St Benedict's College

Online Safety

and

Data Security

Policy for ICT Acceptable Use

Updated March 2017

CONTENTS

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 St Benedict's College we understand the responsibility to educate students on online 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.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the college.

Everybody in the college 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 students) are inclusive of both fixed and mobile internet; technologies provided by the college (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto college premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

All internet activity is logged by the college'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 college employee, contractor or student may result in, but is not limited to, the temporary or permanent withdrawal of college ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the College 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 the College Information Manager (CIM). 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 the ICT system manager.

See flowcharts on page 18 for dealing with both illegal and non-illegal incidents

Acceptable use agreement – Students

Acceptable Use Agreement/Online Safety Rules:

- I will only use IT systems in college, including the internet, e-mail, digital video, mobile technologies, etc. for college purposes.
- I will not download or install software on college IT equipment.
- I will only log on to the college network / cloud storage (Office 365) with my own user name and password.
- I will follow the college's IT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my college e-mail address for college related communication.
- I will make sure that all IT communications with students, teachers or others are responsible and sensible.
- I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a college project approved by my teacher.
- Images of students and/or staff will only be taken, stored and used for college purposes in line with college policy and not be distributed outside the college network without the permission of the Principal.
- I will ensure that my online activity, both in college and outside college, will not cause the staff, students or others distress or bring my college into disrepute.
- I will respect the privacy and ownership of others' work online at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, college sanctions will be applied and my parent/carer may be contacted.

March 2016

<Date>

Dear Parent/Carer

IT including the internet, learning platforms, e-mail and mobile technologies continue to be an important part of learning at St Benedict's College. We expect all students to be safe and responsible when using IT at the college. It is essential that students are aware of online safety and know how to stay safe when using IT. Information about staying safe online is taught in computing lessons and can be found on the college website at http://www.stbenedicts.essex.sch.uk/safety .

Students are asked to read and discuss the attached agreement, which is based on the Essex County Council online safety policy, with their parent or carer and then to sign and follow the terms of the agreement while at the college. Any concerns or explanation can be discussed with their class teacher or any member of the leadership team at the college.

Please return the bottom section of this form to the college for filing by Friday 18th March 2016. Failure to return the form below may result in removal of IT privileges.

Yours faithfully

Mrs J E Santinelli
Principal

✂----------

To: College office by Friday <Date>

Student and parent/carer signature

Name of student: ..... Form: .....

I have discussed this document with my parent/carer and I agree to follow the online safety rules and to support the safe and responsible use of IT at St Benedict's College.

Student signature…….

I have discussed this document with my child and I will encourage him/her to follow the online safety rules and to support the safe and responsible use of IT at St Benedict's College.

Parent/Carer signature …….

Date ……

Acceptable Use Policy – Staff/Governors

Staff, Governor and Visitor Acceptable Use Agreement

IT (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 college. This policy is designed to ensure that all staff, governors and visitors (college personnel) are aware of their professional responsibilities when using any form of IT.

All college personnel are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Principal or appointed representative.

- I will only use the college's e-mail / internet / intranet / cloud storage (Office 365) and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Governing Body.
- I will comply with the IT system security and not disclose any passwords provided to me by the college or other related authorities
- I will ensure that all electronic communications with students 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 students.
- I will only use the approved, secure e-mail system(s) for any college business.
- I will ensure that personal data (such as data held on SIMS software) is kept secure and is used appropriately, whether in college, taken off the college premises or accessed remotely. Personal data can only be taken out of college or accessed remotely when authorised by the Principal or Governing Body.
- I will not install any hardware or software without permission of the business manager or a member of the college IT technical team.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/or staff will only be taken, stored and used for professional purposes in line with the college Online Safety policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the college network without the permission of the parent / carer, member of staff and the Principal.
- 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 Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in college and outside college, will not bring the college or my professional role into disrepute.
- I will support and promote the college's Online Safety policy and help students to be safe and responsible in their use of IT and related technologies.

User Signature

I agree to follow this acceptable use agreement and to support the safe and secure use of IT throughout the college.

Signature …….…… Date ……

Full Name ……..... (printed)

Position/Job title ……..

