Full e-safety

and

Data Security Policy

Guidance Policies for ICT Acceptable Use

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, Cornelius school s 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 the Cornelius 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.

Cornelius school s holds 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 Cornelius school. This can make it more difficult for your Cornelius school to use technology to benefit learners.

Everybody in the Cornelius 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.

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 Cornelius 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 Cornelius school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the Cornelius school staff, at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

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 or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain Cornelius school business related information; to confirm or investigate compliance with Cornelius school policies, standards and procedures; to ensure the effective operation of Cornelius 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 staff, with the permission of the head teacher 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 Cornelius school ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

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

Any policy breach is grounds for disciplinary action in accordance with the Cornelius 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 and any unauthorised use or suspected misuse of ICT must be immediately reported to Mr J Hibben, the Cornelius school 's Senior Information Risk Owner (SIRO) or e-safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your SIRO.

See flowchart on pages 22 for dealing with both illegal and non-illegal incidents

Example of Acceptable Use Agreement for Pupils

Acceptable User Policy

Pupil Acceptable User Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all pupils are fully aware of their responsibilities when using any form of ICT. All pupils are required to sign this policy and adhere at all times to its contents.

I will...

- only use the ICT systems in school; including the internet, email, digital video, mobile technologies etc for school purposes
- only log on to the school network/ learning platform/ devices with my own user name and password
- follow the school's ICT security system and not reveal my passwords to anyone; and change them regularly
- respect the privacy of other users and behave in a sensible and mature way at all times; never giving out personal details or anyone else's details e.g. email, phone number, personal address etc
- only use approved collaboration tools such as forums, chat rooms or messaging for exchanging information and constructive debate or as part of a teacher-led educational project
- always aim to save my work correctly and use sensible file management techniques at all times
- ensure I do not infringe copyright by sharing music, games and videos with others
- only view, download, store, distribute, share or upload lawful and appropriate material; seeking guidance form a member of staff if I am unsure
- not deliberately browse, download, upload or forward or share material that could be considered offensive or illegal; and if you accidentally come across any such material you will report it to a member of staff immediately
- not play games, music or videos without the express permission of a teacher
- make sure that all ICT communications with pupils, teachers or others is responsible and sensible
- not try to add members of staff as "friends" on social network sites that I use outside of school
- not attempt to bypass any internet filtering systems
- ensure that all my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute

I understand that...

- technology should not be used to upset, offend, harass, threaten or harm anyone even if it is meant as a joke
- images of pupils and or members of staff are only for use in school and must not be distributed outside the school network
- it is my responsibility to report any abuse and/ or if I feel unsafe online
- all my use of the internet and other technologies can be monitored and monitored and can be made available to teachers and parents/ carers

• these rules are designed to keep me safe and that if they are not followed school sanctions will be applied and parents/ carers will be contacted

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

Signature _____

Date _____

Full Name _____

Tutor Group _____

Example of Letter to parents

Dear Parent/ Carer

ICT including the Internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our Cornelius school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of e-safety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or Mr Hibben e-safety coordinator.

Please return the bottom section of this form to Cornelius school for filing.

This Acceptable Use Agreement is a summary of our e-safety Policy that is available in full via our publications scheme on our website/on request.

✂----------

Pupil and Parent/ carer signature
We have discussed this document and …….....(pupil name) agrees to follow the e-safety rules and to support the safe and responsible use of ICT at Cornelius school.

Parent/ Carer Signature ……..…….

Pupil Signature…….

Form …… Date ……

Acceptable Use for Staff and Governors

Acceptable User Policy

Staff Acceptable User Agreement

This policy is designed to support the school's adoption of a managed service from September 2011.

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all members of staff are fully aware of their professional responsibilities when using any form of ICT. All members of staff are required to sign this policy and adhere at all times to its contents. In addition, teaching staff should also be aware that this policy also applies to their Teacher Toolkit and in particular their Apple Mac-Book Pro laptop device.

Any concerns or clarifications should be discussed with Mr S Wilson, Deputy Head teacher.

