Epping Upland C. of E. Primary School
E-Safety and ICT Security Policy

ICT in the 21st Century is seen as 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 technologies in order to give young people the skills they need to achieve success.

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:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Smart phones with text, video and 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 Epping Upland we understand the responsibility of educating our pupils on eSafety issues; teaching them the appropriate behaviors and thinking skills 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 the 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.

The policy as outlined in this document is inclusive of both fixed and mobile internet; technologies provided by the school such as PCs, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc; and technologies owned by pupils and staff, but brought onto school premises such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.

Monitoring

Staff authorized by the Headteacher may without prior notice, access the e-mail or voice-mail account of staff and students where it is deemed appropriate and is in the interest in the day-to-day running of the school.

Internet activity is logged by the school and may be monitored by persons authorized by the HT

Incident Reporting

All security breaches, lost/stolen equipment or data (including remote access ID's and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the HT

Computer Viruses

• All files downloaded from the Internet, received via e-mail or on removable media (e.g. external USB devices, CD) must be checked for any viruses using school provided anti-virus software before using them

• Never interfere with any anti-virus software installed on school ICT equipment that you use

• It is the responsibility of the ICT Support team to ensure that all antivirus software installed on any school owed equipment is kept up-to-date

• If your machine is not routinely connected to the school network, you must make provision for regular virus updates directly yourself by instigating a scan or through the ICT Support team.

• If your machine is not owned by the school it is your responsibility to ensure that regular virus updates and scan are carried out.

• If you suspect there may be a virus on any school ICT equipment or privately owned equipment used in school, stop using the equipment, disconnect from the school network and contact ICT support team immediately. The ICT support team will advise you what actions to take and be responsible for advising others that need to know.

Data Security

- The School gives relevant staff access to its Management Information System, with a unique ID and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff 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, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared multi-function print, fax, scan and copiers are used
- Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent.

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. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

All staff and pupils have monitored access to internet resources (where reasonable) through the schools fixed and mobile technology. All users must observe copyright of materials from electronic resources.

Internet Use

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

Pupils and staff are not permitted to download any programs on the school based

technologies without seeking permission from a member of the ICT Support team.

Infrastructure
The schools internet access is controlled through the LA's web filtering service operated by Daisy Updata Communications Ltd (DUCL)

For further information relating to filtering please go to
https://schools-secure.essex.gov.uk/admin/Broadband/School%20Services/Pages/InternetFilteringSecurity.aspx

Email
Many people use email as a substitute for conversation. However, unlike conversations, emails are easily distributed to an audience wider than the intended, can become legal documents and can easily become permanent records.

With this in mind, the following principles must be observed: -

- If you receive material of a defamatory, terrorist, abusive, sexist, racist or pornographic nature, you should inform your manager immediately, record & delete the email and ask the sender not to send such mail to you in future.
- You should always consider the Data Protection implications of any information sent by email. In essence, no data which relates to living individuals should be disclosed (by email, post or otherwise) unless you have that individual's consent.
- You should always use a civil, professional and amicable tone.
- The school will not tolerate bullying by email. The use of obscene language or swear words is prohibited.
- Emails sent or received for personal correspondence are considered as business use and no right of privacy applies to them.
- Emails sent to a school allocated email address are considered the property of the school and can be accessed to deal with any business-related issues retained on that account
- When using email in dealings with outside companies and suppliers, remember how easy it is to inadvertently create a binding contract with a third party. Check your emails before dispatch as carefully as you would check a written contract and obtain advice, if appropriate, before sending.
- Do not send confidential market sensitive information via external email. If you are unsure about the classification of any piece of data, consult the HT.

Social Media

The growth in social media, particularly social networking sites, has created increased opportunity for media communications that have an impact upon the school.

The term 'social media' is used here to describe dynamic and socially-interactive, networked information and communication technologies, for example Web 2.0 sites, SMS text messaging and social networking sites. Popular social media sites which may be used for educational purposes include Facebook and Twitter.

The following guidelines should be considered by anyone engaging in social media sites for educational purposes:

- Staff and students should take effective precautions when utilising social networking sites to ensure their own personal safety and to protect against identity theft;
- Staff should never 'friend' or make direct, individual links with pupils or parents;
- Staff should be mindful that pupils and parents will be naturally curious about their personal life and may try to find out more about you;
- Staff should carefully manage the privacy settings of their personal social media sites and teach and encourage pupils to use appropriate and safe online behaviour;
- Staff should exercise caution when interacting with, and responding to, potentially contentious posts on social media sites;
- Staff need to consider intellectual property rights, copyright and ownership of data when using social media;
- Staff must never discuss pupils, colleagues, parents or carers online or criticise the school or school community;
- The school will continually review the use of social media and may modify its policies should the status of particular social media sites change, e.g. if charges are introduced, changes made to the way content is used, terms of use are changed, or if a site closes down.

eSafety

Staying safe online is an important message shared with students and staff.

Teachers are individuals with private lives, however, off-duty conduct matters and may have bearing on their professional life. Therefore sound judgement and due care should be exercised as conduct which may not directly relate to pupils may be relevant to a teacher's fitness to teach

Passwords
Each login-id has a password created specifically for it by the intended user; together they provide the first line of defence for the safe keeping of information. Every login-id has different levels of access depending on what information each user requires to access on the schools systems. You should under no circumstances ever disclose your password to any other individual as this will compromise the information accessible by your login-id.