March 2016

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. external drive, CD) must be checked for any viruses using college provided anti-virus software before using them
- Never interfere with any anti-virus software installed on college ICT equipment that you use
- If your machine is not routinely connected to the college network, you must make provision for regular virus updates through the IT team
- If you suspect there may be a virus on any college ICT equipment, stop using the equipment and contact the ICT support team immediately. The ICT support team will advise you what actions to take and be responsible for advising others that need to know

Data Security

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

The college follows Becta guidelines Becta Schools - Leadership and management - Security - Data handling security guidance for schools (published Spring 2009) and the Local Authority guidance documents listed below

The safe use of new technologies - Ofsted
http://webarchive.nationalarchives.gov.uk/20120408131156/http:/www.ofsted.gov.uk/resources/safe-use-of-new-technologies

Teachers and Governors Guidance
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/562876/Guidance_for_School_Governors_-_Question_list.pdf

Essex Schools Broadband Service - information
https://schools-secure.essex.gov.uk/admin/Broadband/Pages/Broadband.aspx

School Online Safety – Self Review Tool
https://360safe.org.uk/Files/Documents/School-E-SafetyV3

Security

- The college gives relevant staff access to its Information Management 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 college data
- Staff have been issued with the relevant information for ICT Acceptable Use
- Leadership have identified the College Information Manager (CIM)
- Staff should keep all college 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 printer copiers (multi-function print, fax, scan and copiers) are used

Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent using the Safe Haven Fax procedure below:

Safe Haven Fax procedures

When sending personally identifiable information:

- ensure the recipient knows the fax is being sent.
- ensure the fax will be collected at the other end.
- send the front sheet through first.
- check that it has been received by the correct recipient.
- add the rest of the document to the fax.
- press the **redial** button.
- don’t walk away while transmitting.
- wait for the original to process and remove it from the fax machine.
- wait for confirmation of successful transmission.
- confirm whether it is appropriate to fax to another colleague if they are not there to receive it.
- use only the minimum information and anonymise where possible

College Information Manager (CIM)

The CIM is a member of the Senior Leadership Team who is familiar with information risks and the college's response:

- they own the information risk policy and risk assessment
- they act as an advocate for information risk management
- they monitor protection of sensitive data within the college (see below)

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

The CIM at St Benedict's College is the college **Business Manager**.

Protection of Sensitive Data

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. This data will be held in different areas which will need monitoring by the college CIM. These will include all personal data held in the School Information Management System (SIMS) as well as data held on the college network. The college CIM will be responsible for liaising strategic staff 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, student 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 CIM is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

Although the role of CIM has 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 (under the Data Protection Act 1998).

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.legislation.gov.uk/ukpga/1998/29/contents
  Electricity at Work Regulations 1989
  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

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

- The college'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 and/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

e-mail

The use of e-mail within most schools is an essential means of communication for both staff and students. 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 student based, within college or international. We recognise that students need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, students must have experienced sending and receiving e-mails.

Managing e-mail

- The college gives all staff their own e-mail account to use for all college 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 college e-mail account should be the account that is used for all college business

- Under no circumstances should staff contact students, parents or conduct any college business using personal e-mail addresses

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

- Staff sending e-mails to external organisations, parents or students are advised to cc. the Principal or line manager if it is felt appropriate

- Students may only use college approved accounts on the ICT system and only under direct teacher supervision for educational purposes

- E-mails created or received as part of your 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

- The forwarding of chain letters is not permitted in college. Students should inform their teacher of any chain letters causing them anxiety.

- All student e-mail users are expected to adhere to the generally accepted rules of the use of appropriate language and should not reveal any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission

- Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail

- Staff must inform their line manager if they receive an offensive e-mail

- However you access your college e-mail (whether directly, through the Microsoft Exchange portal when away from the office, or on non-college hardware) all the college e-mail policies apply

- The use of internet based webmail service (such as Hotmail, AOL mail etc) for sending, reading or receiving college 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 below.

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

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

- 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

- College e-mail is not to be used for personal advertising

Receiving e-mails

- Check your e-mail 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

- The use of internet based webmail service (such as Hotmail, AOL mail etc) 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 line 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 organisation/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

Equal Opportunities

Students with Additional Needs

The college endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the college's online safety rules.

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

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

Online Safety

Online Safety - Roles and Responsibilities

As online safety is an important aspect of strategic leadership within the college, the Principal and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. **The named Online Safety co-ordinator in this college is the Business Manager** who has been designated this role as a member of the senior leadership team. All members of the college community have been made aware of who holds this post. It is the role of the online 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 Principal/ online safety co-ordinator and all governors have an understanding of the issues and strategies at our college in relation to local and national guidelines and advice.

