Hampden House

Online Safety, Data Protection and Acceptable Use of ICT Policy

---

Adopted by the Management Committee meeting on: 14 June 2018

Signed: Date:

Chair of Management Committee

Review date: June 2019

Member of staff responsible for review: Head of Care

Introduction

ICT in the 21st 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

Apps

E-mail, Instant Messaging and chat rooms

Social Media, including Facebook and Twitter

Mobile/ Smart phones with text, video and/ or web functionality

Other mobile devices including tablets and gaming devices

Online Games

Learning Platforms and Virtual Learning Environments

Blogs and Wikis

Podcasting

Video sharing

Downloading

On demand TV and video, movies and radio / Smart TVs

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 and that some have minimum age requirements (13 years in most cases).

At Hampden House**,** we understand the responsibility to educate our students on e-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Hampden House holds personal data on learners, staff and others 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 school.

Everybody at Hampden House 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, regular visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, digital video equipment, etc…); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Monitoring

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

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, video 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.

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 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.

Students will have their telephones taken from them on arrival and placed in their lockers whilst at Hampden House, they will be returned when they go home. Other mobile devices such as tablets will be monitored and held by staff, and possibly confiscated should they have inappropriate content on them.

Breaches

A breach or suspected breach of policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. Students may have their device(s) confiscated and sent home.

For staff 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.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

For Students, please see the Discipline and Behaviour Policy.

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 Hampden House's E Safety Lead – Sarah Chesterton.

Additionally, all security breaches, lost/stolen equipment or data (including identity badges, passwords and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person.

The relevant responsible individuals in the school are as follows:

Sarah Chesterton (Head of Care), Jane Hartley (Health and Social Inclusion Manager).

Please refer to the relevant section on Incident Reporting, e-Safety Incident Log & Infringements.

Hampden House Acceptable Use Agreement: Students (under 12 year olds)

I will only use ICT in school for school purposes

I will only use my class e-mail address or my own school e-mail address when e-mailing

I will only open e-mail attachments from people I know, or who my teacher has approved

I will not tell other people my ICT passwords

I will only open/delete my own files

I will make sure that all ICT contact with other children and adults is responsible, polite and sensible

I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately

I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image or anyone else's, unless this is part of a school project approved by my teacher and a responsible adult comes with me

I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe

I will support Hampden House's approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community

I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety

I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher

I will not bring a Smart Watch to school because I am not allowed to wear one during the school day

I understand that I am not allowed to use my mobile phone in School and must hand it in on arrival.

I understand that I can only use my tablet/devise at agreed times on condition that a member of staff can check it for inappropriate content and delete this content as necessary. I also understand that inappropriate use may mean that my devise is confiscated and/or reported to the Police.

I will not sign up to online services until I am old enough

Signed……. Date……

Suffolk County Council

Hampden House PRU
Cats Lane Great Cornard Sudbury Suffolk CO10 2SF
Telephone: (01787) 373583 e-mail: admin@hampdenhouse.net

Headteacher: Mr G P Alcock

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact me on the above numbers.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

Yours faithfully,

Sarah Chesterton
Head of Care

Parent/ carer signature

We have discussed this document with ……………………….............(child's name) and we agree to follow the e Safety rules and to support the safe use of ICT at Hampden House Pru.

Parent/ Carer Signature …….………………….………………………….

Name: ……………………………………………………………………..

Date ………………………………

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes
- I will not download or install software on school technologies
- I will only log on to the school network, other systems and resources with my own user name and password
- I will follow the school's 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 students, 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 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
- I am aware that when I take images of students and/ or staff, that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- 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
- 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
- I will not bring a Smart Watch to school because I am not permitted to wear one during the school day
- I will not sign up to online services until I am old enough to do so

- I understand that I am not allowed to use my mobile phone in School and must hand it in on arrival.
- I understand that I can only use my tablet/devise at agreed times on condition that a

member of staff can check it for inappropriate content and delete this content as necessary. I also understand that inappropriate use may mean that my devise is confiscated and/or reported to the Police.

Signed…… Date:…….

Suffolk County Council

Hampden House PRU
Cats Lane Great Cornard Sudbury Suffolk CO10 2SF
Telephone: (01787) 373583 **e-mail: admin@hampdenhouse.net**

Headteacher: Mr G P Alcock

Dear Parent/ Carer

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

Students are expected to read and discuss this agreement with their parent/ carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with Sarah Chesterton, Head of Care.

Please return the bottom section of this form which will be kept on record at the school

✂----------

Parent/ carer signature

We have discussed this document with……(child's name) and we agree to follow the e-Safety rules and to support the safe use of ICT at Hampden House.

Parent/ Carer Signature …….

Parent/Carer Name……

Student Signature……..

