Macaulay Primary Academy
E-safety Policy

September 2016

We believe that the use of the internet is of great educational benefit to children. Research and our own experience suggest the following benefits:
• Improved motivation and attitudes to learning.
• Improved subject learning across a all curriculum areas, not just ICT.
• Development of independent learning and research skills.
• Children are equipped with the skills that are needed for the 21st century.

What we do at Macaulay Primary Academy

As well as the above benefits, we are aware that there are possible dangers with using the internet. At Macaulay we have taken positive steps to reduce the likelihood of such problems occurring:
• We have an Acceptable Use Policy, (AUP) which is shared and agreed with all children and parents. This is displayed throughout the school and teachers regularly refer to it. The AUP is reviewed annually to take into account changes in technology and the way the school uses technology.
• Comprehensive e-safety education is provided to children in the form of specific units as part of the ICT curriculum and Safeguarding including PREVENT. This deals with e-mail and internet, mobile phones, instant messaging and social networking sites as well as radicalisation and extremism.
• Our internet access restricts access to unsuitable sites. We also use Software on all machines that block unacceptable content and unsuitable sites.

Scope
This policy and guidance applies to both fixed and mobile internet technologies provided by SPTA or an Academy (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.) and technologies owned by students and staff, but brought onto Academy premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).
These technologies are to be used for business purposes in serving the interests of our learners and staff in the course of normal operations.

Acceptable Use Policy
The acceptable use policies ensure ICT can be used to support learning without their being unnecessary risk to users.
There are two AUPs, one for foundation stage and key stage 1, one for key stage 2. The differences between these two policies reflect the level of ICT use by children of that age and their level of understanding.

Foundation Stage/Key Stage 1 AUP:

- We use the internet for our learning.
- We only use our own passwords and usernames.
- We check with a teacher before talking to anyone using the internet
- We know we can ask a teacher if there is anything we are not sure about.

Key Stage 2 AUP:
- I keep my passwords a secret.
- I will tell a teacher straight away if I find something on the internet that is not nice or makes me feel uncomfortable.
- I am polite when communicating using ICT, just like I am when communicating with people face- to-face.
- I do not give out personal details to anyone.
- When I am in school, I only use email through the school's learning platform.
- When communicating using ICT with people outside of the school, I always check with a teacher first.
- We understand that not everything that is said or written on the internet is true.
- I understand that what I write, view, upload and download from the internet will be seen by other people.
- I will only login and use my area of the learning platform. I never use other people's passwords and usernames.
- I will not delete other people's files.

e-Safety in the Curriculum

- SPTA has a framework for teaching internet skills in ICT/ PHSE lessons
- SPTA provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating students on the dangers of technologies that may be encountered outside SPTA is carried out informally when opportunities arise and formally as part of the e-Safety curriculum.
- Students are made 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 and respecting other people's information, images, etc. through discussion, modelling and activities.
- Students are made aware of the impact of online bullying and of how to seek help if they are affected by these issues. Students are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies i.e. Learning Mentors parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ Child Exploitation and Online Protection (CEOP) report abuse button.
- Students are taught to evaluate materials critically and to learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

Students with additional needs
SPTA endeavours to ensure that each Academy creates a consistent message with parents of all students. However, staff are aware that some students may require additional teaching including reminders, prompts and

further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has additional needs in respect of social understanding, careful consideration should be given to group interactions when raising awareness of e-Safety. Internet activities must be planned and well managed for these children and young people.

Parental Involvement

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the Academy.

- 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 an Academy website).

- The Academy disseminates information to parents relating to e-Safety where appropriate in the form of:

    - Information and celebration evenings;
    - Posters;
    - Website/ Learning Platform postings;
    - Newsletter items; and
    - Learning platform training.

Password Security

All users are responsible for implementing password security in all aspects of creating, protecting and managing passwords. Passwords for SPTA systems must be created and managed in accordance with this policy. See Appendix 3 for guidance

Password Disclosure

Users must not disclose their passwords to anyone.

Users must not write their passwords down under any circumstances.

Unauthorised password disclosure is deemed a serious security matter and may be dealt with under the SPTA's Disciplinary Procedure, up to and including termination of employment.

Data Security

The accessing of Academy data is something that SPTA takes very seriously.
Any data shared with an external body must be subject to a data sharing agreement approved by the SPTA Director of ICT.
Staff must be made aware of their responsibilities when accessing Academy data.
They must not:

- access data outside of Academy, except when entering assessment data;
- take copies of the data;
- allow others to view the data;
- Edit the data unless specifically requested to do so by the Principal and/ or the Education Advisory Body;
- Leave SIMS open for students to view;
- Leave their workstations unlocked when leaving the classroom;
- Allow a student to use the classroom PC; and
- Share staff passwords or store passwords insecurely.

Further details and Appendices can be found in the SPTA eSafety policy and guidance and access can be arranged via the Safeguarding team.

P.Costall September 2016

Review Date September 2017