



# The Chauncy School eSafety Policy 2010 - 2011

# Contents

Introduction	3
eSafety - Roles and Responsibilities	4
Monitoring	4
Breaches	5
Incident Reporting	5
eSafety in the Curriculum	5
Passwords and Password Security	6
Managing Internet Access	6
Managing Other Web 2 Technologies	8
Access and Use of School ICT Systems - Guidance for Staff	8
Use of E-Mail	11
Safe Use of Images	13
Equal Opportunities	14
Parental Involvement	14
Acceptable Use Agreement: Staff, Governors and Visitors	16
Acceptable Use Agreement for Students	17
SMILE and Stay Safe Poster	19
Writing and Reviewing this policy	20
Current Legislation	21

## Introduction

ICT in the 21<sup>st</sup> Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. 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

This is not a definitive list as new forms of hardware and software emerge at an increasing rate.

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 Chauncy, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

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. It is of paramount importance that personal data is kept secure at all times to protect the students, staff and the wider school community.

The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Author: S Walton

Next review March 2012

## eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named eSafety co-ordinator in this school is Steve Walton - Deputy Headteacher who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Herts LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

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

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

Everybody in the 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.

### Monitoring

At the request of the Headteacher, authorised staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. At Chauncy the list of ICT authorised staff would include:

- The Headteacher
- Network Manager
- The Deputy Headteachers
- Assistant Headteachers
- ICT Staff

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 School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the

Author: S Walton

Next review March 2012

Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All internet activity is logged by the school's internet provider. These logs are monitored by authorised Chauncy staff.

### Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure. 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 school's Network Manager.

Additionally, all security breaches, lost / stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Senior e-Safety Coordinator.

### eSafety in the Curriculum

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

- The school has a framework for teaching internet skills in ICT lessons.
- The school provides opportunities within a range of curriculum areas to teach about eSafety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Pupils are aware of 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 made aware of the formal electronic communication routes with members of staff who are employed by the school, according to safeguarding guidance.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling 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 .

## Passwords and Password Security

### Using 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 should contain a minimum of six characters and be difficult to guess.
- User ID and passwords for staff and pupils who have left the School are removed from the system.
- Portable storage media such as memory pens, hard disk drives and DVD \ CD-R should be password protected where possible, especially if they contain sensitive school data.
- If you think your password may have been compromised or someone else has become aware of your password report this to the Network Manager.

### Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are 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 school's e-safety Policy and Data Security.
- Users are provided with an individual network, email, Learning Platform and SIMS log-in username.
- From Year 7 students are expected to use personal passwords to access the school network and the e-mail facilities and to keep them private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, SIMS and 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 school network is 5 minutes.

### Managing 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 Chauncy School's network

Author: S Walton

Next review March 2012

and Internet access 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 school maintains students who 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 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 Headteacher's discretion on what internet activities are permissible for staff and pupils and how this is disseminated. Discussion about what is and is not acceptable use will be communicated through whole staff training, new staff induction, ICT Departmental meetings, ICT Steering group meetings, assemblies and ICT lessons.

### Infrastructure

- The Chauncy School has a monitoring solution where web-based activity is monitored and recorded.
- School internet access is controlled through the LA's web filtering service. For further information relating to filtering please go to <http://www.thegrid.org.uk/eservices/safety/filtered.shtml>
- Our school also employs some additional web filtering which is the responsibility of the Network Manager.
- The Chauncy School 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 school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The 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 school, by delegation to the network manager, to

ensure that Anti-virus protection is installed and kept up-to-date on all school machines.

- 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 school's responsibility nor the network manager's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must not contain viruses or software that may harm the individual computer system or the school network
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from class teacher or the Network Manager
- If there are any issues related to viruses or anti-virus software, the network manager should be informed by means of a Network Report Sheet

### 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 school endeavours to deny access to social networking sites to pupils within 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, school details, IM/ email address, specific hobbies/ interests).
- Our pupils and staff are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils and staff are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils and staff are asked to report any incidents of bullying to the school eSafety Coordinator.
- Staff must not link with or communicate with current students via personal social networking sites.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils with prior approval of the Headteacher.
- Staff must comply with the Staff, Governor and Visitor Acceptable Use Agreement & Code of Conduct.

### Access and Use of School ICT Systems - Guidance for Staff

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

Author: S Walton

Next review March 2012

equipment or your own PC.

- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you.
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time.
- Do not introduce or propagate viruses.
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act, the Age Discrimination Act and the Disability Discrimination Act).
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act.
- 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 way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Inform the Network Manager if you have any concerns about personal or confidential data held on school hardware.

