UNSWORTH PRIMARY SCHOOL

Policy for E-Safety

"Together we build understanding"

Rationale

At Unsworth Primary School we take a strategic approach to developing Computing. The DFE e-strategy 2005 stated:

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners. To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom."

We, as a whole school community, work together under the guidance of The Children's Act 2004, Keeping Children Safe in Education 2019 and Teaching Online Safety in school June 2019 documents to safeguard and promote the welfare of our children. In addition we ensure a culture that upholds the General Data Protection Regulations is embedded across the school. Our filtering system (Surf Protect) fully complies with the Internet Watch Foundation (IWF) guidelines

Aims

Through this policy we endeavour to ensure that every child in our care is safe and the same principles apply to the virtual or digital world as would be applied to the school's physical buildings. At Unsworth Primary School creating a safe Computing learning environment includes three main elements:

- An effective range of technological tools; including
  - The Internet
  - e-mail
  - Blogs or Vlogs (an on-line interactive diary)
  - Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
  - Video broadcasting sites (Popular: http://www.youtube.com/)
  - Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/ / http://www.clubpenguin.com)
  - Social media apps (Twitter, Facebook, Snapchat, WhatsApp etc)
  - Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
  - Mobile phones with camera and video functionality
  - Mobile technology (e.g. games consoles) that are "internet ready".
  - Smart phones with e-mail, web functionality and cut down "Office" applications.
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-safety education programme for pupils, staff and parents linked to current practice, which is weaved throughout the curriculum and promoted through the school website and Twitter account.

Leadership

At Unsworth Primary school e-safety and data protection is recognised as an essential aspect of strategic leadership and the Head Teacher, with the support of the trustees and Local Governing Body, aims to embed safe practices into the culture of the school. The Head Teacher ensures that the policy is implemented and compliance with the policy monitored. The responsibility for coordinating e-safety sits with the Head Teacher and all e-safety incidents are reported termly to the local governing body. The schools incident

reporting policies and arrangements are followed as set out in the school safeguarding policies.

The e-safety coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority E-safety Officer and through organisations such as NAACE, NSPCC and The Child Exploitation and Online Protection (CEOP). The Head Teacher is EPICT certified and ensures Oak Learning Partnership, SLT, Governors, staff and children are updated as necessary, through policy updates, a pupil led e-safety group with representatives from each class and regular briefing within staff meetings.

Trustees need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-safety and are updated formally at least annually on policy developments and informally on a more regular basis.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. Central to this is fostering a "No Blame" culture so pupils feel able to report any bullying, abuse or inappropriate materials. All staff are familiar with the schools" policies including:

- Safe use of e-mail.
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social media.
- Safe use of the school network, equipment and data.
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras.
- Publication of pupil information/photographs through the use of Twitter, Trello, Tapestry and the school website.
- Cyberbullying signs and procedures.
- Their role in implementing the school e-safety curriculum.

Staff are reminded and updated about e-safety matters at least once a year and as issues or new developments arise.

Scheme of Work

Our Computing curriculum includes an e-safety programme of study explicitly, which begins in the Reception year through to Year 6 at an age appropriate level and it is built into all other areas of the Computing curriculum. Staff are also aware of the importance of reminding the children of the e-safety rules and messages wherever computing is used to support and enhance other curriculum areas. Each classroom displays a set of safety rules that children refer to regularly when online.

As part of our e-safety curriculum staff and pupils are encouraged to cover all aspects of what it means to be "e-safe". Coverage includes:

- Knowing how to respond to distasteful and inappropriate material by reporting to an adult, covering the screen or by turning the device off.
- Becoming Internet wise, with the idea of "Stop and Think Before you Click" ensuring that personal information remains private. This includes protecting teacher's professionalism by not inviting pupils past or present into personal social networking sites.
- Copyright and sharing information on the internet is investigated. Children are encouraged only do this to this through their class page on the school website under direction of a member of staff or within their Trello portfolio. This is monitored by a member of staff.
- A rolling programme of advice, guidance and training for parents, including: Information leaflets; in school newsletters; on the school web site; demonstrations,

practical sessions held at school; distribution of “think u know" for parents materials, suggestions for safe Internet use at home and provision of information about national support sites for parents.

- Judging the quality, truth and relevance of information they find on the internet. Also understanding that just because something is published does not make it fact, encouraging pupils to evaluate between what is fact, fiction or opinion.
- The dangers and consequences of cyberbullying or grooming incidents and how these need to be dealt with. This includes introducing agencies such as CEOP.
- Extending this education, safety and skills to the dangers of unprotected, unfiltered web access outside of school. For example not chatting to unknown people, sharing information about themselves, understanding why on-line friends may not be who they say they are, and not publishing pictures or videos of others without permission.

This discrete e-safety teaching ensures that pupils are aware of potential risks, how these can be minimised and how to report problems. This practice also ensures and encourages the “No Blame" culture within school where pupils feel able to report any abuse, bullying, misuse or inappropriate content.

EYFS

In our EYFS, we have a duty to provide children with quality internet access as part of their learning experience. Internet access will be tailored expressly for educational use and will include appropriate filtering. Pupils will learn appropriate internet use through our computing curriculum. Staff will guide pupils in online activities that will support their learning journeys. The internet is also used in the Reception classroom to support the professional work of staff, to allow the effective capture of observations through the Tapestry app. All staff are fully trained on how to access and use Tapestry to comply with the school data protection policy.

Training/CPD

To ensure that this teaching is effective and the messages are constantly reinforced all staff are aware of all of the policies relating to Computing and safeguarding including the infringements policy. Training and awareness raising is available as required for all members of staff including governors, administration staff and any adult helpers. A discussion around this also forms part of the induction of new members of staff and students. Staff are also aware that internet traffic is monitored and can be traced to an individual user. Therefore discretion and professional conduct are essential. All of these factors work together to produce “e-safe" children and help to restrict the risk of exposure to inappropriate, offensive and harmful situations. Our e-safety education is a continuing feature of staff CPD and the children’s lifelong learning. This is continuously being reviewed and updated to incorporate current developments and trends.

Parent Support

In addition to in school access, most of our children have access to the internet at home and in some cases this is unrestricted and unsupervised access. To support our parents with e-safety issues we use the e-safety area of the website, monthly newsletters, the school e-safety blog and CEOP’s parent feed which is linked to the home page of the school website.

Infringements and Sanctions

The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. All staff are given information regarding infringements and possible sanctions. These are in line with the Infringements, Cyberbullying and Anti-bullying policies. Our e-safety coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head Teacher. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with school / BISP child protection procedures.

Links to other Policies

- Safeguarding & Child Protection 2019
- Computing Policy 2018
- Content Filtering Statement 2017
- Acceptable Use Policy 2019
- Internet Policy 2019
- Blogging Policy 2019
- Website Policy 2019
- Email Policy 2019
- Password Policy 2019

Policy Prepared by A Rhodes November 2016
Reviewed by A Rhodes September 2019