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

Online Safety in the Curriculum

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

- The college has a framework for teaching internet skills in ICT & PSHE lessons and assemblies
- The college provides opportunities within a range of curriculum areas to teach about online safety
- Educating students on the dangers of technologies that maybe encountered outside college is done informally when opportunities arise and as part of the online safety curriculum
- Students 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
- Students are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. They 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

Online Safety Skills Development for Staff

- Our staff receive regular information on online safety issues as part of child protection training
- New staff receive information on the college'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 online safety and know what to do in the event of misuse of technology by any member of the college community (see flowchart on p 18)
- All staff are required to incorporate online safety activities and awareness within their curriculum areas where appropriate

Managing the college Online Safety messages

- We endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used
- The online safety policy will be introduced to students at the start of year 7
- Online Safety posters will be prominently displayed

Incident Reporting, Online Safety Incident 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 college's CIM or online safety co-ordinator. 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 to your Senior Information Risk Owner. See Page 10.

Online Safety Incident Log

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

St Benedict's College
Online Safety Incident Log

Details of ALL online safety incidents to be recorded by the online safety coordinator. This incident log will be monitored termly by the Principal, Member of SLT or Chair of Governors.

Date & Time	Name of student 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 online safety should be made to the online safety co-ordinator or Principal. Incidents should be logged and the **Essex Flowcharts for Managing an Online 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 online safety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the online safety co-ordinator, depending on the seriousness of the offence; investigation by the Principal/ LA, immediate suspension, possibly

leading to dismissal and involvement of police for very serious offences (see flowchart)

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

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

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 Children's Safeguarding Services on 03330 139797 on 01245 431851 or Essex Police on 0300 333 4444

Has illegal activity taken place?

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 606 1212
- ✓ If it involves a member of staff contact the LADO on 03330 139797

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 Online Safety Co-ordinators in the decision making process related to an online safety incident where no illegal activity has taken place

The Headteacher/Online Safety Co-ordinator should:

- **Record the incident in the online 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

Was the Child the victim or perpetrator?

Pupil as Victim

Support the pupil by one or more of the following:

- Class Teacher
- Online 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

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

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 college maintains students who will have supervised access to Internet resources (where reasonable) through the college's fixed and mobile internet technology
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with students
- If Internet research is set for homework, where specific sites have been suggested, they will 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
- If research tasks, involving the internet, have been set by an exam board as part of controlled assessment, it is not required that teachers check sites that students are using as part of their research
- All users must observe software copyright at all times. It is illegal to copy or distribute college 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
- Do not reveal names of colleagues, parents, students 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 Principal's discretion on what internet activities are permissible for staff and students and how this is disseminated.

Infrastructure

- Essex County Council has a monitoring solution where web-based activity is monitored and recorded

- College internet access is controlled through the LA's web filtering service. For further information relating to filtering please contact Essex County council.

- St Benedict's College 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 students are aware that college based email and internet activity can be monitored and explored further if required

- The college does not allow students access to internet logs

- The college uses management control tools for controlling and monitoring workstations

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

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

- Students 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 college's responsibility to install or maintain virus protection on personal systems. If students wish to bring in work on removable media it must be given to a teacher or technician for a safety check first

- Students and staff are not permitted to download programs or files on college based technologies without prior permission from the ICT team

- If there are any issues related to viruses or anti-virus software, the ICT team 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 students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the college endeavours to deny access to social networking sites to students within college
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Students 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
- Students 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, college details, e-mail address, specific hobbies/ interests)
- Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts online
- Our student are asked to report any incidents of cyber-bullying to the college
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using the LA Learning Platform or other systems approved by the Principal

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting online safety both in and outside of college and also to be aware of their responsibilities. We aim to consult and discuss online safety 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 college
- 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 college website)
- Parents/ carers are expected to sign a Home/School agreement, along with their child, containing the following statement or similar
    - → I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal
- The college disseminates information to parents relating to online safety where appropriate in various forms

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 must 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 eight characters and be difficult to guess
- User ID and passwords for staff and students who have left the college are removed from the system

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

Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students 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 college's Online Safety Policy and Data Security
- Users are provided with an individual network, email, Learning Platform and Information Management System (where appropriate) log-in username. From year 7 they are also expected to use a personal password and keep it private
- Students are not allowed to deliberately access on-line materials or files on the college network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of college 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 college network is 8.00 pm
- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)
- In our college, all ICT password policies are the responsibility of the board of governors and all staff and students are expected to comply with the policies at all times

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any college 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-college environment
- Only download personal data from systems if expressly authorised to do so by your line 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 labelling

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 college 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 college 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-college environment

Social Networking

Social networking applications include but are not limited to:

- blogs i.e. blogger,
- Online discussion forums, for example Facebook;
- Media sharing services for example YouTube, Instagram, Snapchat;
- Professional networking sites, for example Linked In
- 'Micro-blogging' application for example Twitter.

