Northgate High School
Suite of E-Safety Policies
Key Principles 2016/17

Northgate High School's e-Safety Policy is part of our Safeguarding and Child Protection Policy, and relates to other policies including those for ICT (The Acceptable Use Policy (AUP, Appendix 1), Anti-bullying Policy.

- The school have identified staff who have an overview of e-safety comprising the Senior Designated Professional (SDP) team Senior School ICT Service Manager and the Head of Computing

- Our e-Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.

- The e-safety Policy and its implementation will be reviewed annually

- This e-safety Policy: A. Mason, Deputy Head

Teaching and learning

Why Internet and digital communications are important in a 21st Century School

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- Internet use is a part of the curriculum and a necessary tool for staff and pupils.

- At Northgate High School, our aim is for pupils to enjoy learning, achieve highly and enter the adult world with confidence, fulfilling their potential and inspiring excellence. Our ICT provision has developed significantly over the last three years with WiFi installed across the site to support iPad technology alongside netbooks and four suites of PC. In addition, all teaching staff have laptops provided in order that technology is used to enhance learning opportunities for our students.

- Northgate High School recently converted as a single converter academy, however the school Broadband/Internet access currently continues to be provided by Norfolk County Council and includes filtering appropriate to the age of pupils.

- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use (including our Acceptable Use Policy, Appendix One)

- Pupils are educated in the effective use of the Internet as a starting module and focus at the start of all KS3 Computing lessons each year. In 2013/14, pupils received CEOP (Child Exploitation Online Protection) delivered by our Safer Schools Partnership PCSO through Citizenship lessons, which will be delivered again in 2014/15 by our link PCSO. In Summer 2014, the school benefitted from cyberbullying/e-safety sessions led by The Rose Project, a charity based in Norwich working with the MASH. This included a Parents' Information evening entitled 'Help my Child is on Facebook'. Visits by music artists over the last 3 years (Vanquish, Antix and J-SOL and Hussain) are welcomed by the school in engaging students with e-safety messages.

- Pupils are shown how to publish and present information appropriately to a wider audience as part of their Computing studies.

Pupils will be taught how to evaluate Internet content

- The school seeks to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law (See Copyright Regulations held by our Website Co-ordinator and Information Manager)

- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Pupils are taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon on the 'Think you Know' website.

Managing Internet Access

Information system security

- School ICT systems security is reviewed regularly, and as part of our ICT Operations and ICT Strategy Group enlisting the support of Norfolk County Council Advisors and as a Secondary Pilot study on Data Protection completed by Norfolk County Council in Spring 2014.

- Virus protection is updated regularly by the ICT Support Team

- Security strategies are discussed with our Broadband provider who provide our internet and filtering systems.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system. Currently this is Office 365 for teaching and associate staff, and generic @norfolk.sch.uk accounts for senior leaders and some administration staff.

- Pupils must immediately tell a teacher if they receive offensive e-mail

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored. Staff are aware through the DfE Safer Working Practice Document – Keeping Children Safe, and Teacher Standards that the safeguarding of children is paramount and social media links between staff and pupils is unacceptable.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Published content and the school web site

- The contact details on the Web site are the school address, e-mail and telephone number. Staff or pupils personal information are not published.

- Our Communications Manager will take overall editorial responsibility and ensure that content is accurate and appropriate with the oversight and support from Assistant Headteacher (Ethos)

Publishing photographs, images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children. Image consent is always sought and adhered to prior to the publication of any photographs in internal publications, or the wider press.

- Pupils' full names will be avoided on the Web site or VLE, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.

- Written permission from parents or carers (Image Consent forms issued at the start of each academic year) will be obtained before photographs or images of pupils are published

- Written permission from adults will be obtained before their names, photographs or images of themselves are published

- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories through the Image Consent Form.

Social networking and personal publishing on the school learning platform

- The school prohibits/filters out access to social networking sites through the school network/WiFi, and educates pupils in their safe use of passwords.

- All users are advised never to give out personal details of any kind which may identify them, anybody else or their location.

- Pupils must not place personal photos on any social network space provided in the school learning platform without permission.

