Edward Peake C of E (VC) Middle School

Headteacher: Miss Z J Linington

Potton Road • Biggleswade • Bedfordshire • SG18 0EJ
Tel: 01767 314 562 • Fax: 01767 314 006
E-mail: info@edwardpeake.beds.sch.uk
Web: http://www.edwardpeake.beds.sch.uk

ICT Acceptable Use Policy Incorporating E-Safety, Data Security & Disposal of ICT Equipment

Introduction

The Information and Communication Technology Policy 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
- ✓ Mobile/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.

Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff who is familiar with information risks and the school's response to those risks. Edward Peake C of E (VC) Middle School's **SIRO** is **Miss Hayley Butchard** who has the following responsibilities:

- responsible for information risk management, associated policies and risk assessments
- to manage all Information Asset Owners (IAO) in respect of information and data
- to investigate thoroughly and promptly all incidents and breaches reported and discuss with the Headteacher findings and any recommended follow up action
- the SIRO will consult with HR and Partnership Education depending on the level of the breach

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support SIROs in their role.

Information Asset Owners (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of pupils and staff; such as assessment records, medical information and special educational needs data.

The role of any IAO is 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, pupil or staff etc. including UPN, teacher DCSF number 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 off

Examples of IAOs at Edward Peake C of E (VC) Middle School are the Office Manager, Assessment Manager, Finance Manager and SEN Administrator.

However, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even result in legal action.

E-Safety in the Curriculum

At Edward Peake C of E (VC) Middle 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 be safe, responsible digital citizens when using the internet and related technologies, in and beyond the context of the classroom.

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. The school uses Computing and PSHCE lessons to deliver e-safety based activities. In addition, cyberbullying issues are also addressed as part of anti-bullying week each year. However, e-safety is addressed across the curriculum informally as part of SMSC (spiritual, moral, social and cultural) learning wherever digital technology is used to support learning. Further guidance regarding online working can be found in the Safeguarding and Child Protection Policy.

Where appropriate, 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 and respecting other people's information, images, etc. through discussion, modelling and activities.

Pupils are made aware of the impact of online bullying; sharing personal information and images including the implications of 'sexting'. Pupils are also made aware of the impact of online 'grooming'. They know how to seek help if they are affected by these issues. Pupils are also made 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 member, or an organisation such as Childline/ CEOP report abuse button.

E-safety resources and web links are available to pupils and parents via the school website.

For further information and resources relating to e-safety please visit:

www.digizen.org
www.childnet.com
www.kidsmart.org.uk
www.ceop.police.uk
www.childline.org.uk
www.**think**u**know**.co.uk

Social Media
For all information regarding the appropriate use of social media by all stakeholders please refer to the Social Media Policy.

E-mail
The use of e-mail within school is an essential means of communication for staff, Governors 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 the wider community or international.

The school gives all staff, Governors and pupils their own G-mail account which forms part of the Virtual Learning Environment 'Apps'. This is set up with associated security rights and policies through Google and RealSmart (The School Virtual Learning Environment Host/Provider).

It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged. The school email account should be the account that is used for all school business. Email accounts may be subject to track and trace procedures if concerns arise.

Staff Emails
Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

Staff are expected to acknowledge emails within 48 hours and action within 72 hours.

Staff must inform SIRO if they receive an offensive email.

However, school emails are accessed (whether on school equipment or non-school hardware such as laptops, tablets or smartphones) all the school email policies apply.

Pupil Emails
Pupils may only use school approved Gmail accounts through the Virtual Learning Environment and are restricted to 'Domain Users' only, to increase security.

Pupil emails are filtered using Google security policies and emails containing banned words or phrases will be blocked.

Pupils must immediately tell a teacher/ trusted adult if they receive an offensive email.

Breaches
The network is monitored in real time using 'Smoothwall', the school's firewall and filtering solution. All breaches are flagged as 'violations' or 'alerts' referenced against a database of banned words and content. The system is monitored by the school Network Technician and any initial breaches by pupils are passed to the SIRO in the first instance. Information regarding the procedures for dealing with a breach by a pupil can be found in the 'Behaviour Policy'.

A breach or suspected breach of policy by a pupil or contractor may result in the temporary or permanent withdrawal of School ICT hardware, software and/or services from the offending individual.

A breach or suspected breach of policy by a member of staff or governor could lead to disciplinary action. Please refer to section 1.4 in the Code of Conduct for All Adults Policy.

Incident Reporting
All incidents of misuse or unauthorised use of ICT and any non-compliance issues resulting in a policy breach must be reported to the school SIRO as soon as possible – this includes (but is not limited to):

- security breaches or attempts
- lost/stolen equipment or data (including remote access and PINs)
- unauthorised use or suspected misuse of ICT
- virus notifications, unsolicited emails.

E-Safety Incidents Reporting
All incidents of access to inappropriate material using the school network, equipment or internet connection must be reported to the SIRO.

All incidents involving pupils should be recorded on the schools MIS behaviour log.

When access to inappropriate material is reported, the SIRO will take immediate action to block future access.

Staff should ensure all complaints relating to e-safety are dealt with in accordance with the School Complaints policy.

Internet Access
Internet access is provided through a firewall. Firewall settings are subject to the network's access rights and security settings of the user.

Pupils will have supervised access to Internet resources. They are encouraged to report to the teacher any inappropriate content or images they encounter.

Staff will preview any recommended sites before use.

Internet Use
When accessing the internet by whatever means on the school premises by a stakeholder the following are not allowed:

- The posting of personal, sensitive, confidential or classified information or the dissemination of such information in any way that may compromise its intended audience
- On-line gambling or gaming
- The viewing of sites containing offensive, inappropriate or pornographic material.

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

At present the school denies access to social networking sites to pupils and staff within school.