Access to Social Networking Sites

The following permissions are given in respect of social networking applications:

Restricted access for work purposes only, where explicit permission has been given by the Principal

School managed social networking sites

This may include internal forums for staff and outward facing forums for school activities/clubs etc.

It is important to ensure that employees, members of the public and other users of online services know when a social networking application is being used for official school/ purposes. To assist with this, all employees must adhere to the following requirements:

- only use an official (i.e. not personal) email addresses for user accounts which will be used for official purposes;
- appropriate feedback and complaints information must be published in a prominent place which is easily accessible to other users;
- the school's logo and other branding elements should be used where appropriate to indicate the school's support. The school's logo should not be used on social networking applications which are unrelated to or are not representative of the school's official position;
- employees should identify themselves as their official position held within the school on social networking applications. eg through providing additional information on user profiles;
- employees should ensure that any contributions on any social networking application they make are professional and uphold the reputation of the school– the general rules on internet/email apply;
- employees should not spend an unreasonable or disproportionate amount of time during the working day developing, maintaining or using sites;
- employees must not promote or comment on personal, political, religious or other matters;
- employees should be aware that sites will be monitored.

Personal social networking sites

All employees of the school, individuals engaged by the school or individuals acting on behalf of the school from third party organisations should bear in mind that information they share through social networking applications, even if they are on private spaces, may still be the subject of actions for breach of contract, breach of copyright, defamation, breach of data protection, breach of confidentiality, intellectual property rights and other claims for damages. Employees must therefore not publish any content on such sites that is inappropriate or may lead to a claim, including but not limited to material of an illegal, sexual or offensive nature that may bring the school or the local authority into disrepute (see Appendix C for examples of such content).

Employees using social networking sites must also operate at all times in line with the school's Equality and Diversity policy, failure to do so may lead to disciplinary action, up to and including dismissal.

Social networking applications include, but are not limited to, public facing applications such as open discussion forums and internally-facing applications, (i.e. e-folio) regardless of whether they are hosted on school networks or not. The school expects that users of social networking applications will always exercise due consideration for the rights of others and that users will act strictly in accordance with the terms of use set out in this code.

Any communications or content published on a social networking site which is open to public view, may be seen by members of the school community. Employees hold positions of responsibility and are viewed as such in the public domain. Inappropriate usage of social networking sites by employees can have a major impact on the employment relationship. Any posting that causes damage to the school, any of its employees or any third party's reputation may amount to misconduct or gross misconduct which could result in disciplinary action, up to and including dismissal. Employees must not use social networking sites for actions that would put other employees in breach of this policy.

Employees should not use personal sites for any professional activity or in an abusive or malicious manner. The school reserves the right to require the closure of any applications or removal of content published by employees which may adversely affect the reputation of the school or put it at risk of legal action.

Posting inappropriate images

Indecent images of any employee that can be accessed by students, parents or members of the public are totally unacceptable and can lead to child protection issues as well as bringing the school into disrepute.

Posting inappropriate comments

It is totally unacceptable for any employee to discuss pupils, parents, work colleagues or any other member of the school community on any type of social networking site.
Reports about oneself may also impact on the employment relationship for example if an employee is off sick but makes comments on a site to the contrary.

Social interaction with pupils (past and present)

Employees should not engage in conversation with pupils on any personal social networking sites and should be circumspect in personal network contact with former pupils, particularly those under the age of 18 years. This would also apply to individuals who are known to be vulnerable adults. Offers of assistance to a pupil with their studies via any social networking

site are inappropriate and also leaves the employee vulnerable to allegations being made. It would be very rare for employees to need to interact with pupils outside of school in a social setting and by communicating with them on social networking sites, is tantamount to the same. Adults should ensure that personal social networking sites are set at private and that pupils are never listed as approved contacts.

Adults should not use or access social networking sites of pupils.

Making Friends

Employees should be cautious when accepting new people as friends on a social networking site where they are not entirely sure who they are communicating with. Again this may leave employees vulnerable to allegations being made.

Political and financial purposes

Social networking sites must not be used for party political purposes or specific campaigning purposes as the local authority is not permitted to publish any material which 'in whole or part appears to affect public support for a political party' (LGA 1986).
Social networking sites must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns.

