E-Safety Policy

Date for full implementation
March 2017

Date for review
March 2018 (or earlier if considered necessary)

Signature/s

……
Chair of Governors

……
Head Teacher

Introduction

The resources used by pupils at Grange Primary School are usually carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its very nature, will occasionally provide access to information which has not been selected by the teacher - particularly as children reach the later years of Key Stage 2. Within school and our wider community, there is genuine cause for concern that children may access unsuitable material either accidentally or deliberately.

The purpose of this document is to provide a basis for us all to secure safety when using digital technology and when working online. It's content has been devised in accordance with national guidance from BECTA and 3 key documents "*E-Safety: Developing whole-school policies to support effective practice, Safeguarding children in a digital world* and *Signposts to Safety.* It should be considered alongside complementary school policies on Child Protection, Health and Safety, Home-School Agreement and Behaviour (including the Anti-bullying policy). The implementation of this policy seeks to ensure that children stay safe, and that they be protected from harm, neglect and extremism and grow up able to look after themselves.

The Internet and other digital and information technologies are powerful tools that open up new opportunities for everyone. We believe that the benefits to pupils from access to the resources of the Internet, far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the School shares with parents and guardians. We feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

Roles and Responsibilities

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the E-Safety Co-ordinator / Officer • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager)

E-Safety Co-ordinator / Designated Child Protection Lead	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
	• promotes an awareness and commitment to e-safeguarding throughout the school community
	• ensures that e-safety education is embedded across the curriculum
	• liaises with school ICT technical staff
	• To communicate regularly with SLT and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• To ensure that an e-safety incident log is kept up to date
	• facilitates training and advice for all staff
	• liaises with the Local Authority and relevant agencies
	• seek advice from The Prevent Duty guidance when concerns of extremism.
	• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media
	  • extremism

Governors / E-safety governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: • regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs)

Role	Key Responsibilities
Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly • Manage, monitor and filter DB Primary forums. • Communicate with parents and provide e-safety advice. • Arrange and manage Safer Internet Day. • Work closely and support teachers
Network Manager/technician	• To report any e-safety related issues that arises, to the e-safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • LGfL is informed of issues relating to the filtering applied by the Grid • that he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • that the use of the *network / Virtual Learning Environment (LEARNING PLATFORM) / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *E-Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction* • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures • To contact DB Primary for further information.
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To set E-Safety tasks on DB primary to refresh and update children's awareness. • To explain how the 'Whistle' on DB Primary helps them to stay safe. • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws. • To teach children the SMART rules for the internet. • To explain how Hector the protector works. • To be aware of those young people who are being targeted by or exposed to harmful influences from violent extremists via the internet. Young people should be warned of the risks of becoming involved in such groups and it should be against service policy to access such sites.

Role	Key Responsibilities
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • to know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • to help the school in the creation/ review of e-safety policies • To know the SMART rules. • To use Hector the protector when necessary.
Parents/carers	• to support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to access the school website / LEARNING PLATFORM / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement. • to consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Using the Internet for Education

The benefits include:

¨ access to a wide variety of educational resources including libraries, art galleries and museums, that can stimulate discussion and promote creativity

¨ rapid and cost effective world-wide communication

¨ gaining an understanding of people and cultures around the globe

¨ staff professional development through access to new curriculum materials

At Grange, we teach pupils about the vast information resources available on the Internet, using it as a planned aspect of many lessons. All staff will review and evaluate resources available on web sites appropriate to the age range and ability of the pupils being taught and the ICT Leader will assist in the dissemination of this information.

Initially the pupils may be restricted to sites that have been reviewed and selected for content. They may be given tasks to perform using a specific group of web sites. Pupils may have the opportunity to exchange information with others via email however access to public chat rooms and social networking sites is prohibited and therefore blocked by the schools filtering system.

As pupils gain experience, they will be taught how to use searching techniques to locate specific information for themselves. Comparisons will be made between researching from different sources of information such as CD Roms, books and the World Wide Web. We hope that pupils will learn to decide when it is appropriate to use the Internet as opposed to other sources of information, in terms of: the time taken; the amount of information found; the usefulness and reliability of information located.

At times information, including photographs and images, may be downloaded from carefully selected Internet sites for use in pupils' presentations. As children become older, tasks will be set to encourage pupils to view web sites and information with a critical eye. However, Grange Primary specifically discourages the downloading of text for inclusion in pupils' work. *This includes inclusion of such text for homework projects!* As well as encouraging pupils to create original work and avoid plagiarism (a serious academic offence), Grange Primary School considers it appropriate to emphasise the importance of protecting intellectual property rights and, in particular, copyright. Pupils will be made aware of these issues and, as soon as they are able, will be encouraged to look for copyright information on websites, so reinforcing their understanding of the importance of copyright.