Data Security Measures
All users of the school digital network are provided with a unique username and password. This is set up with associated security rights and policies using industry standard security.

The Digital network is protected by a firewall. This is maintained by the school IT support service.

The School gives relevant staff access to its Management Information System, with a unique

username and password. This is set up with associated security rights and policies.

Staff and Governors are expected to change network and Virtual Learning Environment passwords at the beginning of each new term. It is the responsibility of all staff and Governors to keep passwords secure.

Staff and Governors are aware of their responsibility when accessing school data as outlined in the Data Protection Policy.

Only the school IT Service provider and Senior Information Risk Owner (SIRO) will have Network administrative rights.

Staff will avoid leaving any Laptop or workstation unattended. Where this is not possible, usernames should be digitally locked to stop unauthorised access to data.

Staff will adhere to the code of conduct outlined in the 'Loan of Laptops Scheme'.

Images and Film

Edward Peake C of E (VC) Middle School seeks consent of parents (on behalf of pupils) to take images and film of pupils at the beginning of each academic year or on admission. A list of pupils who are not permitted to have images or film taken is compiled and shared with all staff.

Publishing Pupil's Images and Work

Images and film may be used:

- on the school web site or Virtual Learning Environment
- in the School Prospectus and other printed publications that the school may produce for promotional purposes
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas such as exhibitions 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)

Consent by the parent is considered valid for all the above. Parents/ carers may withdraw permission, in writing, at any time.

Pupils' full names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

Before posting pupil work/images on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Asset Management

All digital equipment is logged on the school's Asset Register against the product information such as serial number or tag code. This information can only be changed by the school's Network Technician.

External and Personal Devices

The school prohibits the use of external storage devices such as USB & external hard drives. PC devices which are brought onto the school premises must only be those provided by the school.

Computer Viruses

All files downloaded from the Internet and received via email are checked for viruses using school provided anti-virus software.

Anti-virus software installed on school ICT equipment will be maintained by the school IT support provider and must not be altered by any other individual.

Suspected viruses must be reported to the Network Technician/SIRO immediately or as soon as is reasonably possible.

Disposal of Redundant ICT Equipment Policy
All redundant ICT equipment is disposed of through appropriate agencies. This includes a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant ICT equipment which may have held personal data will have the storage media over-written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. Only authorised companies are used who will supply a written guarantee that this will happen.

Disposal of any ICT equipment will conform to:

- The Waste Electrical and Electronic Equipment Regulations 2006
- The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
- Data Protection Act 1998
- Electricity at Work Regulations 1989

The school maintains a comprehensive Asset Register of all its ICT equipment including a record of disposal.

Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

Both this policy and the Acceptable Use Agreements for staff, governors, visitors and pupils (Appendix A and B) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, virtual environments, 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.).

Signed _____

Chair of Governors

Date approved June 2022

Review date June 2023

Appendix A

Edward Peake C of E (VC) Middle School
Staff, Governors and Visitors
Acceptable Use Agreement / Code of Conduct

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, Governors and visitors are aware of their responsibilities when using any form of ICT equipment and applications in school. For members of staff with a school laptop this policy also applies to its use away from the school premises. Any concerns or clarification should be discussed with the Senior Information Risk Owner (SIRO).

- I will only use the school's email / Internet / Intranet / Virtual Learning Environment and any related technologies for professional purposes associated with the work being undertaken at Edward Peake C of E (VC) Middle School.
- 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 pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system 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 data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be password protected or encrypted.
- I will not install any non-educational hardware or software without permission of the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils 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. Images will not be distributed outside the school network without the permission of the parent/ carer.
- 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 the Headteacher.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand that any breach in this agreement could lead to disciplinary action. Please refer to section 1.4 in the Code of Conduct For All Adults Policy.

Declaration

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.....

Acceptable Use Policy (Computers)

We expect all pupils to understand and follow a few simple rules when using the School Network. These rules are as follows:

- You must only use the computers for school related work or for activities authorised by a teacher.
- You must not install any software on the network. This includes screensavers and games.
- You must not use anyone else's username to log on to the network and you must not tell anyone else your password.
- You must not eat or drink in the computer rooms.
- You may only use the Internet when there is a teacher or supervisor in the room or if you have a note from a teacher which is dated and signed and which states clearly what you are researching.
- When accessing the Internet you must not try to download anything that is unlawful, obscene or abusive. If you come across such information accidentally you should turn off the computer monitor and quietly tell a teacher.
- You must not use the Internet for buying or selling goods.
- You must not log onto chat sites on the Internet.
- When using email you must not send any message that is harmful, offensive or abusive to other people.

If you break these rules you will lose the right to use the computers and you are likely to be given a detention or other school punishment.

The computer rooms are monitored and we can monitor what pupils do on the network. Please do not feel offended by this. The aim is to give you as much freedom as possible to use the network properly and to prevent other people from spoiling this facility.

Our school promotes safe use of the Internet. For further information on safe Internet use at home log on to: www.direct.gov.uk/en/parents/yourchildshealthandsafety/internetsafety

Acceptable Use Policy (Computers)

Please Complete

Pupil Name: _____ Form: _____

I have read and understand the school Acceptable Use Policy (Computers). I will use the computer system and Internet in a responsible way and obey these rules at all times.

Pupil Signature: _____ Date: _____

Parent/Carer's Consent for Internet Access

I have read and understand the school Acceptable Use Policy (Computers) and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of material accessed through the Internet. I agree that the school is not liable for any damages arising from the use of the Internet facilities.

Parent/Carer Name: _____

Signed: _____ Date: _____

Parent/Carer's Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter's work may be published on the school website and other publications. I also agree that photographs which include my son/daughter may be published subject to the school rules, that photographs will not identify individuals and that full names will not be used.

Signed: _____ Date: _____