
- School PCSO

Inform parents/ carer as appropriate
If the child is at risk inform CSPLO immediately
Confiscate the device, if appropriate.

Pupil as instigator

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions and/ or support based on school rules/ guidelines
- Inform parents/ carers if serious or persistent incident
- In serious incidents consider informing the CPSLO as the child instigator could be at risk
- Review school procedures/ policies to develop best practice

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and talk to a member of staff or the eSafety Coordinator

Internet Access

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.

Managing the Internet

- Students should have (supervised) access to Internet resources (where reasonable) through the school’s fixed and mobile internet technology.

- Staff should preview any recommended sites before use.

- Image searches are discouraged when working with students.

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

- All users must observe copyright of materials from electronic resources.

Internet Use

- Staff must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.

- Staff must not reveal names of colleagues, customers or clients or any other confidential information acquired through their job on any social networking site or blog.

- On-line gambling or gaming is not allowed.

Staff may find it useful to refer to the relevant guidance and policies relating to professional conduct which are provided in the shared area. (See appendix for a list.)

Filters

- School internet access is controlled through an in-house filtering service.

- The ICT Network Director should be made aware of their responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000 and the Human Rights Act 1998.

- Staff and students are aware that school based e-mail and internet activity can be monitored and explored further if required.

- The school does not allow students access to internet logs.

- The school uses management control tools for controlling and monitoring workstations.

- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the ICT Network Support Team or teacher as appropriate.

- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

- Students and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school’s responsibility nor the network manager’s to install or maintain virus protection on personal systems. If students wish to bring in work on removable media it should be given to an ICT technician or the teacher for a safety check first. Sensitive data must **never** be taken off site unless it is encrypted. An encrypted memory stick can be obtained from the network support team if required.

- If there are any issues related to viruses or anti-virus software, the network manager should be informed by phonecall or e-mail.

Social Networking

- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

- Students are taught to avoid placing images of themselves (or details within images that could give background details) and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ e-mail address, specific hobbies/ interests).

- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

- Students are encouraged to be wary about publishing specific and detailed private thoughts online.

- Students are asked to report any incidents of bullying to the school.

Parental Involvement

It is essential for parents/ carers to be fully involved with promoting E-Safety both in and outside school and also to be aware of their responsibilities. The school regularly consults and discuss E-Safety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on school website).

- The school disseminates information to parents relating to E-Safety where appropriate in the form of;

  - Information evenings
  - Website/ Learning Platform postings
  - Newsletter items

Protecting Personal, Sensitive, Confidential and Classified Information

- Staff should ensure that any school information accessed from your own PC or removable media equipment is kept securely.

- Staff should ensure they lock their machine before moving away from their computer during the normal working day to prevent unauthorised access.

- Staff should ensure the accuracy of any personal, sensitive, confidential and classified information they disclose or share legitimately with others.

- Staff should ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.

- Staff should ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print.

- Staff must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.

- Staff should ensure hard copies of data are securely stored and disposed of (shredded) after use.

Using Removable Media

- Staff should store all removable media securely.

- Staff should securely dispose of removable media that may hold personal data.

- Staff should always encrypt all files containing personal, sensitive, confidential or classified data. (Training on this can be obtained from the network support team.)

- Staff should ensure hard drives from machines no longer in service are removed and stored securely or wiped clean via the network support team.

Remote Access

- Staff are responsible for all activity via the remote access facility.

- Staff should only use equipment with an appropriate level of security for remote access. (e.g. staff should not use machines in a public place (internet café.))

- Staff should protect school information and data at all times, including any printed material produced while using the remote access facility. Staff should take particular care when access is from a non-school environment.

Safe Use of Images - Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. Staff should remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment.

- Staff are not advised to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips.

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Publishing Students' Images and Work

On a student's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Learning Platform (if applicable)
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
- This consent form is considered valid for the entire period that the child attends this school.
- Parents/ carers may withdraw permission, in writing, at any time.
- E-mail and postal addresses of students will not be published.
- Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Video Conferencing

- Any school conferencing equipment will not set to auto-answer and will only be switched on for scheduled and approved events.
- No part of any video conference will be recorded in any medium.

School ICT Equipment

- Staff and students are responsible for any activity undertaken on the school's ICT equipment provided to them.

- Staff should not allow visitors to use their ICT hardware in conjunction with the school network without consultation with the ICT network support team.

- Staff should ensure that all ICT equipment that is used is kept physically secure.

- Staff should not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.

- Staff should save their data on a frequent basis to the school's network drive. Staff are responsible for the backup and restoration of any data that is not held on the school's network drive.

- Personal or sensitive data should not be stored on the local drives of desktop PCs.