Pupils' Access to the Internet

Grange Primary will use London Grid for Learning's (LGFL) actively monitored and 'filtered' Internet Service, which will minimise the chances of pupils encountering undesirable material. If staff or pupils discover unsuitable sites, the URL (web address) and content will be immediately reported to the Internet service provider via the ICT leader and will be blocked within a short period of time. We will only ever allow children to use the Internet when there is a responsible adult present to supervise them. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, on a regular basis, the expectation we have of them. Rules for Internet access will be posted near computer systems. The 'Rules for Responsible Internet Use' could be printed as posters. The ICT co-ordinator will have access to pupils' emails and workspaces, and will make periodic checks these on a regular basis to ensure expectations of behaviour are being met. Children will be aware of how to use Hector the protector in the event that they encounter something online that worries them,

Securus has been installed on all of the PC's and laptops in the school. Securus detects inappropriate content as soon as it appears on screen, whether it has been typed or received by the user. A screen capture is taken of every incident, showing what was displayed at the time, who was involved and when the incident took place. Our external IT support company monitors the Securus system and reports any inappropriate activity to the head teacher.

Acceptable Use of Personal Technology

No pupil is able to use a mobile phone during school hours/trips and so Internet access should only occur via the school networks. The use of personal technology such as cameras, CD's and memory sticks is also strictly prohibited.

Expectations for Internet use

¨ We expect everyone to be responsible for their own behaviour on the Internet, just as they are anywhere else in school.

¨ Pupils must always ask permission before using the Internet and have a clear idea why they are using it.

¨ Children and staff will never reveal personal details, home addresses and telephone numbers on the web or in dialogue with other Internet users.

¨ Children are only permitted to use EasyMail class addresses or DB Primary email accounts. All email will be moderated and monitored by the class teacher. The use of unfiltered web-based email (such as Hotmail) is not permitted and therefore cannot be accessed on school computers.

¨ Children will not engage in any form of conversation or dialogue with other users on the Internet without permission and supervision from their teacher. This may only occur within privately created chat rooms with closely guarded passwords.

¨ The use of public chat rooms and Internet Messaging Services is prohibited.

¨ The use of social networking sites such as MySpace are not generally appropriate to primary education and the use of the Internet for such purposes is not currently permitted.

¨ The use of personal technology such as mobile phones, cameras, CD's and memory sticks is prohibited.

¨ Computers should only be used for schoolwork and homework.

¨ Files may only be downloaded by staff, or children under supervision.

¨ Pupils using the Internet are expected not to deliberately seek out offensive materials. Should any such material be encountered accidentally, or if any child finds themselves uncomfortable or upset by anything they discover on the Internet, they will click on Hector the Protector icon immediately and report it to the supervising adult. (Any adult should report it to the ICT Leader or Head Teacher immediately. Arrangements can then be made to request that the Internet Service Provider blocks the site).

In Reception and year 1, children may log on using a year group login, but from Year 2 upwards, pupils should generally only access the network using their own personal login. No network user should access other people's files unless permission has been given.

Any infringement of these conditions of use will be dealt with by the class teacher/Head Teacher as appropriate and sanctions may apply. Parents will be informed.

School Web Site Guidelines

A web site can celebrate good work, promote the School, publish resources for projects and homework, and link to other good sites of interest. However, to protect our children, the following guidelines will be adhered to:

- Photographs of pupils will only be of general groups, in full clothing, preferably at a distance or otherwise not easily identified- e.g. with face averted. Individual photos will not be used.

- No names or other identifying information will be attached to photographs.
- The content of pictures should be considered for good taste and the dignity of people in the pictures.
- Pupil's work displayed online will be identified only by class – e.g. "painting/writing by a P3 pupil" and will not contain information, such as family names, which might identify that pupil or family members. Nicknames which do not allow identification of child may be allowed.
- Any incident of an image considered by a pupil, staff member or parent to have been inappropriate to the website or these guidelines should be reported to the headteacher. The person reporting may chose to do so anonymously, but must give reasons why they feel the images is not appropriate.
- Teacher's pages must not contain: CVs and personal messages;
  non-job related personal information; personal opinions about school policy or related controversial issues; personal contact details.
- Governing Body and Friends of Grange pages should not contain personal contact details of members.
- Pupil or class pages are generally created as class assignments. However, they must nevertheless be checked to ensure that they do not contain personal contact information about the student, including email addresses.
- Pupil or class pages must be reviewed by the teacher prior to posting or modification
- Pupil or class pages must not include links to their own or other pupils' personal web sites containing personal contact information or materials and contents contrary to the Pupil Acceptable Use Policy or these guidelines.
- Events and trips. General information only. An email link will be provided for parents to request details to be sent home with their child, on paper.