I will...

- only use the school's email/ internet/ intranet/ learning platform and any related technologies for professional purposes or for uses deemed "reasonable" by the Head Teacher
- use the ICT technologies sensibly, professionally, lawfully, and in a manner consistent with my duties and with respect for pupils and colleagues
- comply with the ICT system security and not disclose any usernames or passwords provided to me by the school or other related authorities
- ensure that all electronic communications with pupils and staff are compatible with my professional role
- not give out my own personal details, accounts or data (e.g. mobile phone number, Face-book details, emails etc) to pupils or parents
- only use the approved, secure email systems for any school business
- ensure that personal data (such as data held on SIMS) 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 teacher
- not install any hardware or software without permission of Mr S Wilson, Deputy Head teacher
- browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- support the school approach to online safety and not deliberately upload or add any images, video sounds or text that could upset or offend any member of the school community
- respect copyright and intellectual property rights and teaches my pupils to do so
- ensure my online activity, both in school and outside school, will not bring my professional role into disrepute
- ensure that pupils only use and know how to use ICT technologies sensibly, lawfully and appropriately
- support and promote the school's e-safety policy and help pupils to be safe and responsible in their use of ICT technologies

I understand that...

- I am expected to use my Teacher Toolkit in every lesson (only applies to teachers)
- images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy – in relation to images of pupils it is required that staff check the appropriate permission from home has been given
- images will not be distributed outside the school network without permission of the parent/ carer, member of staff and Head teacher
- all my use of the internet and other related technologies can be monitored and logged; in addition, this can be made available to the Head teacher and or the line manager
- it is my responsibility to look after any laptop (including a MacBook Pro)
- this policy forms part of the terms and conditions set out in my contract of employment

User Signature

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

Signature _____

Date _____

Full Name _____

Job Title _____

Computer Viruses

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

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

- If your machine is not routinely connected to the Cornelius school network, you must make provision for regular virus updates through your IT team

- If you suspect there may be a virus on any Cornelius school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know

Data Security

The accessing and appropriate use of Cornelius school data is something that the school takes very seriously.

Teachers and Governors Guidance
http://esi.essexcc.gov.uk/vip8/si/esi/content/binaries/documents/Service_Areas/HR/Workload_Agreement/Guidance_Docs/dfes-InformationManagementSkillsforSuccess.pdf

Internet filtering for Essex Cornelius school s
http://www.e-gfl.org/index.cfm?s=1&m=283&p=31,view_item&start=1&id=4816

E-Safety Audit Tool - Information for Governors, Management and Teachers
http://www.nen.gov.uk/hot_topic

Security

- The Cornelius 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 Cornelius school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff have read the relevant guidance documents available on the EGfL website
- Leadership have identified Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO)
- Staff keeps all Cornelius 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 mopiers (multi-function print, fax, scan and copiers) are used

Impact Levels and Protective Marking

- Appropriate labelling of data should help Cornelius school secure data and so

reduce the risk of security incidents

- Apply labelling in accordance with guidance from your Senior Information Risk Owner (SIRO)
- Most learner or staff personal data will be classed as Protect, although some data e.g. Child Protection data, should be classed as Restricted.
- Protect/Restrict and caveat classifications that Cornelius school s may use are;
    - PROTECT – PERSONAL e.g. personal information about an individual
    - PROTECT – APPOINTMENTS e.g. to be used for information about visits from the Queen or government ministers
    - PROTECT – LOCSEN e.g. for local sensitive information
    - PROTECT – STAFF e.g. Organisational staff only
    - RESTRICTED e.g. sensitive personal information about an individual
- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business
- The protective mark should be in bold capital letters within the header and footer of each page of a document
- Applying too low a protective marking may lead to damaging consequences and compromise of the asset
- The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents

Reviews are continuing to look at the practical issues involved in applying protective markings to electronic and paper records and government representatives are working with suppliers to find ways of automatically marking reports and printouts.

Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff (Mr J Hibben) who is familiar with information risks and the Cornelius school 's response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities:

- they own the information risk policy and risk assessment
- they appoint the Information Asset Owner(s) (IAOs)
- they act as an advocate for information risk management

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.

The SIRO in this Cornelius school is J Hibben

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal

data of learners and staff; such as assessment records, medical information and special educational needs data. Cornelius school s should identify an Information Asset Owner. For example, the school ’s Management Information System (MIS) should be identified as an asset and should have an Information Asset Owner. In this example the MIS Administrator or Manager could be the IAO.

The role of an 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

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements. In a Secondary Cornelius school, there may be several IAOs, whose roles may currently be those of e-safety coordinator, ICT manager or Management Information Systems administrator or manager.

Although these roles have been explicitly identified, 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 legal action.

Disposal of Redundant ICT Equipment Policy

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

- All redundant ICT equipment that 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. We will only use authorised companies 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
  http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
  http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
  http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e
  Data Protection Act 1998
  http://www.ico.gov.uk/what_we_cover/data_protection.aspx
  Electricity at Work Regulations 1989
  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

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

- The Cornelius school 's disposal record will include:

  - Date item disposed of
  - Authorisation for disposal, including:
    - verification of software licensing
    - Any personal data likely to be held on the storage media? *
  - How it was disposed of e.g. waste, gift, sale
  - Name of person & / or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- 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

Environment Agency web site

Introduction

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

The Waste Electrical and Electronic Equipment Regulations 2006

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website

http://www.ico.gov.uk/

Data Protection Act – data protection guide, including the 8 principles

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

e-Mail

The use of e-mail within most Cornelius school is an essential means of communication for staff. In the context of Cornelius 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 Cornelius 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 Cornelius school gives all staff their own e-mail account to use for all Cornelius 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 Cornelius school email account should be the account that is used for all Cornelius school business

- Under no circumstances should staff contact pupils, parents or conduct any Cornelius school business using personal e-mail addresses

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

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on Cornelius school headed paper

- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Head teacher, line manager or designated account

- Pupils may only use Cornelius school approved accounts on the Cornelius school system and only under direct teacher supervision for educational purposes

- E-mails created or received, as part of your Cornelius school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- Staff must inform (the e-safety coordinator/ line manager) if they receive an offensive e-mail

- Pupils are introduced to e-mail as part of the ICT Scheme of Work

- However, you access your Cornelius school e-mail (whether directly, through webmail when away from the office or on non-Cornelius school hardware) all the school e-mail policies apply

- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending, reading or receiving business related e-mail is not permitted

Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section E-mailing Personal, Sensitive, Confidential or Classified Information

- Use your own Cornelius school e-mail account so that you are clearly identified as the originator of a message

- If you are required to send an e-mail from someone else's account, always sign on through the 'Delegation' facility within your e-mail software so that you are identified as the sender (if available within your software)

- 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

- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail

- Cornelius school e-mail is not to be used for personal advertising

Receiving e-Mails

- Check your e-mail regularly

- Activate your 'out-of-office' notification when away for extended periods

- Use the 'Delegation' facility within your e-mail software so that your e-mail can be handled by someone else while you are not at work (if available within your software)

- 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

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
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted

- Where your conclusion is that e-mail must be used to transmit such data:

  - Obtain express consent from your manager to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

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

  - Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s) – preferably by telephone
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

In exceptional circumstances, the County Council makes provision for secure data transfers to specific external agencies. Such arrangements are currently in place with:

- Essex Police
- District and Borough Councils within Essex County Council
- Essex NHS Trusts

Future Developments

When sending an e-mail containing personal or sensitive data you need to put a security classification in the first line of the e-mail. For e-mails to do with information about a pupil, for example, you need to put in **PROTECT – PERSONAL** on the first line of the e-mail.

This also needs to go on the top and bottom of any documents that you send (i.e. Word documents, Reports, Forms, including paper documents you send in hardcopy, etc). The name of the individual is not to be included in the subject line and the document containing the information encrypted. This provides additional security.

