E-Safety Suite of Policies

E-Safety & Data Security Policy

ICT is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we build in the use of these technologies in order to support 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. We also 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 or network 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 for example with Facebook.

Northgate High School takes its responsibility seriously to educate 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.

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 financial penalties, media coverage, and potentially damage the reputation of the school. This can make it more difficult for 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).

This policy is focussed on protecting the interests and safety of the whole school community. It is linked to the following school policies: child protection, health and safety, home–school agreements, B4L (Behaviour for Learning - including the anti-bullying policy) and aspects of our Citizenship and PART lesson programmes.

E-Safety in the Curriculum

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

- The school has a framework for teaching internet skills in computing lessons.
- The school provides opportunities within a range of curriculum areas to teach about e-safety
- Educating students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-safety curriculum
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling 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 Childline or CEOP(Think U Know) report abuse button. The Anti- Bullying Ambassadors have led assemblies and activities on this topic, alongside our Safer Schools Partnership PCSO, and the Rose Project, a charity supporting e-safety for pupils and parents
- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum

E-Safety Skills Development for Staff

- Our staff receive regular information and training on e-safety 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 e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

Managing the School E-Safety Messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the students at the start of each school year in their first Computing department lesson

- 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

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-safety both in and outside of school and to be aware of their responsibilities. We seek to consult and discuss e-safety 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 with their child on admission to the school from 2016 on adoption of new policy.
- 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
- Parents 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 e-safety where appropriate in the form of;
- Information and celebration evenings
- Practical training sessions e.g. How to adjust the Facebook privacy settings
- Posters
- Policies present on the school website
- Newsletter items

Monitoring

All internet activity is logged by the school’s internet provider (currently Norfolk County Council). These logs may be monitored by authorised Northgate High School staff.
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 Headteacher. Additionally, all security breaches, lost/stolen equipment or data (including remote access), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Headteacher.

Data Security

- The school gives relevant staff access to its Management Information System (Facility/E-Portal) 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' 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.
Staff should discuss any pupils whom they are concerned regarding their e-safety with relevant Head of Year and/or Head of Learning Support.

Incident Reporting, E-Safety Incident Log & Infringements

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher and an e-safety Incident Log of the issue completed.

Approved by Strategic Governing Body:______________Signed:__________________ (Chair of Governors)