## School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

### 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 School systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

### Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

### Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device. Under certain circumstances, the Headteacher will give discretion to staff to contact students, parent or carers via their own personal mobile device.
- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched off or onto silent.
- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Staff may confiscate any device that impedes teaching and learning or the good order and discipline of the school. Please refer to the Behaviour Policy.

### Use of School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages or e-mails between any member of the 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 school community
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school
- You are responsible for the security of a school mobile phone or laptop.

- Do not leave equipment unattended and on display (especially in vehicles)
- Report the loss or theft of any school equipment immediately
- The school remains responsible for all call costs until a school mobile phone is reported lost or stolen
- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so.

## Use of E-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving e-mails.

## Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses without permission from the Headteacher.
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. to their line manager or the Headteacher.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of your employment 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
- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the eSafety co-ordinator 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 school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.
- The use of Hotmail, Yahoo, Google, 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 school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- School 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; 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

### 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 where 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 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 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)
  - 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:

- Hertfordshire Constabulary
- Hertfordshire Partnership Trust

## 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 school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupil's device

### Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the 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 school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school 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 Website Management Staff have authority to upload to the site.

## Storage of Images

- Images/ films of children are stored on the school's network and *in*
- 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 Headteacher
- Rights of access to this material are restricted to school staff and pupils within the confines of the school network/ Learning Platform / website

## Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the Headteacher, the senior team, site management and the network manager. Notification of CCTV use is displayed at the front of the school
- We do not use publicly accessible webcams in school
- Webcams in school are only ever used for specific learning purposes
- Misuse of the webcam by any member of the school community will result in school sanctions.

## Equal Opportunities

### Pupils with Additional Needs

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

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

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

### Parental Involvement

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

We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents & carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy by reviewing draft documents and policies which are available on the school website prior to review.
- Parents & carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website).
- Parents/ carers are expected to sign a Home School agreement containing the following statement or similar

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

- The school disseminates information to parents relating to eSafety where appropriate in the form of;
  - Information and celebration evenings
  - Posters
  - Website/ Learning Platform postings
  - Newsletter items

## Acceptable Use Agreement: Staff, Governors and Visitors

### Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr Steve Walton Deputy Headteacher and eSafety coordinator or Headteacher Mr Dennis O'Sullivan.

- 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 or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of Mr Nick Goodwin, the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and / or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent / carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress will not bring my professional role in the school into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

#### User Signature

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

Author: S Walton

Next review March 2012

Signature: ..... Date: .....

Full Name: ..... Job title .....

## Acceptable Use Agreement for Students

### Secondary Student Acceptable Use - Agreement / eSafety Rules

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network/ Learning Platform with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address.
- I will make sure that all ICT communications with pupils, teachers or others is 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 school project approved by my teacher.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of The Chauncy School.
- I will ensure that 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 will respect the privacy and ownership of others' work on-line 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 and parents.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent / carer may be contacted.



Date

Dear Parent/ Carer

ICT including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of eSafety 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 S Walton, (Deputy Headteacher and eSafety Coordinator).

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

Yours sincerely,

Mr S Walton  
(Deputy Headteacher)

✂

**Pupil and Parent/ carer signature**

We have discussed this document and .....(pupil name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at The Chauncy School.

Parent/ Carer Signature .....

Pupil Signature.....

Form ..... Date .....



Headteacher: Dennis O'Sullivan BSc MA  
The Chauncy School Park Road Ware Hertfordshire SG12 0DP Tel: 01920 411200 Fax: 01920 411201  
e-mail: [admin@chauncy.herts.sch.uk](mailto:admin@chauncy.herts.sch.uk) web site: [www.chauncy.herts.sch.uk](http://www.chauncy.herts.sch.uk)

## SMILE and Stay Safe Poster eSafety guidelines to be displayed throughout the school



**S**taying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location) .

**M**eeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

**I**nformation online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend' .

**L**et a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

**E**mails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

## 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 senior team meetings, staff meetings, student council meetings and parental consultation of draft version of this document.

### Review Procedure

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

..... Date

..... Signature of Chair of Governors

..... Signature of Headteacher

## Current Legislation

### Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

<http://www.hmso.gov.uk/acts/acts1998/19980029.htm>

### The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

<http://www.hmso.gov.uk/si/si2000/20002699.htm>

### Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

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

### Human Rights Act 1998

<http://www.hmso.gov.uk/acts/acts1998/19980042.htm>

### Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

### Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs. For more information [www.teachernet.gov.uk](http://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

Author: S Walton

Next review March 2012

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 their 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.

Author: S Walton

Next review March 2012

Data Protection Act 1998

[http://www.opsi.gov.uk/acts/acts1998/ukpga\\_19980029\\_en\\_1](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](http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx)