Prospere
LEARNING TRUST

Prospect House
PRIMARY SPECIALIST SUPPORT SCHOOL

E-SAFETY POLICY

E-Safety Policy

E-safety may be described as the school's ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate.

WHY IS THIS IMPORTANT?

Technology offers unimaginable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile and pupils are using technology at an ever earlier age.

For example:

- 91% of children aged 5-15 live in a household with internet access via a PC/laptop, up from 87% in 2010.[1] Smartphone ownership in 2010 comprised 3% of children aged 5-7, 13% of children aged 8-11, and around 35% of children aged 12-15.[2]
- 34% of children aged 8-12 have a profile on sites that require users to register as being 13 or over, up from 25% in 2009.[3]

Technology use and e-safety issues go hand in hand. Many incidents happen beyond the physical geography of the school and yet can impact on pupils or staff.

There are three main areas to consider:

CONTENT

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

CONTACT

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords

CONDUCT

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images)
- copyright (little care or consideration for intellectual property and ownership (for example music and film))

INTERNET SAFETY:

- When using a network workstation all access to the Internet is protected by a number of different filters. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators can manually add site addresses which are considered to be unacceptable. However, no system is 100% safe and we expect users to behave responsibly. *Pupils are taught that the Internet contains many websites that are useful but that there are also websites that are unpleasant, offensive, and not child-friendly or can damage your computer.* **We expect pupils to make no attempt to access a website that they know to be unsuitable for children and/or containing offensive language, images, games or other media.**
- Pupils accessing the Internet at home are subject to the controls placed upon them by their parents. However, any home use of the Internet made in connection with the school or school activities; any of its staff, pupils and governors or any partnership organisation will be subject to this policy and any breach dealt with as if the event took place at school. **We expect all members of our school community to behave as positive ambassadors of the school in all school related activities made through the Internet.**

- The school website contains school policies, newsletters and other information. **We expect all persons accessing the school web site to treat the content with respect and make no attempt to reproduce, use or alter any part in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the school.**

EMAIL SAFETY:

- Some classes have a class email address which pupils can use for sending messages to other classes, schools and other appropriate recipients. The class teacher monitors the pupil's use of this email address and receives a copy of all incoming email. *Pupils are taught that emails sent from their class should have a clear learning purpose and be written in a polite style which is appropriate to the person that will receive it*. **We expect all users to communicate appropriately through email.**

- Some pupils will have their own webmail accounts at home. As these are independent of the school they do not necessarily come with the safeguards that we set for email usage. Therefore we do not permit the use of personalised email accounts by pupils at school or at home for school purposes. *Pupils are taught that using a personalised webmail account in school or for school use is not permitted.* **We expect pupils to use school issued email accounts only.**

DIGITAL IMAGES:

- Digital still and video cameras are used for recording special events as well as being essential tools for everyday learning experiences across the curriculum. As part of pupil induction, parents are asked to sign a consent form for images of their children to be used for school purposes. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website. On the website we never state a child's full name with their image. **The school will happily remove any image of a child on the school website at their parent's request.**

- Digital images may be shared with partner schools and organisations as part of collaborative learning projects. This can include live video conferencing. All such use is monitored and supervised by staff. *Pupils are taught to seek permission before copying, moving, deleting or sending any images taken within school.* **We expect all pupils to seek permission from staff before sharing images outside of the school environment.**

E-BULLYING:

- The school takes bullying very seriously and has robust procedures for identifying and dealing with it. E-bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. *Pupils are taught about bullying as part of the PSHE curriculum***. We expect all members of our community to communicate with each other with respect and courtesy. Bullying of any type will not be tolerated by the school and will be dealt with under the procedures within the Whole School Policy on Behaviour, including bullying.**

MOBILE PHONES:

- Pupils are not permitted to have mobile phones upon their person in school. We recognise that our oldest pupils may walk on their own to and from school and parents may wish them to have a mobile phone for emergencies. However we discourage this on security grounds as they are easily lost, damaged or stolen. *Pupils are taught that they shouldn't have a mobile phone on their person in school and that any phone brought in must be handed to the office/teacher for the duration of the day*. **We expect pupils not to carry a mobile phone in school.**

PREVENT

- All staff are aware of their PREVENT duty and will ensure any internet material is suitable and will report any breaches.

OTHER TECHNOLOGIES:

Podcasting

- Some pupils will be given opportunities to create oral recordings. Some of these recording may be made available as podcasts through the Internet so that they can be shared with interested members of the school community

Copyright:

- Though there are lots of free to use resources on the Internet, the majority of image, sound and music files are covered by copyright laws. Some can be used for educational reasons without permission provided that the source is stated and that they are not made available outside the school. Some cannot be used under any circumstances, this is particularly so for music but can apply to other types of file e.g. photographic images. Care therefore needs to be taken with multi-media work which incorporates anything downloaded from the Internet or any other published source that it is not uploaded onto the school's website or broadcast through any other technology. *Pupils are taught that the people who put their work on the Internet may not always want people to copy or use their work and that they should check whether they have permission.* **We expect all users to respect copyright laws.**

- It is important to know what work is original and when chunks of text have been copied from other sources such as the Internet. *Pupils are taught that they should not present the work of others as their own work. Older pupils are taught about copyright and how to extract or paraphrase information.* **We expect all pupils to make it clear what is their own work and what is quoted from other sources.**

DATA PROTECTION ACT:

- The Data Protection Act 1998 gives you the right to access information held about you or your child by the school. The school has the right to charge for supplying this information. Further information on the Data Protection Act can be obtained from the Department of Constitutional Affairs – www.justice.gov.uk

E-safety Rules for school and home use
• We ask permission before using the Internet. • We only use websites that an adult has chosen/or are supported by an adult. • We tell an adult if we see anything we are uncomfortable with. • We immediately close any web page we not sure about. • We only e-mail people an adult has approved. • We send e-mails that are polite and friendly. • We never give out personal information or passwords. • We never arrange to meet anyone we don't know. • We do not open e-mails sent by anyone we don't know. • We do not use Internet chat rooms without asking.