- Pupils, parents and staff will be advised on the safe use of social network spaces

- All pupils are responsible for their behaviour, both in and outside the school, including the internet. All pupils must conduct themselves in a respectable manner on any social media accounts

- Pupils will be advised to use nicknames and avatars when using social networking sites are discussed as part of our CEOP or core Computing delivery in Years 7,8, and 9

- Any members of staff with a Northgate affiliated social media account (e.g. a Twitter or Facebook page) must provide the Communications Manager with the login details for the account. This account belongs to the school, therefore any posted content must be in line with the school's safeguarding procedures and practices. You must meet with the Communications Manager in the first instance/setting up of the page to ensure that the

'About' content is consistent with the school's brand and its assets. The account password must be changed every three months – you must keep the Communications Manager updated of any password changes

- Any negative (or where relevant, positive) comments/feedback seen by any member of staff on social media accounts must be reported to the Business or Communications Manager to ensure that any discussions surrounding the school within the local community can be monitored and managed by the relevant individuals.

Managing filtering

- The school currently works in partnership with Norfolk Children's Services to ensure systems to protect pupils are reviewed and improved linked to filtering. As an Academy, as contracts are revised, filtering responsibility may be subject to change and this policy will be update accordingly.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the nominated member of staff (the Senior Schools ICT Service Manager who reports the concern directly to the Headteacher).

- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Video-conferencing

- Video-conferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.

- Currently, pupils are unable to make or answer a video conference call by our filtering system.

- Video-conferencing will be appropriately supervised for staff meetings where it is an appropriate tool for communication.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. This included discussions in 2013/14 with Norfolk County Council on possible plans for a Bring Your Own Device (BYOD) system and policy (technology not yet implemented).

Other devices

- **Mobile phones and associated cameras will <u>not</u> be used during lessons or formal school time except as part of an educational activity.**

- The sending of abusive, offensive or inappropriate material is forbidden and pupils receive education from CEOP Materials delivered by our Safer Schools' partnership PCSO in class sessions and assemblies. The PCSO also provides advice and guidance to students who may be subject to receipt or sending of abusive information through technology in line with changes to the law around digital communications and social media.

- Staff should not share personal telephone numbers with pupils and parents. (School mobile phones are provided for staff where contact with pupils is required on school visits through our Educational Visits Co-ordinator (EVC)).

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. (See our related Data Protection Policy)

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff AUP/Code of Conduct for ICT' before using any school ICT resource.

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

- Parents will be asked to sign the Home School Agreement, and pupils must agree to the Acceptable Use Policy for the use of the VLE and school provided ICT equipment.

- **Pupils must agree to comply with the Acceptable Use statement before being granted computer access. This is revoked if students break the agreement, parents are informed and restricted ICT access for students is implemented for an agreed period of time.**

- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' form before being allowed to access the Internet on the school site, for example Adult Education provision.

Assessing risks

- The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Norfolk Children's Services can accept liability for the material accessed, or any consequences of Internet access.

- The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the Headteacher immediately.

- Complaints of a child protection nature must be referred to the Designated Safeguarding Leads (DSLs) for Safeguarding and dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of the complaints procedure.

- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school Online-safety policy.

Communications Policy

Introducing the Online-safety policy to pupils

- Appropriate elements of the E-safety policy will be shared with pupils.

- E-safety rules will be posted in all networked rooms.

- Pupils will be informed that network and Internet use will be monitored.

- Curriculum opportunities to gain awareness of online-safety issues and how best to deal with them will be provided for pupils.

Staff and the E-safety policy

- All staff will be given the School E-safety Policy and its importance explained.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential and expected through our Safeguarding and Child Protection Policy and practice.

- Staff who manage filtering systems or monitor ICT use (Senior Schools ICT Service Manager) will be supervised by senior management (Assistant Head Ethos) and have clear procedures for reporting issues**.**

Enlisting parents' support

- Parents' and carers attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.

- Parents and carers will from time to time be provided with additional information on E-safety.

- The school will ask all new parents to sign the Home School agreement when they register their child with the school.

Approved by Strategic Governing Body:_____

Signed:_____ (Chair of Governors)