Reporting breaches of this code

Anyone who becomes aware of inappropriate postings on social networking sites must report it to their line manager straight away. The line manager will then follow the disciplinary procedure where appropriate. If an employee fails to disclose an incident or type of conduct relating to social networking sites, knowing that it is inappropriate and falls within the remit of this code of conduct, then that employee may be subject to disciplinary action up to and including dismissal.

Should an employee become aware of an underage person using social networking sites, (Facebook and Bebo have set it at 13 years and MySpace have set it at 14 years), then they should report this to the site operator and if that child is at their particular school, then this should also be reported to their line manager.

Cyber bullying

The school will not tolerate any form of cyber bullying by employees. Any such behaviour will result in disciplinary action, up to and including dismissal. Cyber bullying may include but is not limited to:

- Offensive emails including joke emails which may offend other employees
- Email threats
- Leaving offensive or inappropriate comments on blogs or networking sites
- Offensive comments sent by text, email or posted on social networking sites
- Sharing another person's details/personal information online without appropriate consent
- Employees who feel they are the subject of cyber bullying must notify their line manager at the earliest opportunity.

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 college community or public, without first seeking consent and considering the appropriateness. NSPCC guidance can be found at:

https://www.nspcc.org.uk/preventing-abuse/safeguarding/photography-sharing-images-guidance/

With the written consent of parents (on behalf of students) and staff, the college permits the appropriate taking of images by staff and students with college equipment

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips
- Students 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.

Publishing Student's Images and Work

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

- on the college web site
- on the college's Learning Platform
- in the college prospectus and other printed publications that the college may produce for promotional purposes
- in display material that may be used in the college's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the college
- 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 college 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 all adults with parental responsibility in order for it to be deemed valid.

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

Further information relating to issues associated with School websites and the safe https://schools-secure.essex.gov.uk/Pages/EssexSchoolsInfolink.aspx

Storage of Images

- Images/ films of children are stored on the college's network
- Students and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Principal
- Rights of access to this material are restricted to the teaching staff and students within the confines of the college network/ Learning Platform
- ***The ICT team*** has the responsibility of deleting the images when they are no longer required, or the student has left the college

Webcams, Visualisers and CCTV

- The college uses CCTV for security and safety. The only people with access to this are the college Business Manager and Safeguarding team**.** Notification of CCTV use is displayed at the front of the college. Please refer to the hyperlink below for further guidance
  https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/
- We do not use publicly accessible webcams in college
- Webcams and visualisers in college are only ever used for specific learning purposes, i.e. monitoring experiments
- Misuse of the webcam or visualiser by any member of the college community will result in sanctions

For further information relating to webcams
http://www.actnow.org.uk/media/articles/Guidance_Note_on_use_of_images.pdf

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 college
- All students are supervised by a member of staff when video conferencing
- All students are supervised by a member of staff when video conferencing with end-points beyond the college
- The college keeps a record of video conferences, including date, time and participants.
- Approval from the Principal is sought prior to all video conferences within college
- The college 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

For further information relating to Video Conferencing
http://schools.becta.org.uk/index.php?section=re&&catcode=&rid=188

College ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

College ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the college's ICT equipment provided to you
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the college's inventory
- Do not allow your visitors to plug their ICT hardware into the college network points (unless special provision has been made or they are ECC based visitors). 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 college's network drive. You are responsible for the backup and restoration of any of your data that is not held on the college'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 college 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 college systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all college data is stored on college'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 college 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 college 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 college is allowed. Our college chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

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

- Students are allowed to bring personal mobile devices/phones to college 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 Principal. The device user, in this instance, must always ask the prior permission of the bill payer

- The college 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 college community is not allowed

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

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

College Provided Mobile Devices (including phones)