GLOSSARY OF TERMS FOR STAFF

Acronyms and jargon are common place in technology and often obscure meaning and understanding. The following link provides access to a wide ranging glossary of technological terms in current use http://www.digizen.org/glossary/.

In addition, the following terms used in this document are explained below

360 degree safe	SWGfL's online self-review tool for school improvement in online safety www.360safe.org.uk.
Age related filtering	Differentiated access to online content managed by the school and dependent on age and appropriate need (commonly used providers include Smoothwall, Lightspeed, Netsweeper, RM).
AUP	Acceptable Use Policy
Byron Review	Professor Tanya Byron's seminal report from 2008, 'Safer Children in a Digital World'.
CEOP	Child Exploitation and Online Protection centre.
Cyber bullying	Bullying using technology such as computers and mobile phones.
Encryption	Computer program that scrambles data on devices such as laptops and memory sticks in order to make it virtually impossible to recover the original data in event of the loss of the device; schools often use this to protect personal data on portable devices.
EPICT	European Pedagogical ICT Accreditation.
E-safety mark	Accreditation for schools reaching threshold levels within 360 degree safe through assessment by external assessor.

Frape	Short for 'Facebook rape', referring to when a Facebook user's identity and profile are compromised and used by a third party to cause upset.
Games Console	Examples include XBOX 360, Nintendo Wii, PlayStation 3, Nintendo DS.
Grooming	Online grooming is defined by the UK Home Office as: 'a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes'.
Hacker	Originally thought of as a computer enthusiast, but now a hacker is normally used to refer to computer criminals, especially those who break into other people's computer networks.
ISP	Internet Service Provider (a company that connects computers to the internet for a fee).
Lifestyle website	An online site that covertly advocates particular behaviours and issues pertaining to young and often vulnerable children for example anorexia, self-harm or suicide.
Locked down system	In a locked down system almost every website has to be unbarred before a pupil can use it. This keeps the pupils safe, because they can use only websites vetted by their teachers, the technicians or by the local authority, any other website has to be unbarred for a pupil to be able to use it, which takes up time, detracts from learning and does not encourage the pupils to take responsibility for their actions (note that a locked down system may be appropriate in an EYFS setting or in a special school).
Malware	Bad software or programs that damage your computer (viruses), steal your personal information (spyware), display unwanted adverts (adware) or expose your computer to hackers (Trojan horses).
Managed system	In a managed system the school has some control over access to websites and ideally offers age-appropriate filtering. Pupils in schools that have managed systems have better knowledge and understanding of how to stay safe than those in schools with locked down systems because they are given opportunities to learn how to assess and manage risk for themselves.
Phishing	Pronounced the same as 'fishing' this is an attempt to trick people into visiting malicious websites by sending emails or other messages which pretend to come from banks or online shops; the e-mails have links in them which take people to fake sites set up to look like the real thing, where passwords and account details can be stolen..
Profile	Personal information held by the user on a social networking site.
RBC	Regional Broadband Consortium, often providers of schools broadband internet connectivity and services in England, for example SWGfL, London Grid for Learning (LGfL).
Safer Internet Day	Initiated by the European Commission and on the second day, of the second week of the second month each year.
Sexting	Sending and receiving of personal sexual images or conversations to another

	party, usually via mobile phone messaging or instant messaging.
SHARP	Example of an anonymous online reporting mechanism (Self Help And Reporting Process).
SNS	Social networking; not the same as computer networking, social networking is a way of using the internet and the web to find and make friends and stay in touch with people.
Spam	An e-mail message sent to a large number of people without their consent, usually promoting a product or service (also known as Unsolicited Commercial Email (UCE) or junk email).
Trojan	A malware program that is not what it seems to be. Trojan horses pretend to be useful programs like word processors but really install spyware or adware or open up a computer to hackers.
Youtube	Social networking site where users can upload, publish and share video.

SAMPLE QUESTIONS FOR PUPILS

1. If you felt uncomfortable about anything you saw, or if anybody asked you for your personal details such as your address on the internet would you know where to go for help?
2. If anybody sent you hurtful messages on the internet or on your mobile phone would you know who to tell?
3. Can you tell me one of the rules your school have for using the internet?
4. Do you understand what the risks of posting inappropriate content on the internet are (secondary students only)?

SAMPLE QUESTIONS FOR STAFF

1. Have you had any training that shows the risks to your and pupils online safety?
2. Are there policies in place that clearly demonstrate good and safe internet practice for staff and pupils?
3. Are there sanctions in place to enforce the above policies?
4. Do all staff understand what is meant by the term cyber-bullying and the effect it can have on themselves and pupils?
5. Are there clear reporting mechanisms with a set of actions in place for staff or pupils who feel they are being bullied online?
6. Does school have any plans for an event on Safer Internet Day

Policy Information and Review

Policy review dates (frequency of review: every 3 years)

Date	Changes made	By whom