When choosing a password you should make it as difficult as possible to guess, in order to do this the points listed below should be followed:
• Do not use personal information which others know or could guess, such as DOB, pet names, Phone numbers, hobbies
• Do not use a word in any dictionary (in any language), if you must spell then spell it backwards or substitute some the letters for numbers or special characters. E.g. $h3lt3r (to mean shelter) or f00t8a11 (to mean football)
• Use at least 8 alpha numeric characters, a mixture of letters and numbers, its harder to break or guess
• Utilise a combination of numbers, upper- and lower-case letters, and special characters (such as !$£&@)
• Do not use consecutive keys on a keyboard (qwerty, zxcvbn, 12345) or all like characters (99999, aaaaaaa)
• Type in private and do not write it down.
• Change your password regularly.

Each individual is responsible for all access and activities that take place with their assigned login-id. Do not use any examples listed above for your password as this document will be read by a lot of people.

Workstation Security

It important to secure the workstation whenever away from the area and when leaving at the end the day or at the end of a lesson.

If a workstation is left unsecured it can lead to classified information being modified, deleted, copied, or emailed to someone else without the consent of the login-id owner.

The following procedures should be followed for effective workstation security:

- Secure the workstation when away from the work area, even if you are only planning to be away from it for a minute, staff can do this using alt, ctrl and del then selecting lock this workstation.
- If you are planning to be away for a long period of time considering logging off so that another user may be able to use the machine
- Always log off at the end of each lesson\day
- Make sure anyone accessing a workstation in the area is authorised to do so
- When sensitive information is on the screen that no one else can see it
- If your machine has a projector connected make sure it is switched off before accessing your emails or other sensitive information
- Use good password practices

Mobile Device Security

Mobile devices (laptop or a netbook) are easily stolen or damaged when they are removed from the office/classroom. When using a mobile device, please remember these important points:

- Never keep your login-id and password details with your mobile device
- Never agree to turn off or agree to disable the security software (Antivirus, firewall etc).
- Never hold confidential or sensitive data in unsecured folders on your mobile device, it should be encrypted.
- Do not leave it unsecured and unattended at any time. If you have to leave it in your car place it in the boot and ensure all doors are locked
- Never leave your mobile device in your vehicle overnight

Physical Security

Physical security is also very important. Technological solutions are of little benefit if sensitive information is left in the open, on a desk or an unattended workstation. Spilled food and drinks can cause a great deal of harm to computer equipment and documents.

Be sure to:

Lock sensitive information on any removable media (USB, CD etc) in a draw or cabinet and keep the keys in secure place. Do not leave removable media in your workstation it can easily be removed and taken away from your work area.

Be careful with food and drink in your work area keep it as far away from workstations and mobile devices as possible.

The role of ICT Security

Everyone within the school has a significant role in ensuring the schools ICT security protection in upheld.

For good operational and organisational reasons the school occasionally has to make an exception to its own rules, when a need that outweighs the ICT security policy and procedures, all potential risks are evaluated and communicated with a member of the SLT and a decision is then made. The exceptions are tracked, recorded and then removed when no longer needed.

Epping Upland School Twitter Usage Policy (July 2015)
Aims of Using Twitter:
To quickly share and celebrate children's achievements, successes and school updates.
To demonstrate safe and responsible use of social media
To encourage the use of 21st Century technology

- The school Twitter account will be run from school devices by persons authorised by the Headteacher.
- The school Twitter account will be a Public account (June 2015). The Headteacher will monitor the followers and block any who appear to not be school focused.
- The school Twitter account will only tweet between the hours of 6am and 6pm between Monday and Friday. The only time the school will tweet outside of these times is if authorised by the Headteacher or if there are relevant school events (e.g. football matches, residential trips, performances) or to share urgent school news (e.g. School closure due to adverse weather).
- The school Twitter account will only follow educationally linked accounts and those associated with the school. No personal accounts, unless they are educationally linked, will be followed. For example a children's author.
- The school Twitter account will not reply to any 'replies' on Twitter. This is not the platform to discuss or debate school related issues.
- The school Twitter account will only use children's first names when referencing children.
- The school Twitter account will use Twitter to share positive messages about the school.
- The account may be used to share news and information during a school trip. The account will be run by a senior teacher for the period of the trip.
- Photos taken on a mobile device for the purpose of sharing on Twitter will be deleted once they have been shared.
- Individually targeted content will not be posted e.g. "Well done Josh a better lesson today". Tweets to a year group or class along the lines of "don't forget the..." are acceptable.
- By endorsing twitter we may be encouraging children to use twitter so please reinforce e-safety rules such as "Never tweet anything that would be potentially upsetting; make sure you know how to report to anything you find that disturbs you; be careful who you talk to they may not be all they appear; never meet anyone from twitter world without telling your parents." Etc. Please Note: that twitter have a minimum age policy that stipulates a person must be age 13 or over to set up a Twitter account.

Acceptable Use Agreement/Code of Conduct: Pupils of Epping Upland C.of E. School

Responsible use of the Computer and Internet Agreement for Key Stage 2 Pupils

In order to keep myself and others safe I agree to the following:

1. I will use the school computers, Internet, and all our technological equipment sensibly.
2. I will ask permission before entering any web site, unless my teacher has already approved that site.
3. If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
4. I will never insert my personal details, home address, or telephone numbers on the Internet or in an e-mail.
5. I will only e-mail people or open e-mails from people I know, or my teacher has approved.
6. . I will always be polite and sensible when sending e-mails.
7. I will not look at or delete other people's files without their permission.
8. I will only use my own username and password to access the computer network.
9. I know that the school may check my computer files, monitor the Internet sites I visit and filter the contents of my e-mails.

I understand that if I deliberately break these rules, I could be stopped from using the school network and accessing the Internet.

Child's signature……

Signature of Parent or Carer ……..

Date…….