Parents who would prefer that their children do not appear on our school website, for whatever reason, are asked to inform the school office in writing. An up-to-date list of such children is kept in the school office and referred to before new pages are added. If, at any time, a parent expresses concern about usage of an image or piece of work, it will be removed from our site as quickly as possible.

Learning Platform

As our community moves towards use of a Learning Platform, it is important to note that any user who accesses this provision will be expected to agree to a Community Acceptable Use Policy before access is granted. As online reporting and parental engagement develops, our e-safety guidelines will be reviewed.

Information and further guidance for parents:

We have done all that is possible to ensure children are protected through the use of a filtered service and a requirement that an adult always supervises Internet access. Our children are taught to use the facility sensibly - the rules concerning Internet use are regularly discussed in class and we welcome your endorsement of these. We strongly recommended that parents consider and develop a similar set of rules for the use of the Internet outside of school. You might also like to discuss as a family the issues surrounding the downloading of music, mobile phones, social networking sites, and the use of blogs, within the home environment. You may find the "Know IT all" CD and the following websites extremely useful to help ensure that children stay safe.

Childnet International is a non-profit organisation working to help make the Internet a great and safe place for young people. These sites are all created by this organisation

http://www.childnet-int.org http://www.kidsmart.org.uk http://www.chatdanger.com

You can find downloadable safety leaflets here:

http://www.childnet-int.org/downloads/parents-leaflet.pdf

http://www.childnet-int.org/downloads/musicLeaflet.pdf

http://www.childnet-int.org/downloads/ICRA-Bill-of-Rights.pdf

http://www.childnet-int.org/downloads/a2poster.pdf

Other useful sites include:

Safe Kids	http://www.safekids.com
Cyber Patrol	http://www.cyberpatrol.co.uk
Net Nanny	http://www.netnanny.com
CBBC	http://www.bbc.co.uk/cbbc/help/safesurfing (aimed at KS1)
Bullying Online	http://www.bullying.co.uk
Think U Know	http://www.thinkuknow.co.uk

(including Hector's WorldTM - suitable for 5-7 year olds)

Further guidance can be found in the following documents (see ICT Leader or SWGFL):

BECTA: Safeguarding Children online (2009); SWGFL Trust: Safety and Security (2009); SWGFL School e-safety Policy (2009)

E-safety Policy Appendices

Can be found on the following pages:

Think before you click!

S

I will only use the Internet and email with an adult

A

I will only click on icons and links when I know they are safe

F

I will only send friendly and polite messages

E

I will click on Hector the Protector when I feel unsafe.

My Name:

My Signature:

KS2 Pupil Acceptable Use Agreement

The 12 Rules for Responsible ICT use

These rules will keep me safe and help me to be fair to others.

1. I will only use the school's computers for schoolwork and homework.
2. I will only edit or delete my own files and not look at, or change, other people's files without their permission.
3. I will keep my logins and passwords secret.
4. I will not bring files into school without permission or upload inappropriate material to my workspace.
5. I am aware that some websites and social networks have age restrictions and I should respect this.
6. I will not attempt to visit Internet sites that I know to be banned by the school.
7. I will only e-mail people I know, or a responsible adult has approved.
8. The messages I send, or information I upload, will always be polite and sensible.
9. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
10. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
11. I will never arrange to meet someone I have only ever Previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
12. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will use Hector the Protector and call my teacher/ additional adult.

I have read and understand these rules and agree to them.

Signed: …… *Date: ……*

Grange Primary School e-safety agreement form: Parents

Parent / guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter(s) or son(s) to have access to use the Internet, LGfL e-mail* and other ICT facilities at school.

I know that my daughter or son has signed an e-safety agreement form and that they have a copy of the '12 Rules for responsible ICT use' (KS2) or the 'Think before you click' form (KS1).

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email*, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their e-safety or
e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent / guardian signature: _____

Date: ___/___/___

Use of digital images - photography and video: I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital and video images'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent / guardian signature: _____ **Date:** ___/___/___

Grange Primary School
Use of digital images - photography and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow these rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity;
  e.g. photographing children at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the children to see their work and make improvements.

