BAMBURGH SCHOOL

E-Safety / Acceptable Use Policy

Content

November 2017

1. Context
   - 1.1. Development of this Policy
   - 1.2. Aims
   - 1.3. Teaching and Learning
2. Managing the School Network and Internet access
   - 2.1. Information Systems Security and Monitoring
   - 2.2. Communication Systems
   - 2.3. Copyright and Plagiarism
   - 2.4. Protecting Personal Data
   - 2.5. Managing Emerging Technologies
3. Mobile Devices
   - 3.1. Taking digitaì Images using Cameras and Video
   - 3.2. Mobiìe Phones
   - 3.3. Laptops
   - 3.4. Portable Storage Devices
   - 3.5. Games Machines
   - 3.6. Video/DVD
4. Assessing Risks and Handiing e-Safety issues
   - 4.1. Assessing Risks
   - 4.2. Reporting Procedures
   - 4.3. Sanction
5. Authorìsing Access
6. Communicating this Policy

Appendix

- KS 1/2 Pupil Acceptable Use Agreement
- KS 3/4 Pupil Acceptable Use Agreement
- Parent Letter /Agreement Form
- Staff Acceptable Use Agreement

Context

1.1. Development of this Policy

Our e-Safety/Acceptable Use Policy has been written by the school, building on the guidance provided by DfE, the Northern Grid for Learning (NGfL), and BT Service. It has been agreed by senior management and approved by governors. it will be reviewed annually.

The E Safety/Acceptable Use Policy is part of the School Development Plan and relates to other policies, including Child Protection, information Technology and Healthy School.

1.2. Aims

This policy is intended to help provide clarification on unacceptable behaviours, relating to any information and communications technology (ICT) owned by the school, or personal technology used within the context of the school (this includes off site visits, using school systems at home etc).

It aims to cover all ICT including:-

- the use of computers on the school network.
- network and internet connectivity.
- all mobile devices including laptops, mobile phones, desktop computers and audio/visual equipment.
- all software, electronic communication and storage Systems.

It appîies to

- staff (teaching and non teaching).
- pupils.
- governors.
- parent heîpers.
- visitors.
- community users.

1.3 Teaching and Learning

1.3.1 Benefits of Information and Communications Technology

- The Internet and other digital technologies are an essential element in 21st century life for education, business and social interaction. The school has a duty to embrace such technologies and provide pupils with duality access and guidance, as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet use will enhance learning so the school access be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Internal networks and electronic communications, portable storage devices, audio visualequipment, laptops and PCs have become an essential part of the educational environment, so the whole school community needs to understand the appropriate and effective use of such technologies, to support teaching and learning.

1.3.2 Risks associated with Informatìon and Communications 'i'echnoiogy There are unfortunately some risks associated with the positive educational and social benefits of using the internet and other digital technologies. Pupils will therefore be:

- taught whaî Internet use is acceptable.
- be educated in the effective use of the Internet in research, inciuding the of knowledge location, retrieval and evaluation.
- taught what is not acceptable and be given clear objectives and guidelines for the use ofthe internet and other digital technologies.

2. Managing the School Network and Internet Access

2.1 Information systems security, filtering and monitoring.

- School ICT systems security Will be reviewed reguîarîy.
- The Headteacher is the @Safety C30-ordinator, who is responsible for ensuring that the policy is implemented, updated and complied with.
- The e~Safety Coordinator Will ensure that the school Community is kept up to date with e safety issues and guidance in collaboration with the LEA and Child Protection authorities.
- Security strategies will be discussed with the Local Authority.
- Virus protection Will be updated regularly.
- The school Will Work in partnership with South Tyneside LEA and NGfL to ensure that filtering systems are effective as possible.
- The Headteacher Will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- If staff or pupils come across unsuitable online materials, the site must be reported to the e Safety Coordinator.
- All users must observe password protocols for network and internet access.
- Passwords should be kept secret and never shared.
- PC/laptop screens should! be sited so they can be monitored by the teaching and support staff.
- The School maintains the right to regularly monitor internet traffic, the school's network and user email. We are obliged to monitor to fulfill our responsibilities with regard to UK law.

2.2 Communication Systems

2.2.1 Learning Piatform and Email

- Pupils are not aìlowed to access personal Email accounts from the school network at any time.

