E-Safety Policy

Reviewed & Updated Nov 2017

Our e-Safety has been written by the school, building on the London Grid For Learning (LGFL) exemplar policy and Local authority NPW guidance.

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant messaging (www.skype.com http://info.aol.co.uk/aim/) often using simple web cams
- Blogs (an on-line interactive diary)
- Forums (online message board about pre-selected topic of discussion)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.facebook.com www.myspace.com / www.piczo.com / http://www.hi5.com / www.bebo.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/ / http://www.clubpenguin.com)
- 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 (apps).

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-safety education programme for pupils, staff and parents.

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the policy is implemented and compliance with the policy monitored. The responsibility for e-safety has been designated to the e-safety coordinator.

Our school e-safety Co-ordinator is Mr Richard Langford.

Our e-Safety Coordinator ensures he keeps up to date with e-safety issues and guidance through liaison with the Local Authority e-safety Officer, NPW Education ICT, and through organisations such as the London Grid for Learning (LGFL) and The Child Exploitation and Online Protection (CEOP)[1]. The school's e-safety coordinator ensures the Headteacher, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of e-safety issues and strategies at our school. We ensure our governors are aware of the local and national guidance on e-safety and are updated at least annually on policy developments.

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 should be familiar with the school's policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data and cloud-based storage;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of pupil information/photographs and use of website;
- E-Bullying / Cyber bullying procedures;
- Their role in providing e-Safety education for pupils;
-

[1] http://www.ceop.gov.uk/

Staff are reminded / updated about e-Safety matters at least once a year.

At William Davies, e-safety is embedded in the curriculum to ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to control (build on the knowledge, link actions and link learning on line) and minimise online risks and how to report a problem.

We ensure that we engage with parents with regard to e-safety matters and that, on entry, parents/carers have signed an e-safety Acceptable User Policy (AUP) form.

How we communicate with pupils on e-safety.

- There is an e-safety training programme to raise the awareness and importance of safe and responsible Internet use.
- Instruction in responsible and safe use precedes any lesson with Internet access.
- An e-safety module is included in the PSHCE, Citizenship or ICT programmes covering both school and home use.
- Age appropriate internet safety videos and websites are posted on our website.

How we communicate with staff on e-safety

- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-safety Policy will be provided as required.
- Long term supply staff on temporary contracts will be issued a login and directed to the acceptable use policy in the Staff Handbook.

How we communicate with parents on e-safety.

- A partnership approach with parents is encouraged. This includes parent evenings with demonstrations and suggestions for safe home Internet use.
- Internet issues are handled sensitively, and parents will be advised accordingly.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet is made available to parents.

What are the e-safety issues?

Although the use of ICT and the Internet provide ever-increasing opportunities for children to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to the risk of harm.

Apart from the risk of children accessing Internet sites, which contain unsuitable material, risks to the well being of children may also exist in a variety of other ways.

At William Davies we create a safe learning environment, which means having effective arrangements in place to address a range of issues and we ensure that we have policies (Safeguarding, Child Protection, Anti bullying) and procedures in place, which are reviewed and adhered to by all staff, teaching and non-teaching whether in a paid or voluntary capacity.

How will complaints regarding e-safety be handled?

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. The Internet is managed via filtered access by LGFL and locally by NPW. Children are trained how to act if they should access an unsuitable site or image. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions might be;

- Interview/counselling by class teacher / e-safety Coordinator / Headteacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system.]
- Referral to NPW School Support (Alan Merry Head of School Support Service) If advised, Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with child protection procedures.

How we Manage Equipment

At William Davies we:

- Ensure staff read and sign that they have understood the staff handbook, which includes reference to e-safety. Following this, they are given Internet, email access and an individual google log-in username and password;
- Provide pupils with an individual network and google login. Increasingly the children are expected to use a personal password;
- Make it clear that staff must keep their username and password private.
- Make clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Make clear that no one should log on as another user;
- Have a shared Google drive with appropriate restrictions in place;
- Require all users to always log off when they have finished working or are leaving the computer unattended;
- Follow the guidance of the LGFL use of digital and video images policy;
- Follow the guidance of the LGFL acceptable use of the Internet and related technologies;
- Follow the guidance of the LGFL on e-safety for Parents/carers
- Follow the guidance of the LGFL on e-safety for staff and adults working with children.