E-safety Policy

Introduction

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. 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
- Search engines
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

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 and that some have minimum age requirements (13 years in most cases).

At Ocean Lodge Independent School we understand the responsibility to educate our pupils on E-safety Issues; teaching them the appropriate behaviours and critical 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.

Revised November 2016
Next review Nov 2017

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

Both this policy and the Acceptable Use Agreement (for all staff, regular visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, 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 and other mobile devices).

Legislation

Legislation used to inform this policy is as follows:

- Data Protection Act 1998
- The Telecommunications (Lawful Business Practice)
- (Interception of Communications) Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Racial and Religious Hatred Act 2006
- Sexual Offences Act 2003
- Communications Act 2003
- The Computer Misuse Act 1990
- Malicious Communications Act 2003
- Copyright, Design and Patents Act 1988
- Public Order Act 1986
- Childrens' Act 2004
- Obscene Publications Act 1959 and 1964
- Protection from Harassment Act 1997

Roles and Responsibilities

As E-safety is an important aspect of strategic leadership within the school, the Headteacher has ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-safety co-ordinator is Amy Loines, Headteacher. All members of the school community have been made aware of who holds this post. It is the role of the E-safety co-ordinator to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.

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 telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) 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 or voice-mail account where applicable, 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.

Breaches

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

breach is grounds for disciplinary action. Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

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 school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individual in the organisation is the Safeguarding Lead, Karen Ward. Karen will then log an incident report with Dan Filby, IT Manager at Head Office.

E-safety policy

Disposal of ICT equipment

Disposal of ICT equipment will be arranged through Dan Filby, IT Manager, Head Office.

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

Email

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsible online.

Managing e-mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

E-safety policy

- Staff should use their school email for all professional communication
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive or upsetting e-mail
- Staff must inform the Headteacher if they receive an offensive e-mail
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending emails

- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising

E-safety policy

Receiving e-mails

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; consult your network manager first
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact itsupport@sqcp.com immediately.
- IT Support will advise you what actions to take and be responsible for advising others that need to know.

E-safety in the curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety.

- Ocean Lodge Independent School provides opportunities within a range of curriculum areas to teach about E-safety
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the curriculum

E-safety policy

- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff adult, or an organisation such as Childline or NSPCC.

  We endeavour to embed E-safety messages across the curriculum whenever the internet and/or related technologies are used
- The E-safety policy will be introduced to the pupils at the start of each school year
- E-safety posters will be prominently displayed
- The key E-safety advice will be promoted widely through school displays, newsletters, class activities etc

Pupils with additional needs

The school endeavours to create a consistent message for all pupils and this in turn should aid establishment and future development of the schools' E-safety rules. However, staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-safety. Internet activities are planned and well managed for these pupils.

E-safety policy

Taking Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must 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 written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
  Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication

Publishing Pupil Images and Work

On a child'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
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/transmitted on a video or webcam
- on the school's learning platform or Virtual Learning Environment
- 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, eg 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 unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents or carers may withdraw permission, in writing, at any time. Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names 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. Only the IT Manager or Headteacher has authority to upload to the internet.

Webcams and CCTV

The school uses CCTV for security and safety. The only people with access to this are the staff at Ocean Lodge Independent School and Potton Homes.

We do not use webcams in Ocean lodge Independent School.

School ICT Equipment

As a user of the school ICT equipment, you are responsible for your activity

It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory.

- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do 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

E-safety policy

- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:

    - Maintaining control of the allocation and transfer
    - Recovering and returning equipment when no longer needed
    - 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

This section covers such items as laptops, mobile devices and removable data storage devices.

- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted

E-safety policy

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- 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 support team, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Removable Media

If storing or transferring personal, sensitive, confidential or classified information using Removable Media:

- Always consider if an alternative solution already exists
- Only use recommended removable media
- Encrypt and password protect
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school blocks Facebook and Twitter.
- Staff ***are not*** permitted to access their personal social media accounts using school equipment at any time during school hours
- Pupils are not permitted to access their social media accounts whilst at school

E-safety policy

- Staff, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

To be read in-conjunction with:

- Mobile Phone Policy
- Child Protection Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Pupil Code of Conduct
- PSHE Policy
- Curriculum Policy

Proprietor signature  **.....** **Date: 30/11/16**

Revised November 2016
Next review November 2017