E-Safety Policy 2016

2016/01/01 Version Number: 1 (Transferred)

F Pass Review Date: 2018/01/01

Northern House School

1.0 Terms of Reference

1.1 Northern House School (City of Wolverhampton) aims to provide access to high quality education and learning experiences, both in school and in the community and seeks to maximise each pupil's achievement as part of his or her lifelong learning. It is the school's aim to be a digitally safe centre of Educational Excellence in the heart of the community.

1.2 This Policy has been written for all staff at Northern House School (City of Wolverhampton); pupils, parents and carers. All staff should have a working knowledge of this policy.

1.3 The aim of this policy is to:

- 1.3.1 Deal with the "here and now": informing and making children, young people and their families aware of the benefits and also the potential dangers of working on-line.
- 1.3.2 Build learning opportunities to develop children and young people as safe and e-confident learners, enabling their families to understand and support them in this area of their lives.
- 1.3.3 Provide technical safeguards such as appropriate web filtering and levels of access

1.4 Copies of this Policy may be obtained from;

- 1.4.1 Available electronically on the School Website.
- 1.4.2 Reference copy in the main School Office
- 1.4.3 Shared Area – Electronically

1.5 Edition, review and frequency;

- 1.5.1 Edition 1 released January 2016
- 1.5.2 The Objectives will be reviewed annually

1.6 Relevant Statutory guidance, circulars, legislation and other sources of information are:

- 1.6.1 Keeping Children Safe in Education July 2015
- 1.6.2 Please see appendix 1

1.7 The lead members of staff are Fran Pass, Head teacher (01902 551564) and Amanda MacDonald

1.8 The policy is broken down in to the following sections:

- 1.8.1 Introduction
- 1.8.2 Teaching And Learning
- 1.8.3 Managing Information Services
- 1.8.4 How Will Risks be Assessed
- 1.8.5 How Will E-safety Complaints Be Managed
- 1.8.6 How Should The Internet Be Used Across The Community
- 1.8.7 How Will Cyber-bullying Be Managed
- 1.8.8 Communication of This Policy
- 1.8.9 How Will Parents And Carers Support Be Enlisted
- 1.8.10 Appendices
- 1.8.11 Persons With Particular Responsibility

2.0 Introduction

2.1 Northern House School (City of Wolverhampton) believes that the use of information and communication technologies in school brings great benefits. Recognising E-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

2.2 Northern House School (City of Wolverhampton) is part of a world where technology is integral to the way life is led in the 21st Century. Compared to even five years ago the technology available outside school is rapidly increasing. In line with the Gilbert review document 2020 Vision, schools need to increasingly respond to:

- 2.2.1 An ethnically and socially diverse society
- 2.2.2 Far greater access and reliance on technology as a means of conducting daily interactions and transactions
- 2.2.3 A knowledge-based economy
- 2.2.4 Demanding employers, who are clear about the skills their businesses need and value
- 2.2.5 Complex pathways through education and training, requiring young people to make choices and reach decisions.

2.3 Why do students need to be safe working with technology?

- 2.3.1 As the uses of online technological resources have grown, so has the awareness of risks and potential dangers which arise for their use. Northern House School (City of Wolverhampton) aims to prepare its students to be able to thrive and survive in this complex digital world. This policy outlines the safeguarding approach to achieve this.

2.4 Who will write and review the policy?

- 2.4.1 The Designated Child Protection Coordinator – Member of the Governors.

3.0 Teaching and Learning

3.1 Why is Internet use important?

3.1.1 The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

3.1.2 Internet use is part of the statutory curriculum and a necessary tool for learning.

3.1.3 Internet access is an entitlement for students who show a responsible and mature approach to its use.

3.1.4 The Internet is a part of everyday 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.

3.1.5 Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

3.2 How does Internet use benefit education?

3.2.1 Educational and cultural exchanges between pupils world-wide;

3.2.2 Vocational, social and leisure use in libraries, clubs and at home;

3.2.3 Access to experts in many fields for pupils and staff;

3.2.4 Professional development for staff through access to national developments, educational materials and effective curriculum practice;

3.2.5 Collaboration across networks of schools, support services and professional associations;

3.2.6 Access to learning wherever and whenever convenient.

3.2.7 Exchange of curriculum and administration data with Northern House School (City of Wolverhampton) and DfE

3.2.8 Access to world-wide educational resources including museums and art galleries.

3.3 How can Internet use enhance learning?

3.3.1 The school Internet access will be designed to enhance and extend education.

3.3.2 Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

3.3.3 The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

3.3.4 Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

3.3.5 Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

3.3.6 Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

3.3.7 Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.

3.4 How will Pupils learn how to evaluate content?

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

3.4.2 The evaluation of on-line materials is a part of teaching/learning in every subject.

4.0 Managing Information Services

4.1 How will information systems be maintained?

4.1.1 Virus protection will be updated regularly.

4.1.2 The security of the school information systems and users will be reviewed regularly.

4.1.3 Portable media may not be used without specific permission followed by an anti-virus/malware scan.

4.1.4 Unapproved software will not be allowed in pupils' work areas or attached to email.

4.1.5 Files held on the school's network will be regularly checked.

4.1.6 The ICT co-ordinator / network manager will review system capacity regularly.

4.1.7 Personal data stored on portable storage devices will be encrypted.

4.1.8 Portable media may be used in agreed circumstances with specific permission followed by a virus check.

4.2 How will Email be managed?

4.2.1 Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.

4.2.2 Staff should not use personal email accounts during school hours or for professional purposes.

4.2.3 Excessive social e-mail use can interfere with learning and may be restricted.

4.2.4 E-mail sent to external organisations should be written carefully, in the same way as a letter written on school headed paper.

4.2.5 The forwarding of chain messages is not permitted.

4.2.6 Staff may only use approved e-mail accounts.

4.2.7 Staff must immediately tell their Line Manager if they receive offensive e-mail.

4.3 How will published content be managed?

4.3.1 The contact details on the website should be the school address, email and telephone number, staff or pupils' personal information must not be published.

4.3.2 Email addresses will be published carefully online, to avoid being harvested for spam.

4.4 Can Pupils Images And Work Be Published?

4.4.1 The Head teacher and Chair of the Governing body will take overall editorial responsibility and ensure that content is accurate and appropriate.

4.4.2 Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

4.4.3 Written permission from parents or carers will be obtained before images of pupils are electronically published.

4.4.4 Pupils work can only be published with their permission or their parents/carers.

4.5 How Will Social Networking And Personal Publishing Be Managed?

4.5.1 The school will control access to social media and social networking sites.

4.5.2 Newsgroups will be blocked unless a specific use is approved.

4.5.3 Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

4.5.4 Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.

4.5.5 Teachers' official blogs, wikis etc. should be password protected and run from the school website or approved school communication channels. Teachers should be advised not to run social network spaces for student use on a personal basis.

4.5.6 Pupils should be advised on security and encouraged to set safe passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to communicate to known friends only and deny access to others.

4.5.7 Students should be advised not to publish specific and detailed private thoughts.

4.5.8 Staff wishing to use Social Media tools with students as part of the curriculum should risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate and must obtain documented consent from the Senior Leadership Team before use.

4.6 How Will Filtering Be Managed?

4.6.1 The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

4.6.2 Breaches of filtering will be reported to the Senior Leadership Team and the appropriate action taken in line with school policy. All members of the school community (all staff and all pupils) will be aware of this procedure.

4.6.3 The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.

4.6.4 Any material that the school believes is illegal must be reported to appropriate agencies.

4.6.5 The school's broadband access will include filtering appropriate to the age and maturity of pupils.

4.6.6 If staff or pupils discover unsuitable sites, the URL must be reported immediately to the e–Safety Coordinator.

4.7 How Can Emerging Technologies Be Managed?

4.7.1 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

4.8 How Should Personal Data Be Protected?

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

4.9 Policy Decisions

4.9.1 The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

4.10 How Will Internet Access Be Authorised?

4.10.1 All staff must read and sign the Acceptable Use Policy before using any school ICT resource.

4.10.2 Students will have supervised access to the internet as part of their study programme and during social times.

4.10.3 Failure to follow usage guidance will result in access being reviewed.

5.0 How Will Risks Be Assessed?

5.1 The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.

5.2 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.

6.0 How Will E-Safety Complaints Be Handled?

6.1 Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.

6.2 Any complaint about staff misuse must be referred to the principal. Pupils and parents will be informed of the complaints procedure. Parents and pupils will need to work in partnership with staff and the school to resolve issues.

6.3 Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Education Safeguards Team to establish procedures for handling potentially illegal issues.

6.4 Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

6.5 All e–Safety complaints and incidents will be recorded by the school, including any actions taken.

6.6 All members of the school community will be reminded about safe and appropriate behaviour online and the importance on not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

7.0 How Will Cyber-Bullying Be Managed?

7.1 Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti- bullying.

7.2 There will be clear procedures in place to support anyone affected by Cyberbullying.

7.3 All incidents of Cyberbullying reported to the school will be recorded.

7.4 There will be clear procedures in place to investigate incidents or allegations of Cyberbullying. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

7.5 The school will take steps to identify the individuals whom are using 'bullying' behaviours, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

7.6 Sanctions for those involved in Cyberbullying may include:

7.6.1 Removing any material deemed to be inappropriate or offensive.

7.6.2 A service provider may be contacted to remove content.

7.6.3 Internet access may be suspended at school for the user for a period of time.

7.6.4 Parent/carers may be informed.

7.6.5 The Police will be contacted if a criminal offence is suspected.

8.0 Communication Of This Policy

8.1 How Will The Policy Be Introduced To Pupils?

8.1.1 An e–Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.

8.1.2 An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.

8.1.3 Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

8.2 How Will The Policy Be Discussed With Staff?

8.2.1 The e–Safety Policy will be formally provided to and discussed with all members of staff.

8.2.2 Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is supervised by the Senior Leadership Team, and there are clear procedures for reporting issues.

8.2.3 Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

9.0 How Will Parents/Carers Support Be Enlisted?

9.1 Parents' attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the school website.

9.2 Interested parents will be referred to relevant organisations

9.3 A partnership approach to e-Safety at home and at school with parents will be encouraged. This could include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e–Safety at other attended events e.g. parent evenings, sports days.

9.4 Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.

10.0 Appendices

10.1 This policy has 3 appendices

10.1.1 Contacts Resources and References

10.1.2 Roles and responsibilities

10.1.3 Procedures

11.0 Appendix 1 - e-Safety Contacts, Resources and References:

11.1 CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

11.2 Childline: www.childline.org.uk 0800 1111

11.3 Childnet: www.childnet.com

11.4 Children's Safeguards Service www.kenttrustweb.org.uk?safeguards

11.5 Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

11.6 Cybermentors: www.cybermentors.org.uk

11.7 Digizen: www.digizen.org.uk

11.8 Internet Watch Foundation: www.iwf.org.uk

11.9 Kent e–Safety in Schools Guidance: www.kenttrustweb.org.uk?esafety

11.10 Kidsmart: www.kidsmart.org.uk

11.11 Safer practice with technology: https://shareweb.kent.gov.uk/Documents/KSCB/Safer%20Practice%20with%20Technology.pdf

11.12 Think U Know website: www.thinkuknow.co.uk

11.13 Virtual Global Taskforce: www.virtualglobaltaskforce.com

12.0 Appendix 2 – Management of Digital Safeguarding

12.1 Clearly stated roles and responsibilities:

12.2 Head of School

12.2.1 Ensure that the digital safeguarding policy is implemented and compliance with the policy monitored, and that the appropriate roles (see this section) and responsibilities of the school's digital safeguarding structure is in place.

12.2.2 Ensure regular reports of the monitoring outcomes on digital safeguarding are reported to the governing body.

12.3 Nominated e-Safety Coordinator

12.3.1 There is an identified e-safety coordinator who is responsible for e-safety developments in school and sharing of practice with staff and the wider community.

12.3.2 This person will be in receipt of current training on the latest guidance and procedures and is the main contact for the Local Authority e-Safety networks.

12.3.3 All digital safeguarding incidents within the school need to be reported to this person. They need to keep the log of incidents and with the Head teacher make decisions about how to deal with reported incidents.

12.4 E-Safety Governor

12.4.1 There is an identified e-safety governor who monitors and liaises with the e-safety coordinator and who will report to full governing board as appropriate.

12.5 E-Safety responsibility within subject and management roles:

12.5.1 All staff with subject and management roles have a duty to incorporate e-safety principles in their area of responsibility, deputising for any of the above roles where appropriate.

12.6 Teachers/Teaching Assistants

12.6.1 All staff understand the need for care and caution when using technology both for academic and social purposes and apply it to teaching and learning situations.

12.6.2 They need to work to agreed guidelines. They have a "front line" monitoring and reporting role for incidents.

13.0 Appendix 3 – Procedures

13.1 Are as defined in the School Disclosure and reporting procedures described in the School Safeguarding Procedures and policies

- 13.1.1 Procedures for reporting beyond the school to the LA
- 13.1.2 Incident log
- 13.1.3 Signing lap top agreements
- 13.1.4 Entitlement to training and support
- 13.1.5 Monitoring

13.2 Risks and acceptable behaviours

- 13.2.1 General use of the internet
- 13.2.2 Passwords/personal details
- 13.2.3 Data Security
- 13.2.4 E-mail
- 13.2.5 Learning Platform
- 13.2.6 Appropriate use of hardware
- 13.2.7 Photographs video and sound recording
- 13.2.8 Copyright
- 13.2.9 Social networking/cyber bullying
- 13.2.10 Mobile phones/technology

13.3 Physical and technical security

- 13.3.1 Firewall provision
- 13.3.2 Filtering provision
- 13.3.3 Antivirus software
- 13.3.4 Passwords/Biometric
- 13.3.5 Network monitoring