Date ……

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 Graham Alcock or Jane Sharp

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable 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 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, personal Twitter account, or any other social media link, to students
- 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 MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, eg on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the Head teacher.
- 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 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 will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- 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 bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help students 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

Signature …… Date ……

Full Name ……(printed)

Job title ……

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

- Never interfere with any anti-virus software installed on school ICT equipment.

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

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

Data Security

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

The Local Authority guidance documents listed below

HGfL: School Admin: School Office: Data Protection and Freedom of Information

- Headteacher's Guidance – Data Security in Schools – Dos and Don'ts
- Network Manager/MIS Administrator or Manager Guidance – Data Security in Schools
- Staff Guidance – Data Security in Schools – Dos and Don'ts
- Data Security in Schools - Dos and Don'ts

Security

- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff have read the relevant guidance documents available on the SITSS website concerning 'Safe Handling of Data' (available on the grid at - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata)
- Leadership have identified relevant responsible persons as defined in the guidance documents on the SITSS website (available - http://www.thegrid.org.uk/info/traded/sitss/)
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal,

sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used

- Anyone sending a confidential or sensitive fax should notify the recipient before it is sent

Protective Marking of Official Information

Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them, in line with local business processes.

- There is no requirement to mark routine OFFICIAL information.
- Optional descriptors can be used to distinguish specific type of information.
- Use of descriptors is at an organisation's discretion.
- Existing information does not need to be remarked.

In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE'**

Information Asset Owner (IAO)

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

A responsible member of staff should be able to identify across the school:

what information is held, and for what purposes

what information needs to be protected, how information will be amended or added to over time

who has access to the data and why

how information is retained and disposed of

As a result this manager is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

At Hampden House this Manager is Carol Hibberd.

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

Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed of through an authorised agency. 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
https://ico.org.uk/for-organisations/education/
Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

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

The school's disposal record will include:

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

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

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

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

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

The Waste Electrical and Electronic Equipment Regulations 2006

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

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

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

Information Commissioner website

https://ico.org.uk/

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

https://ico.org.uk/for-organisations/education/

PC Disposal – SITSS Information

http://www.thegrid.org.uk/info/traded/sitss/services/computer_management/pc_disposal

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 school or international. We recognise that students need to understand how to style an e-mail in relation to their age and how to behave responsible online.

Managing e-mail

- Hampden House gives all staff & Managers/governors their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

- Staff & governors should use their school email for all professional communication.

- 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 students, parents or conduct any school 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 school headed paper

- Staff sending e-mails to external organisations, parents or students are advised to cc. the Headteacher, line manager or designated line manager

- Students 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 school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
  - Save files and folders to the Microsoft 365 cloud.

- All student e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour 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

- Students must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail
- Staff must inform (the e-Safety co-ordinator or line manager) if they receive an offensive e-mail
- Students are introduced to e-mail as part of the Computing Programme of Study
- 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

---

Sending e-mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, please use encryption
- 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
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising

Receiving e-mails

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; consult your network manager first
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed

e-mailing Personal, Sensitive, Confidential or Classified Information

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

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

  - Encrypt and password protect. See http://www.thegrid.org.uk/info/dataprotection/#securedata
  - 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 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

Equal Opportunities

Students with Additional Needs

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

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

Where a student 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.

eSafety

eSafety - Roles and Responsibilities

As e-Safety 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 Sarah Chesterton 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 CEOP (Child Exploitation and Online Protection) and Childnet and Suffolk Safeguarding Portal.

Senior Management and governors are updated by the eSafety Lead and all Managers/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 students, 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/student discipline (including the anti-bullying) policy and PSHCE.

e-Safety 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 students 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 lessons

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

Educating students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety 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, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate 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. Students 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 Cybermentors, Childline or CEOP report abuse button

Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the computing lessons and in care time for the boarders.

eSafety Skills Development for Staff

Our staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages in the form of updates at staff meetings.

New staff receive information on the school's acceptable use policy as part of their induction

All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see eSafety Co-ordinator)

All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the School eSafety Messages

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

The e Safety policy will be introduced to the students at the start of each school year

E Safety posters will be prominently displayed

The key e Safety advice will be promoted widely through school displays, newsletters, class activities and so on

We will participate in Safer Internet Day every February.

Incident Reporting, eSafety 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 school's relevant responsible person or eSafety 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 Information Asset Owner. See Page 15.

eSafety Incident Log

Keeping an incident log can be a good way of monitoring what is happening and identify trends or specific concerns.

'School name' **eSafety Incident Log**

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying may also need to be recorded elsewhere

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

This can be downloaded http://www.thegrid.org.uk/eservices/safety/incident.shtml

Misuse and Infringements

Complaints
Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher.

Incidents should be logged and the **Suffolk Flowcharts for Managing an eSafety Incident** should be followed.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher and or MASH may occur. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)

- Users are made aware of sanctions relating to the misuse or misconduct by discussion in supervision; signing the AU agreement and by reading the Code of Conduct.