Equal Opportunities

Pupils with Additional Needs

The Cornelius school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the Cornelius school s' e-safety rules.

However, staff is aware that some pupils may require additional 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 eSafety. Internet activities are planned and well managed for these children and young people.

E-safety

E-safety- Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the Cornelius school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-safety co-ordinator in this Cornelius school is *Mr J Hibben,* who has been designated this role as a member of the senior leadership team. All members of the Cornelius 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 ECC, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ e-safety co-ordinator and all governors have an understanding of the issues and strategies at our Cornelius school in relation to local and national guidelines and advice.

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

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.

- The Cornelius school has a framework for teaching Internet skills in ICT/ PSHE lessons.
- The Cornelius school provides opportunities within a range of curriculum areas to teach about e-Safety
- Educating pupils on the dangers of technologies that maybe encountered outside Cornelius school is done informally when opportunities arise and as part of the e-safety curriculum
- 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, modeling and 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 member, or an organisation such as Childline or CEOP report abuse button

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum*, i.e. Year 5 QCA unit 5c. Year 8 ICT and PSHE units*

E-safety Skills Development for Staff

- Our staff receives regular information and training on e-safety issues in the form of training.
- Details of the ongoing staff training program can be obtained by the deputy head teacher for Teaching and Learning
- New staff receive information on the Cornelius school 's acceptable use policy as part of their induction
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the Cornelius school community (see enclosed flowchart)
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas

Managing the Cornelius school e-safety Messages

- 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 Cornelius school year
- E-safety posters will be prominently displayed

Incident Reporting, e-safetyl ncident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Cornelius school 's SIRO or e-safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner. See Page 11.

E-safety Incident Log

Some incidents may need to be recorded in other places, if they relate to a bullying or racist incident.

Cornlieus Vermuyden
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 e-safety should be made to the e-safety co-ordinator or Head teacher. Incidents should be logged and the Essex Flowcharts for

managing an e-safety 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 e-safety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-safety co-ordinator, depending on the seriousness of the offence; investigation by the Head teacher/ 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 by Mr Hibben.

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
- Extreme cases of cyberbullying

Still unsure?

For further advice ECC ISIS helpdesk on 01245 431851 or Essex Police on 0300 333 4444

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 disciplinary procedures (if deliberate) and contact Schools HR on 01245 436120 or your schools Link Officer

NO

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 phone to take video during a lesson
- Using technology to upset or bully

Was the Child the victim or perpetrator?

Pupil as Victim

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 Officer as the child instigator could be at risk

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. All use of the **Essex Grid for Learning** (EGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

The Cornelius school maintains 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
- Raw image searches are discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute Cornelius school software or illegal software from other sources
- 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 any way that may compromise its intended restricted audience
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog
- On-line gambling or gaming is not allowed

It is at the Head teacher's discretion on what Internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- Essex County Council has a monitoring solution via the Essex Grid for Learning where web-based activity is monitored and recorded
- Cornelius school Internet access is controlled through the LA's web filtering service. For further information relating to filtering please go to essexcc-servicedesk.sen.uk@siemens-enterprise.com
- Our Cornelius school also employs some additional web filtering which is the

responsibility of *Research Machines*

- (Cornelius school name) is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

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

- The Cornelius school does not allow pupils access to internet logs

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

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate

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

- *E-safety for personal removable media*-Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the Cornelius school's responsibility nor the network manager, to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the *(technician/teacher)* for a safety check first

- Pupils and staff are not permitted to download programs or files on Cornelius school based technologies without seeking prior permission from *the Head teacher/technician/ICT subject leader.*

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

Managing Other Web 2 Technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the Cornelius school endeavors to deny access to social networking sites to pupils within Cornelius school
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, Cornelius school details, IM/ email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online
- Our pupils are asked to report any incidents of bullying to the Cornelius school
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Head teacher

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of Cornelius school and also to be aware of their responsibilities. We regularly consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ careers and pupils are actively encouraged to contribute to adjustments or reviews of the Cornelius school e-safety polic*y.*
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to Cornelius 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 Cornelius school website)
- Parents/ carers are expected to sign a Home Cornelius school agreement containing the following statement or similar
    - → **We will support the Cornelius 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 Cornelius school community**
- The Cornelius school disseminates information to parents relating to e-safety where appropriate in the form of;
    - Information and celebration evenings
    - Posters
    - Website/ Learning Platform postings
    - Newsletter items
    - Learning platform training

Passwords and Password Security

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
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- 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
- Passwords must contain a minimum of six characters and be difficult to guess
- User ID and passwords for staff and pupils who have left the Cornelius school are disabled and their areas are removed after a year .

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

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff is expected to have secure passwords, which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the Cornelius school 's e-safety Policy and Data Security
- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username; they are also expected to use a personal password and keep it private
- Pupils are not allowed to deliberately access on-line materials or files on the Cornelius school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of Cornelius school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the Cornelius school network is ***(fill in)***

- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)

- In our Cornelius school , all ICT password policies are the responsibility of RM for individual profiles and J O 'Neill, Head of ICT , for CLIC and all staff and pupils are expected to comply with the policies at all times

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the Cornelius school and therefore no longer have authorised access to the Cornelius school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the Cornelius school has left

- Prompt action on disabling accounts will prevent unauthorized access

- Regularly change generic passwords to avoid unauthorized access (Microsoft© advise every 42 days)

Further advice available http://www.itgovernance.co.uk/

Personal Information Promise

The Information Commissioner's Office launched a Personal Information Promise in January 2009. Cornelius school s may wish to sign up to this promise which is shown below.

The personal information promise is:

I (name and title), on behalf of (name of organisation) promise that we will:

1. value the personal information entrusted to us and make sure we respect that trust;
2. go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
3. consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
4. be open with individuals about how we use their information and who we give it to;
5. make it easy for individuals to access and correct their personal information;
6. keep personal information to the minimum necessary and delete it when we no longer need it;
7. have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
8. provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;
9. put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and
10. regularly check that we are living up to our promises and report on how we are doing

More information available -

To view the promise
http://www.ico.gov.uk/upload/documents/personal_info_promise/pip%20final.pdf
To sign up to the Promise
http://www.ico.gov.uk/about_us/news_and_views/current_topics/personal_info_promise.aspx
go down to the bottom of the page

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any Cornelius 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 access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-Cornelius school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

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

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 Cornelius school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- 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 Cornelius 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-Cornelius school environment

Safe Use of Images

Taking of 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 Cornelius school community or public, without first seeking consent and considering the appropriateness. ECC guidance can be found: http://esi.essexcc.gov.uk/vip8/si/esi/content/binaries/documents/Service_Areas/Governance/Information_Governance_doc_February_2010_2.doc

- With the written consent of parents (on behalf of pupils) and staff, the Cornelius school permits the appropriate taking of images by staff and pupils with Cornelius 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 Head teacher, images can be taken provided they are transferred immediately and solely to the Cornelius 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 the others, this includes when on field trips. However with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the Cornelius school 's network and deleted from the pupil's device

Consent of Adults Who Work at the Cornelius school

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

Publishing Pupil's Images and Work

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

- on the Cornelius school web site
- on the Cornelius school 's Learning Platform
- in the Cornelius school prospectus and other printed publications that the Cornelius school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the Cornelius school 's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the Cornelius 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 Cornelius 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/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

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 Web Manager has authority to upload to the site.

