Prettygate Infant School
E safety and Data Security Policy

Spring 2014 Review annually Spring term

Introduction

ICT in the 21st Century is 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 these technologies in order to arm our young people with the skills to access life-long learning and employment.

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
- Mobile/ Smart phones with text, video and/ or 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 Prettygate Infant School, we understand the responsibility to educate our pupils on eSafety 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.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties. All staff are made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), 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
All internet activity is logged by the school's internet provider. These logs may be monitored by authorised Essex County Council (ECC) staff.

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.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the Essex County Council Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting
Any security breaches or attempts, loss of equipment or data and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher.

Acceptable Use Agreements

The following acceptable use agreements are in place for staff, governors, parents and children at Prettygate Infant School.

Prettygate Infant School
Plume Avenue
Colchester
Essex
CO3 4PH

Tel: 01206 572357
Fax: 01206 768735
www.prettygate-inf.essex.sch.uk

Headteacher: Mrs R. Tingle B.Ed CANTAB

Dear Parent

Internet Permission Form

As part of the school's ICT programme we offer pupils supervised access to the internet. Access to the internet enables pupils to explore thousands of libraries, databases, and bulletin boards. The school uses an internet provider (through Essex County Council) that filters the material that pupils can access.

Before being allowed to use the internet, we must obtain parental permission for all pupils. Please talk about the attached Rules for Responsible Internet Use sheet with your child and return as evidence of your approval and their acceptance of the school rules on the use of the internet. A duplicate copy is enclosed for you to retain.

We believe that the benefits to pupils from access to the internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to agree to access. We do stress however that only a limited range of sites will be available and all internet use will be closely supervised.

We would be grateful if you could complete and return the enclosed form. Thank you.

Yours sincerely

Mrs R Tingle

Headteacher

This is your copy to keep at home.

Prettygate Infant School

Rules for Responsible Internet Use

The school has installed computers and internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will only use the computers for school work.
- I will ask permission from a member of staff before using the internet.
- I will not download programmes from the internet or bring CDs or memory sticks to school.
- I will only e-mail people my teacher has approved.
- The messages I send will be polite and responsible.
- I will not give out my own details such as my name, phone number or home address.

Internet Permission Form

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use electronic mail and the internet. I understand that my child's use of the internet will be supervised at all times.

Parent/Guardian signature ..... date .....

Name of pupil .....

Class .....

Please return this copy to school.

Prettygate Infant School

Rules for Responsible Internet Use

The school has installed computers and internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will only use the computers for school work.
- I will ask permission from a member of staff before using the internet.
- I will not download programmes from the internet or bring CDs or memory sticks to school.
- I will only e-mail people my teacher has approved.
- The messages I send will be polite and responsible.
- I will not give out my own details such as my name, phone number or home address.

Internet Permission Form

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use electronic mail and the internet. I understand that my child's use of the internet will be supervised at all times.

Parent/Guardian signature ..... date .....

Name of pupil .....

Class .....

Prettygate Infant School
Plume Avenue
Colchester
Essex
CO3 4PH

Tel: 01206 572357
Fax: 01206 768735
www.prettygate-inf.essex.sch.uk

Headteacher: Mrs R. Tingle

PRETTYGATE INFANT SCHOOL

Staff, Governor and Visitor 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 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 ICT Co-ordinator or the Headteacher

- I will only use the school's email, Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will not use personal cameras, phones or other web-enabled devices for school business.
- 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, personal e-mail address and social networking identities to pupils.
- I will only use my school email account 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 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 inline with school policy. 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 the Headteacher.
- 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 not discuss pupils or school business in social media.
- 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 this forms part of the terms and conditions set out in my contract of employment.

This Acceptable Use Agreement is a summary of our e-Safety Policy which is available in full on request.

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 . . . . . .

Computer Viruses

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

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the ICT coordinator immediately.

Security

The school gives relevant staff access to its Management Information System with a unique ID and password.

Personal cameras/phones or other web enabled devices are kept in a secure place out of pupils reach.

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 removal storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.

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.

Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed of through an authorized agency only. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

e-Mail

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 good network etiquette; 'netiquette'.

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 minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

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

The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder

Pupils may only use school approved accounts on the school system and only under direct

teacher supervision for educational purposes

Staff check their emails regularly.

Never open attachments from an untrusted source.

Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

E-mailing personal, sensitive, confidential or classified information
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 wherever possible

Where the conclusion is that e-mail must be used to transmit such data, exercise caution.

Equal Opportunities

Pupils with additional needs
The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

eSafety – Roles and Responsibilities
As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Penny Carter. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such ECC, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our 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 pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE

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

The school provides opportunities within a range of curriculum areas to teach about eSafety.

Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.

Pupils are 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 or CEOP report abuse button.

eSafety 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 eSafety and know what to do in the event of misuse of technology by any member of the school community

Managing the School eSafety Messages

We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.

The eSafety policy is introduced to the pupils at the start of each school year.

eSafety posters are prominently displayed

Incident Reporting, eSafety Incident Log and Infringements

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported.

eSafety Incident Log

PRETTYGATE INFANT SCHOOL

e-Safety Incident Log

Details of ALL e-Safety incidents to be recorded by the e-Safety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors.

Date & Time	Name of pupil or staff member	Male or Female	Room and computer/device number	Details of incident (including evidence)	Actions and reasons

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the **Essex Flowcharts for Managing an eSafety Incident** should be followed.

Inappropriate Material
All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)

Users are made aware of sanctions relating to the misuse or misconduct through the acceptable use policy.

Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an illegal e-safety incident

Following an e-safety incident a decision will have to be made quickly as to whether the incident involved any illegal activity

Has illegal activity taken place?

Examples of illegal activity would include:

- Downloading abusive images
- Passing child pornography to others
- Inciting racist or religious hatred

Still unsure?

For further advice ECC ISIS helpdesk on

YES

- ✓ Inform Essex Police and Essex County Council
- ✓ Follow the advice given by the Police, or
- ✓ Confiscate the device and if related to the school network disable user account
- ✓ Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence
- ✓ If a pupil is involved contact Social Care Direct to make an emergency referral on 0845 603 7634
- ✓ If it involves a member of staff contact the LADO on 01245 436744

NO

Go to next flowchart which outlines the process for non-illegal incidents

Users must be aware that if they find something unpleasant or frightening they should switch off their screen or close the laptop and talk to a member of staff

Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an e-safety incident where no illegal activity has taken place

The Headteacher/e-Safety Co-ordinator should:

- **Record the incident in the e-safety log**
- **Keep any evidence**

Did the incident involve a member of staff?

YES

If a 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 that indicates that s/he may be unsuitable to work with children Contact LADO on 01245 436744

- Review evidence and determine whether the incident was accidental or deliberate
- Decide upon the appropriate course of action
- Follow school

NO

Was the Child the victim or perpetrator

Pupil as

Support the pupil by one or more of the following:

- Class Teacher
- e-Safety Co-ordinator
- Headteacher/Senior Leader
- Designated Child Protection Officer
- School PCSO

Inform Parent/carer as appropriate

If the child is at risk contact Social Care Direct to make an emergency referral on 0845 603 7634

Pupil as Instigator

- Review incident to decide if other pupils were involved
- Decide appropriate sanctions
- Inform Parent/Carer if serious or persistent incident
- If serious, consider informing the Duty Safeguarding

Incident types could be:

- Using another persons user name or password
- Accessing websites which are against the schools policy e.g. gaming
- Using a mobile

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

The school maintains students who will have supervised access to internet resources (where reasonable) through the school's fixed and mobile internet technology.

Staff will preview any recommended sites before use.

All users must observe copyright of materials from electronic resources.

Infrastructure

School internet access is controlled through the LA's web filtering service

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

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety co-ordinator 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.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety 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)

Parents/carers are expected to sign a Home School agreement containing the following statement or similar

We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community

The school disseminates information to parents relating to eSafety where appropriate in the form of;

- Information evenings
- Posters
- Website
- Newsletter items

Passwords

Always use your own personal passwords to access computer based services.

Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.

Change passwords whenever there is any indication of possible system or password compromise.

Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team.

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

Ensure that any school information accessed from your own PC or removable media equipment is kept secure.

Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised acess.

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

Ensure removable media is purchased with encryption.

Store all removable media securely.

Securely dispose of removable media that may hold personal data.

Encrypt all files containing personal, sensitive, confidential or classified data.

Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

Safe Use of Images

Taking of images and film

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.

Pupils and parent helpers are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others.

Staff are not permitted to use school digital equipment for personal use.

Publishing Pupil's images and work

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

- On the school website
- 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 ie. 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.

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

Further information relating to issues associated with School websites and the safe use of images in Essex schools on the Essex Schools Infolink. **Storage of Images**
Images/films of children are stored on the school's network and school ipads.

Pupils and staff are not permitted to use personal media for storage of images (e.g. USB sticks) without the express permission of the Headteacher.

Webcams and CCTV

Webcams in school are only ever used for specific learning purposes i.e. monitoring hens' eggs and never using images of children or adults.

School ICT Equipment includng Portable and Mobile ICT Equipment and Removable Media

School ICT Equipment
As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.

The school logs ICT equipment issued to staff and records serial numbers on the inventory. Ensure that all ICT equipment that you use is kept physically secure.

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

It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's newtwork drive.

Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted.

Any PCs etc accessing personal data must have a locking screensaver as must any user profiles.

Privatedly 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 log ons 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.

Portable and Mobile ICT Equipment
This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

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 the laptop. Any equipment where personal data is likely to be stored must be encrypted

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

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

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. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer

using their personal device.

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

The sending of inappropriate text messages between any member of the school community is not allowed.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided mobile devices (including phones)
The sending of inappropriate text messages between any member of the school community is not allowed.

Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.

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

- Only use recommended removable media
- Store all removable media securely.
- Removable media must be disposed of securely by your ICT support team.

Servers
Newly installed servers holding personal data should be encrypted, therefore password protecting data. SIMs Database Servers installed by SITSS since April 2009 are supplied with encryption software

Always keep servers in a locked and secure environment

Limit access rights to ensure the integrity of the standard build

Always password protect and lock the server

Existing servers should have security software installed appropriate to the machine's specification

Back up tapes should be encrypted by appropriate software

Data must be backed up regularly

Back up tapes/discs must be securely stored in a fireproof container

Back up media stored off-site must be secure

Remote back ups should be automatically securely encrypted.

Regular updates of anti-virus and anti-spyware should be applied

Systems and Access

You 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

Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you

Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else

Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access

Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time

Do not introduce or propagate viruses

It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or ECC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, 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

Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Writing and Reviewing this Policy

Staff and Pupil involvement in Policy creation

Staff, governors and pupils have been involved in making and reviewing the Policy for ICT Acceptable Use through staff meetings, governor meetings and the School Council.

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety or data security that concerns them.

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read, amended and approved by the staff, head teacher and governors on 11th March 2014.

Appendix

Current Legislation

Acts Relating to Monitoring of Staff eMail

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. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

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

Other Acts Relating to eSafety

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 (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

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
http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx