NANTWICH PRIMARY ACADEMY & NURSERY

PRINCIPAL – Sue Spence

E-safety Policy

PAGE: 1 of 9 **ISSUE: two** **DATE: November 2020** **REVIEW: November 2021**
Approved by:Sue Spence

Nantwich Primary Academy & Nursery
Manor Road, Nantwich, Cheshire, CW5 5LX
Tel – 01270 685000
admin@nantwichprimaryacademy.co.uk

Introduction

Computing 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.

Computing 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
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much computing, 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.

At Nantwich Primary Academy and Nursery we understand the responsibility to educate our pupils 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.

Both this policy and the St Bart's Acceptable Use Policy (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by staff, but brought onto school premises (such as laptops, mobile phones and camera phones.

Roles and Responsibilities

As E-safety 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. The named eSafety co-ordinator in our school is Lee Bebbington who has been designated this role as the Computing Subject Lead. All members of the academy community have been made aware of who holds this post. It is the role of the E-safety co-ordinator to keep abreast of current issues and guidance through organisations such as Education Bradford, Becta, CEOP (Child Exploitation and Online Protection) and Childnet. He works closely with the Designated Safeguarding Lead and the school Learning Mentor.

Senior Management and Governors are updated by the Principal/E-safety co-ordinator and all governors have an understanding of the issues and strategies at our academy in relation to local and national guidelines and advice.

This policy, supported by the academy's acceptable use agreements for staff, governors, visitors and pupils is to protect the interests and safety of the whole academy community. It is linked to the following mandatory academy policies: safeguarding, health and safety and behaviour/pupil discipline (including the anti-bullying) policy and PHSCE**.**

E-safety skills development for staff

- Our staff receive regular information and training on E-safety issues in the form of staff meetings, twilights and written correspondence.
- New staff receive information on the academy's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-safety and know to report the misuse of technology by any member of the school community to the E-safety co-ordinator or the Principal.
- 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 pupils at the start of each academy year.
- E-safety rules are displayed next to computers.

E-safety in the Curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for E-safety guidance to be given to the pupils 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 provides opportunities within a range of curriculum areas to teach about E-safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-safety curriculum.
- Pupils are 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/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models and discussions.

Managing the Internet

Use of the Internet to Enhance Learning:

- The academy internet access is designed for pupil use and includes filtering.
- Pupils are taught what internet use is acceptable and what is not.
- Internet access will be planned to enrich and extend learning activities.
- Staff will preview any recommended sites before use.
- Staff will guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.

Authorised Internet Access

- The academy maintains a current record of all staff and pupils who are granted Internet access.
- All staff must read the 'St Bart's Acceptable Use Policy Learners and Staff' before using any school ICT resource.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk or the support technician via the Principal or E-safety co-ordinator.
- Our academy will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- It is the responsibility of the academy, by delegation to the network manager (RedTop), to ensure that Anti-virus protection is installed and kept up to date on all school machines.

Social Networking

The use of public social networking sites (e.g. bebo, myspace, face book) is not allowed in our academy.

- The Academy will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils are taught not to place personal photos on any social network space.
- Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal face book site.

Mobile technologies

- The academy allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the academy allow a member of staff to contact a pupil or parent/ carer using their personal device.
- Staff are not permitted to use mobile phones / texts during lesson time.

- Currently pupils are not allowed to use personal mobile devices/phones in school. KS2 children, who may be walking home alone, carry a mobile phone but **must** give this to their classteacher / School Office as soon as they enter the classroom. This is at parents' own risk.
- The academy is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the academy community is not allowed.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of our academy, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve expected levels in Computing, pupils must have experienced sending and receiving emails.

- The academy gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils or parents using personal email addresses.
- Pupils may only use approved e-mail accounts on the school system.
- 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.
- Access in school to external personal e-mail accounts may be blocked.

Safe Use of Images

- With the written consent of parents (on behalf of pupils) and staff, the academy permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.
- Staff must adhere to the St Bart's "Bring Your Own Device" policy.

Consent of adults who work at the academy

- Permission to use images of all staff who work at the school is sought on induction.

Publishing pupil's images and work

On a child's entry to the academy, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).
- This consent form will be valid for the entire period that the child attends this academy. However, parents/ carers may withdraw permission, in writing, at any time.

Published content and the academy website and learning platform

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site or Blog, especially in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site/school prospectus.

Webcams and CCTV

- Some webcam sites may contain, or have links to, inappropriate or adult material. Teachers view any webcam sites or listings before allowing pupils to do so.
- Pupils are alerted to the danger of using web cams as an extension of a chat room. Although this will be highly unlikely at the academy, pupils need to know the risks involved when using web cams at home.
- Parents are asked to sign and return a consent form for pupil access.

Filtering

The academy will work in partnership with the Local Authority, Becta and the Internet Service Provider to ensure filtering systems are as effective as possible.

Managing Emerging Technologies

Emerging technologies will be examined by the Computing co-ordinator for educational benefit and a risk assessment will be carried out before use in school is allowed.

Information System Security

Academy ICT systems capacity and security will be reviewed regularly.

Virus protection will be installed and updated regularly.

Security strategies will be discussed with the Local Authority / Trust.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The St Bart's Data Protection Policy available upon request.

Assessing Risks

- The academy will take 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 an academy computer.
- The academy will audit Computing use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate.

Equal Opportunities

Pupils with additional needs
The academy endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the academy's E-safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil 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.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting E-safety both in and outside of the academy.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school E-safety policy via E-safety training, governor meetings, parents questionnaire
- Parents/ carers are asked to read through the acceptable use agreements on behalf of their child.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website). See above for detail.

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by the E-safety co-ordinator or Principal and recorded in the Incident Log.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be reported to the Designated Safeguarding Lead.

Pupils and parents will be informed of the complaints procedure.

Pupils are encouraged to inform their teacher or other adults in the academy regarding anything which makes them feel uncomfortable while using ICT.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms (SMART rules).
- Pupils will be informed that Internet use will be monitored.

Staff

- All staff will be given the academy 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.

Parents

- Parents' attention will be drawn to the academy E-safety Policy in newsletters, the academy prospectus and on the academy website.

Linked Policies:-

- Privacy Notice (for parents)
- Data Protection Policy
- Bring Your Own Device Policy
- St Bart's Acceptable Use Policy Learners and Staff

Signed by Chair of Governors

…………………………………………………………………………..

Signed by Principal

………………………………………………………………………….

Date

………………………………….

Nantwich Primary Academy and Nursery

Primary Pupil Acceptable Use

Agreement / E-safety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use programs that my teacher has agreed I can use.
- ✓ I will only open attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address.
- ✓ I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E-safety.

Signed by Classteacher

……………………………………………………………………..

Signed by Child

…………………………………………………………………….

Date

………………………………….