Further information relating to issues associated with Cornelius school websites and the safe use of images in Essex Cornelius school s on the Essex Cornelius school s Infolink: http://esi.essexcc.gov.uk

Storage of Images

- Images/ films of children are stored on the Cornelius school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head teacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the Cornelius school network/ Learning Platform
- *Staff* have the responsibility of deleting the images when they are no longer required, or the pupil has left the Cornelius school

Webcams and CCTV

- The Cornelius school uses CCTV for security and safety. The only people with access to this are designated members of staff .Notification of CCTV use is displayed at the front of the Cornelius school .
- We do not use publicly accessible webcams in Cornelius school
- Webcams in Cornelius are only ever used for specific learning purposes, i.e. monitoring experiments, PE etc and their usage is supervised by members of staff.
- Misuse of the webcam by any member of the Cornelius school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
    - Consent is sought from parents/carers and staff on joining the Cornelius school , in the same way as for all images

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the Cornelius school
- All pupils are supervised by a member of staff when video conferencing
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the Cornelius school
- The Cornelius school keeps a record of video conferences, including date, time and participants.
- Approval from the Head teacher is sought prior to all video conferences within Cornelius school
- The Cornelius school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be CRB checked
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

Cornelius school ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

Cornelius school ICT Equipment

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

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

- Do not allow your visitors to plug their ICT hardware into the Cornelius 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

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

- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles

- Privately owned ICT equipment should not be used on a Cornelius 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 within their Unit
    - 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, 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 Cornelius school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all Cornelius school data is stored on Cornelius 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
- Synchronise all locally stored data, including diary entries, with the central Cornelius 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

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 Cornelius 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 Cornelius school is allowed. Our Cornelius school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The Cornelius 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
- Pupils are allowed to bring personal mobile devices/phones to Cornelius school

but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent

- This technology may be used, however for educational purposes, as mutually agreed with the Head teacher. The device user, in this instance, must always ask the prior permission of the bill payer

- The Cornelius 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 Cornelius school community is not allowed

- Permission must be sought before any image or sound recordings are made on these devices of any member of the Cornelius school community

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

Cornelius school Provided Mobile Devices (including phones)

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

- Permission must be sought before any image or sound recordings are made on the devices of any member of the Cornelius school community

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

- Where the Cornelius school provides a laptop for staff, only this device may be used to conduct Cornelius school business outside of Cornelius school

---

Removable Media

If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section '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
- Backup tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Backup tapes/discs must be securely stored in a fireproof container
- Backup media stored off-site must be secure
- Remote backups should be automatically securely encrypted.
- Regular updates of anti-virus and anti-spyware should be applied
- Records should be kept of when and which patches have been applied
- Ensure that web browsers and other web based applications are operated at a minimum of 128 BIT cipher strength

e-safety guidelines to be displayed throughout the Cornelius school

Systems and Access

- You are responsible for all activity on Cornelius school systems carried out under any access/account rights assigned to you, whether accessed via Cornelius school ICT equipment or your own PC

- Do not allow any unauthorised person to use Cornelius 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 Cornelius school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the Cornelius school or may bring the Cornelius 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 Cornelius 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 Cornelius school systems, hardware or used in relation to Cornelius school business may be subject to The Freedom of Information Act

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

- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing of the data.

Telephone Services

- You may make or receive personal telephone calls provided:

    1. They are infrequent, kept as brief as possible and do not cause annoyance to others

    2. They are not for profit or to premium rate services

    3. They conform to this and other relevant ECC and Cornelius school policies.

- Cornelius school telephones are provided specifically for Cornelius school business purposes and personal usage is a privilege that will be withdrawn if abused

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

- Ensure that your incoming telephone calls can be handled at all times

- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask your unit manager

---

Mobile Phones

- You are responsible for the security of your mobile phone. Always set the PIN code on your mobile phone and do not leave it unattended and on display (especially in vehicles)

- Report the loss or theft of any mobile phone equipment immediately

Writing and Reviewing this Policy

Staff and Pupil Involvement in Policy Creation

- Staff and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use through *how, i.e. Cornelius school council, staff meetings.*

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 Cornelius 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. Cornelius school s 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 person's 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

---

Review Procedure

There will be an on-going opportunity for staff to discuss with the e-safety coordinator any issue of e-safety that concerns them

There will be an on-going opportunity for staff to discuss with the SIRO/AIO any issue of data security that concerns them

This policy will be reviewed every (12) months and consideration given to the implications for future whole Cornelius 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…….