NORTH NORFOLK ACADEMY TRUST

E-Safety and Data Policy

Review frequency: Every three years
Last reviewed: March 2015

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
- 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 with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

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, usually 13 years.

At our school we understand the responsibility to educate our students 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. 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.

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.

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 school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, 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).

eSafety

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. Each school will have an eSafety co-ordinator. 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.

Senior Management and governors are updated by the Headteacher/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 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 PSHE

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the 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 ICT 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 ICT curriculum in Year 8.

eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online message
- 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 enclosed flowcharts)
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- The eSafety policy will be introduced to the students at the start of each school year
- eSafety posters will be prominently displayed
- The key eSafety advice will be promoted widely through school displays, newsletters, class activities and so on

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 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 of new technologies, together with the associated risks

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and 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 text, image, sound or videos 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
  - Practical training sessions e.g. How to adjust the Facebook privacy settings
  - Posters
  - School website
  - Newsletter items

Monitoring

All internet activity is logged by the school's internet provider. These logs may be monitored by authorized s c h o o l staff.

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.

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 ICO's new 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

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 eSafety Co-ordinator. Additionally, all security breaches, lost/stolen

equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the ICT Co-ordinator.

Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements.

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 that you use
- 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

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 keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- 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 copiers (multi-function print, fax, scan and copiers) are used

Anyone expecting a confidential or sensitive fax should notify the sender before it is sent.

Equal Opportunities

Students with Additional Needs

The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the schools' eSafety 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 eSafety issues.

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

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 SIRO 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 a member of

the Leadership Team.

eSafety Incident Log

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

E-Safety 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 the LT or Chair of Governors. Any incidents involving Cyberbullying may also need to be recorded elsewhere.

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 eSafety should be made to the eSafety co-ordinator or Headteacher.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct via the Staff handbook

Internet Access

The internet is an open worldwide communication medium, available to everyone, 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. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The school provides students with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with students
- 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 the intended restricted audience
- Do not reveal names of colleagues, students, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion as to what internet activities are permissible for staff and students and how this is disseminated.

Infrastucture

- School internet access is currently controlled through a web filtering service.
- Our school also employs some additional web-filtering which is the responsibility of the ICT Technician
- Our 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 students are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow students access to internet logs
- The school 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 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
- 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 school's responsibility nor the network manager's to install or maintain virus protection on personal systems. If students wish to bring in work on removable media it must be given to the ICT Technician for a safety check first
- If there are any issues related to viruses or anti-virus software, the network manager should be informed.

Smile and Stay Safe Poster

eSafetyguidelinestobedisplayedthroughouttheschool

SMILE **and stay safe**

Staying 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)

Meeting 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

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

Let 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

Emails, 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

.