2.2.2. Managing approved Email Accounts

- All users who log on to the learning platform and school email system at home or at any other location, must only use these systems for educational use and are bound by the acceptable use guidelines.
- No users should ever use the school's communication systems to access or send inappropriate materials such as pornographic, racist or offensive material or to send or forward anonymous messages and chain letters.
- Users should not access public chat rooms and messaging systems (eg. MSN Messenger, etc.)
- Users should not use the schools communication technologies for personal financial gain, gambling, political purposes or advertising.
- Pupils when using e rnails Wilî be advised to never disclose personaì details such as name, address, age or telephone number.
- Any inappropriate communications received must be reported to a member of staff immediately.

2.2.3 Accessing Internet Sites

- Users should not visit sites that Contain illegal.obscene, hateful or other objectionable material.
- Users should use the schools internet for professional/educational purposes only and not for personal reasons, without the permissìon of the ESafety Coßordinator.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-Line materials.
- Teaching staff shouìd always research potential sites before directing pupil activities.
- Staff will always use a child friendly safe Search engine when accessing the web with pupils.

2.2.4 School web site

The School website is currently under Construction but the foìlowing protocols will be observed:

- Staff and pupil Contact information will not generally be published. The Contact information given, Will be that of the school office.

- The headteacher will take overail editorial responsibility to ensure that Content is accurate and appropriate.
- Photographs that include pupils will be carefully selected so that individuals Cannot be identified or their image misused. Group photographs will be used.
- names will not be used.
- The permission of parents be sought, before photographs or Work are published on the school website.

2.2.5 Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and Webcam use will be appropriately supervised for the pupils age.
- Webcams should be checked and monitored to ensure that misuse does not occur accidentally or otherwise.

2.2.6 Social networking, instant messaging and personal publishing

- The term ‘social networking’ refers to online communities where typically text, photos, music, video are shared by users. Instant messaging refers to online chatting to others in ‘real time’.
- The school will not normally allow adults and pupils access to social networking and instant messaging sites.
- Newsgroups will be blocked unless a specific use is approved.
- The school does accept that there can be educational benefits (eg collaborative work nationally and internationally) and will therefore examine their use for teaching and learning as the need arises.
- The school will consider how to educate pupils in their safe use.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location,
- Pupils will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

2.2.7 Social networking for staff and school representatives

This part of the policy covers the use of social networking applications by School Employees, Governors and/or Elected Members and by partners or other third parties on behalf of the School. These groups are referred to collectively as ‘school representatives’ for the purpose of this policy.

The requirements of this policy apply to all uses of social networking applications which are used for any school or local authority related purposes and regardless of whether the applications are hosted corporately or not.

They must also be considered where school representatives are contributing in an official capacity to social networking applications provided by external organisations.

- Social networking applications include, but are not limited to: blogs, online discussion forums, collaborative spaces, media sharing services, ‘microblogging’ applications. Examples include: Twitter, Facebook, MSN, YouTube.
- Many of the principles of this policy also apply to other types of online presence such as virtual worlds.
- All school representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School and Local Authority Equality and Safeguarding Policies.
- School staff will not invite, accept or engage in communications with parents or children from the school community to any personal social networking sites whilst in employment at Bamburgh School.

- Any communication received from children to school representatives must be immediately reported to the Head Teacher/Designated Child Protection Officer and procedures for safeguarding followed.
- If a school representative is made aware of any other inappropriate communications involving any child and social networking, these must be reported immediately as above. School internet policy must be used at all times when children use ICT and access the internet in school.

Enforcement

Any breach of the terms set out could result in the application or offending content being removed in accordance with the published complaints procedure and the publishing rights of the responsible school representative being suspended. The Local Authority reserves the right to require the closure of any applications or removal of content published by school representatives which may adversely affect the reputation of the school or put it at risk of legal action.

Any communications or content you publish that causes damage to the School, Local Authority, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the School and Local Authority Dismissal and Disciplinary Policies apply.

Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.

The Local Authority expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

2.3 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.4 Copyright and Plagiarism

- The school will ensure that copyright and intellectual property right laws are not infringed.
- Pupils will be taught to reference all material used from the internet and other sources, as they develop their research skills.

2.5 Managing Emerging Technoìogies

- The technology available to schools is constantìy evolving and the range of data and ICT services and products ever increasing. The school will therefore:
    - Examine emerging technologies for educational benefit and a risk assessment Wilt be carried out before use in school is allowed.
    - The senior leadership team should note that technologies such as mobile phones with Wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

3. Mobile Devices

3.1 Taking digital images using cameras and videos

lt is recognised that the taking of digital images is an integral part ofthe teaching and learning experience, but there must be a clear educational reason for Creating, storing, distributing andlor manipulating images of members of the school community.

- Staff and pupils may take digital photographs or videos using school equipment, providing that they support educational activities.
- Imageslvideo should not be taken with personal mobile phone Cameras (eg whilst on school visits).
- All images of children stored on the school network or on staff laptops should be placed in a common folder with a clear explanation of the intended use of the images, not in the personal areas of staff or other users of the systems.
- Pupils' names should not be used when saving images.

- Images should be deleted from laptops and PCs at the end of the academic year, unless retention is approved by the e-Safety co-ordinator.
- Pupils Will be taught how images can be misused, through their eSafety learning.

3.2 Mobile phones

- Pupils should not bring mobile phones into school. in exceptional circumstances, a written request may be sent to the headteacher. If approved, the phone wilt be stored in a central place until home time.
- Pupils will be advised the sending of abusive and inappropriate text messages or files by Bluetooth or any other means is forbidden.

3.3 Laptops

- Staff should store school laptops in a secure location overnight.
- If School laptops are taken home, staff are responsible for their security.
- School laptops are for sole use of the staff member to which they are loaned.
- The school IT technician is responsible for maintenance of school laptops and no other person shouîd tamper

with them.

3.4 Portable Storage Devices-

- All users should ensure that data stored on pen drives, disks, CD Roms etc has been downloaded using anti virus software.
- All users are responsible for the security of mobile storage devices.
- Images of children should not be stored on pen drives.
- Pupils are not allowed to use their own devices unless they have been checked for viruses by the teacher.

3.5 Games Machines

- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- Staff shouìd check that gaming software is age appropriate if machines are allowed (eg fun/toy days).

3.6 Video and DVD

- These should be age appropriate, as outlined by the classification authority.

4. Assessing Risks and Handling e-Safety Issues

4.1 Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor LEA can accept liability for any 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

4.2 Reporting Procedures

4.2.1 Reporting Accidental Access to inappropriate Material Any user of the school and/or Northern Grid Network who accidentaliy comes across inappropriate or offensive material should do the following:

1. Inform the school's E-Safety (co-ordinator of the incident and give the website address.
2. Ask the E-Safety Co~ordinator to log the web address, time and username in the school web log book.
3. The schools E-Safety Co~ordinator should ring the LEA school support helpdesk tel no 0191 4272120 and report the web address asking for an investigation as to whether the website should be permanently blocked.
4. if BT decide that the website is not sufficiently inappropriate for permanent blocking, the school should block the website via its own Smoothwall or other proxy server.

4.2.2 Reporting Accidental Access to Illegal Material Any User of the Northern Grid Network who accidentally report the incident to the e-Safety Coordinator/headteacher or senior manager.

1. Do not show anyone the content or make public the URL.
2. Make sure a reference is made of the incident in a log-book.
3. Go to the IWF website at WWW.IWF.GOV.UK and click the report button.
4. lf reporting a URL do not use Copy and paste, type the URL.

4.2.3 Reporting Suspected Deliberate Abuse or Misuse Any person suspeoiìng another of deliberate misuse or abuse of the regional broadband network should take the following action:-

1. Report in confidence to the school e-Safety Co-ordinator/headteacher of the school

2. The headteacher shouìd inform the Local Authority.
3. The Local Authority should complete an internal RIPA form, requiring Northern Grid to complete an internal investigation.
4. if this investigation results in confirmation of access to illegal materials or the committing of illegal acts, Northern Grid will inform the relevant police authority who will compete their own investigations.
5. if the investigation confirms that inappropriate behaviours occurred, Northern Grid will inform the relevant authority. This may be the Local Authority or the School's Board of Governors.
6. In exceptional Circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the police will be informed and a criminal prosecution may foltow.
   Examples of Inappropriate

   - Visiting pornographic sites (adult top shelf materials)
   - Causing offence to religious groups
   - inappropriate use of email
   - Deliberate sabotage of the network; i.e. hacking, mail bombing etc.

4.2.4 Access to llïegal Material

lf this investigation results in confirmation of access to illegal materials or the committing of illegal acts, Northern Grid or BT Will inform the relevant police authority that will complete their own investigations and a criminal investigation may follow.

Examples of Illegaì Acts:

- Accessing any child abuse images.
- Incitement to racial hatred
- Incitement to violence
- Software media counterfeiting or illegitimate distribution of copied software.