- Privately owned ICT equipment including personal portable devices should not be used on a school network unless with express permission from the SLT member with responsibility for ICT. Any privately owned ICT (or ICT related) equipment must be subject to the usual rules and regulations surrounding the protection of children and e-safety as laid out in this and other policies or guidance.

- It is the responsibility of the staff to ensure that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

Portable & Mobile ICT Equipment

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.

- Staff must ensure that all school data is stored on school's network, and not kept solely on a portable device. Any equipment where personal data is likely to be stored must be encrypted and/or password protected.

- Staff should ensure that equipment is kept physically secure in accordance with this policy to be covered for insurance purposes. (When travelling by car, best practice is to place the portable device in the boot of the car before starting the journey.)

- Staff should ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

- The installation of any applications or software packages must be authorised by the ICT network support team and fully licensed. All other packages will be removed.

- In areas where there are likely to be members of the general public, portable or staff must not leave mobile ICT equipment unattended and, wherever possible, kept out of sight.

- Portable equipment must be transported in its protective case.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. The school chooses to manage the use of these devices in the following ways so that they are used appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use.

- Students are allowed to bring personal mobile devices/phones to school but must only use them in line with the relevant guidance on their use.

- The school is not responsible for the loss, damage or theft of any personal mobile device.

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between members of the school community is not allowed.

- Permission must be sought before any image or sound recordings are made.

Systems and Access

- Staff are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC (which is not recommended).

- Staff should not allow any unauthorised person to use school ICT facilities and services that have been provided to them.

- Staff should use only their own personal logons, account IDs and passwords and must not allow them to be used by anyone else.

- Staff should ensure that they logoff from the PC completely when they are going to be away from the computer for a longer period of time.

- Staff must not intentionally introduce or propagate viruses.

- It is imperative that staff do not access, load, store, post or send from school

ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, e-mails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

- Any information held on school systems, hardware or used in relation to school business may be subject to The Freedom of Information Act.

- Where necessary, staff should obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. (This to be done by the network support team.)

The Ongar Academy and its Governing Body is committed to ensuring consistency of treatment and fairness and will abide by all relevant equality legislation.

Appendix

Relevant policies

- Child Protection Policy
- Communications Policy
- Employees Code of Conduct
- Guidelines on Appropriate Professional Behaviour
- Whistleblowing Policy
- Disciplinary Policy
- Grievance Policy

Acts Relating to Monitoring of Staff E-Mail

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) - Interception of Communications Regulations 2000 **http://www.hmso.gov.uk/si/si2000/20002699.htm**

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Acts Relating to E-Safety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.
For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 200*0*
http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Information Commissioner Website http://www.ico.gov.uk/

ICT Code of Conduct: Students

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will respect copyright and intellectual property rights.
- I will only log on to the school network with my own user name and password.
- I will follow the school's ICT security system and not reveal my passwords to anyone; I will change my passwords regularly.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible. I am responsible for e-mail I send and contacts made.
- I will be responsible for my behaviour when using the Internet; this includes a consideration of the resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material which 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 give out any personal information such as name, phone number or address.
- I will ensure that my online activity, both in and out of school, will not cause my school, the staff, students or others distress or bring them into disrepute.
- I will support the school's approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- 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 may be contacted.

Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, 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 senior member of staff with responsibility for ICT and E-Safety.

- I will only use the school's e-mail / Internet / Intranet 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 ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as personal mobile phone number and personal e-mail address to students.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without the permission of the ICT network support 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 consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- 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 Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- 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 support and promote the school's e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …………………………………… Date ……………………

Full Name ……………………………….. (printed)

Job title . . . .

Portable Device Loan Agreement

The portable device and accessories remain the property of The Ongar Academy and are only for the use of the member of staff to whom they have been issued. They must be returned when the member of staff ceases to be employed by the school. The portable device is issued to a member of staff for school related use and private use must be insignificant and incidental.

Under the school's insurance the portable device will be covered against theft and accidental damage provided the member of staff has taken reasonable precautions. Leaving an unattended portable device on view, either in a vehicle or around the school, would not be regarded as a reasonable precaution. Any theft must be reported to the police immediately and to the school as soon as possible.

If the portable device or any of the accessories are lost or damaged by a member of staff, s/he may be asked to contribute towards the cost of replacing them at the discretion of the Headteacher.

The school does not take responsibility for the loss of data files should a fault occur on the portable device. The member of staff to whom the portable device has been issued is responsible for ensuring that his/her data files are backed up; they should be copies onto a memory stick onto a regular basis.

Additional software may only be installed onto the portable device by the member of staff after s/he has provided the licence/proof of registration to the ICT Network Director who will note details for auditing purposes.

Any software found on the portable device that has not been approved by the ICT Network Support Team is subject to removal after a formal written notice has been issued.