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

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

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

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

Removable Media

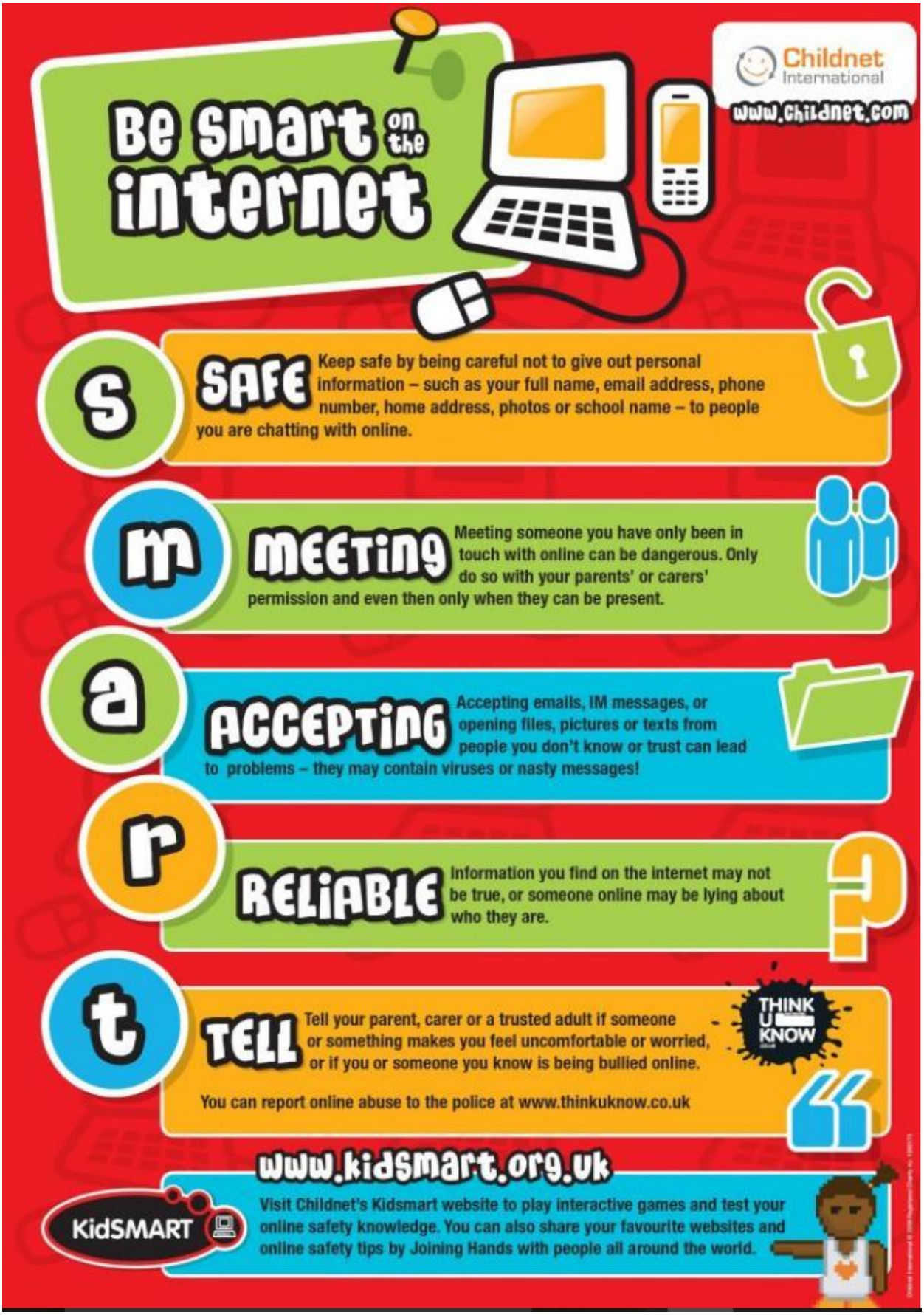
If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section 'Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media' - page 23

- 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
- 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

Be SMART on the Internet Poster



Systems and Access

- You are responsible for all activity on college systems carried out under any access/account rights assigned to you, whether accessed via college ICT equipment or your own PC
- Do not allow any unauthorised person to use college 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 college ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the college or may bring the college 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 college'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 college systems, hardware or used in relation to college 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 college policies.

- College telephones are provided specifically for college 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. In the first instance, contact the college business manager immediately and provide details of the call.

Writing and Reviewing this Policy

Staff involvement in policy creation

- Staff have been involved in making/ reviewing the Policy for ICT Acceptable Use

Review Procedure

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

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

This policy will be reviewed every twelve months and consideration given to the implications for future whole college 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 Principal, staff and governors on the **19th June 2013.**

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.legislation.gov.uk/ukpga/1998/29/contents

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.legislation.gov.uk/uksi/2000/2699/regulation/3/made

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.legislation.gov.uk/ukpga/2000/23/contents

Human Rights Act 1998

http://www.legislation.gov.uk/ukpga/1998/42/contents

Other Acts Relating to Online Safety

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.

www.legislation.gov.uk/ukpga/2006/1/pdfs/ukpga_20060001_en.pdf

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.

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 committed 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.legislation.gov.uk/ukpga/1998/29/contents

The Freedom of Information Act 2000

http://www.legislation.gov.uk/ukpga/2000/36/contents