Any telephone charges or fees payable to the Internet Service Provider incurred by the member of staff accessing the Internet from home are not chargeable to the school.

The portable device must be brought into school when requested so that software can be updated and annual electrical testing take place.

I have received the equipment and have read and understood the agreement.

Signed…………………………......…… Name…………..…..……………… Date……………..

The Ongar Academy

Responsible ICT Use

Student agreement to abide by the code of conduct on responsible ICT use

Student's name: **Form:**

As a user of ICT at school, I agree to comply with the school's code of conduct on its use. I will use the computer system and Internet in a responsible way and observe the restrictions explained to me by the school.

Student's signature: **Date:**

Parental consent to ICT access

Name of parent: ***(please use block capitals)***

As the parent or legal guardian of the above named student, I grant permission for my child to use electronic mail and the Internet. I have read and understood the school's policy on responsible ICT use and understand that students will be held accountable for their own actions, and that the school will not be liable for any damages resulting from the use of the ICT facilities. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my daughter/son to follow when selecting, sharing and exploring information and media.

Signed: **Date:**

Parental consent to website publication of work and photographs:

Name of parent: ***(please use block capitals)***

I agree that, if selected, my daughter/son's work may be published on the school website. I also agree that photographs that include my daughter/son may be published, subject to the school rules that photographs will not clearly identify individuals, and that full names will not be used unless express permission has been received.

Signed: **Date:**

Please complete, sign and return either to your Computing teacher during your next Computing lesson, or to Reception before that time.

<u>You will not be able to access the ICT facilities until this form is returned</u>.

Using ICT safely at home: guidance for parents

What can parents do to reduce the risks?

Internet Service Providers (ISPs) have systems in place for parents to block out parts of the service they feel are inappropriate for their children. ISPs mostly provide parental controls for editing and censoring the material visible on their systems. If parents wish to utilise, or find out about, any available parental controls then they should contact their ISP to find out how the control systems can be applied.

The Internet and some private bulletin boards contain areas designed specifically for adults who wish to post, view, or read sexually explicit, racist or anarchic material. As with all safeguards, parents should be aware that there will always be cases where individuals, groups or organisations fail to enforce them or where children find ways around them.

Children need parental supervision and common-sense advice in order that their experiences whilst on-line are happy, healthy, and productive. Children need to act independently in order to develop; however, in the same way that they still need parental involvement and supervision (direct and indirect) in their daily lives if security is to be maintained, they also need parental involvement and supervision whilst on-line.

Keeping your daughter/son safe on-line

1 Stay in touch with what your children are doing by spending time with them whilst they are on-line, i.e. make on-line time a family activity.

2 Make sure that you know the services your children use. Find out what types of information and services are offered and whether there are ways for parents to protect their children.

3 Keep the computer in a family room rather than a child's bedroom.

4 Go on-line yourself so that you are familiar with and understand the potential benefits and risks associated with Internet access. If you don't know how to log on, get your child to show you.

5 Get to know your child's 'on-line friends' just as you do their other friends.

6 If you are concerned about your child's on-line activities, talk to her/him about it.

7 Develop an agreed set of 'Family Internet Rules' - see later for an exemplar.

8 Make sure that your children are familiar with, and adhere to, your 'Family Internet Rules' which should be posted near the computer as a reminder.

9 Monitor your children's compliance with these rules.

10 Should you become aware of the presence of child pornography on-line, report this immediately to the National Society for the Prevention of Cruelty to Children.

Family Internet rules

1 Always keep to the agreed times of day to be on-line, the length of time to be on-line, and the areas that you can visit.

2 Never give any passwords to anyone outside your family – even friends!

3 Always tell a parent about any threatening or bad language you see on-line.

4 Never give out any of the following information during a 'chat' session or when accessing on-line forums or message boards:

- your real name (use a pseudonym – a false name)
- your parents' or brothers'/sisters' real names (use pseudonyms)
- home address
- home telephone number
- parents' work address/telephone number
- the name, address or location of your school

5 Never send an on-line person any photographs or anything else without first checking with a parent.

6 Never arrange for someone you meet on-line to visit your house.

7 Never arrange a face-to-face meeting with another computer user without parental permission. If a meeting is to be arranged let your parents arrange this for you. The first meeting should be in a public place and at least one parent should accompany you. Your house should remain occupied during the meeting to prevent burglary.

8 Never respond to messages or to on-line forums or message boards items that are suggestive, obscene, threatening or that make you feel uncomfortable. If you encounter such messages then tell a parent immediately.

9 Remember that what you read on-line is not necessarily true, e.g. the person who says she is a 15 old girl could in fact be a middle aged man.

10 Never try and order something on-line unless you are over 18 years old.