- Your child's image for presentation purposes around the school;
  e.g. in school wall displays and PowerPoint© presentations to capture images around the school or in the local area as part of a project or lesson.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website. In rare events, your child's could appear in the media if a newspaper photographer or television film crew attend an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

• Computer storage areas will be treated like school lockers. ICT staff may review your files and communications to ensure that you are using the system responsibly.
• When sensitive or personal data is required by an authorised user from outside the school's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
• If secure remote access is not possible, users must only remove or copy personal or sensitive data from the school premises if the storage media, portable or mobile device (memory stick) is encrypted and is transported securely for storage in a secure location. Council policy requires the use of a specific whole-disk encryption software called PGP Whole Disk Encryption on any laptop which is used to store confidential data.

Internet

• Staff should access the Internet only for school activities during work time.
• Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
• Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
• 'Chat' activities take up valuable resources which could be used by others to benefit their studies, and you can never be sure who you are really talking to. For these reasons use of 'chat' rooms are not allowed.
• Members of staff should be wary of compromising their professional standing through inappropriate use of social media.

Email

• Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behavior is as anti-social on the Internet as it is on the street.
• Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your compute and compromise the whole school network..
• If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of SLT and Network Manager. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden and is monitored.
• Staff e-mail and Internet use is also filtered for the safety of all members of staff.

Please read this document carefully. Only once it has been signed and returned to the Network Manager access to the school network will be given. If you violate these provisions, access to the school network will be denied and you will be subject to disciplinary action. Access to LGFL emails, shared drives and personal drives can be accessed at any time on request from SLT during or after employment has ended.

Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Signature: _____ Date: _____

Name: _____

E-safety incident report form

This form should be kept on file and a copy emailed to Harrow's _____?

School/organisation's details:

Name of school/organisation: **Grange Primary School**
Address: Welbeck Road, Harrow, HA2 0RY
Name of e-safety contact officer: **A. Szymaniak** (Headteacher)
Contact details:

Details of incident

Date happened:

Time:

Name of person reporting incident:

If not reported, how was the incident identified?
Where did the incident occur?
□ In school/service setting □ Outside school/service setting
Who was involved in the incident?
□ child/young person □ staff member □ other (please specify
Type of incident:
□ bullying or harassment (cyberbullying
□ deliberately bypassing security or access
□ hacking or virus propagation
□ racist, sexist, homophobic religious hate material
□ terrorist material
□ drug/bomb making material
□ child abuse images
□ on-line gambling
□ soft core pornographic material
□ illegal hard core pornographic material
□ other (please specify)

Description of incident

Nature of incident

□ Deliberate access

Did the incident involve material being;

□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Could the incident be considered as;

□ harassment □ grooming □ cyberbullying □ breach of AUP
□ Accidental access

Did the incident involve material being;

□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Action taken

□ Staff

□ incident reported to head teacher/senior manager
□ advice sought from Family Services and Social Work
□ referral made to Family Services and Social Work
□ incident reported to police
□ incident reported to Internet Watch Foundation
□ incident reported to IT
□ disciplinary action to be taken
□ e-safety policy to be reviewed/amended

Please detail any specific action taken (ie: removal of equipment)

□ Child/young person

□ incident reported to head teacher/senior manager
□ advice sought from Family Services and Social Work
□ referral made to Family Services and Social Work
□ incident reported to police
□ incident reported to social networking site
□ incident reported to IT
□ child's parents informed
□ disciplinary action to be taken
□ child/young person debriefed
□ e-safety policy to be reviewed/amended

Outcome of incident/investigation

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology)
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
DCSF	Department for Children, Schools and Families
ECM	Every Child Matters
FOSI	Family Online Safety Institute
HSTF	Home Secretary's Task Force on Child Protection on the Internet
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICT Mark	Quality standard for schools provided by Naace
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network and RBCs.
KS1	Key Stage 1 (2, 3 or 4) – schools are structured within these multiple age groups e.g. KS2 = years 3 to 6 (age 7 - 11)
LA	Local Authority
LAN	Local Area Network
Learning Platform	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
LSCB	Local Safeguarding Children Board
MIS	Management Information System
VLE	Virtual Learning Environment

NEN	National Education Network – works with the Regional Broadband Consortia (eg LGfL) to provide the safe broadband provision to schools across Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
RBC	Regional Broadband Consortia (eg LGfL) have been established to procure broadband connectivity for schools in England. There are 10 RBCs covering 139 of the 150 local authorities:
SEF	Self Evaluation Form – used by schools for self evaluation and reviewed by Ofsted prior to visiting schools for an inspection
SRF	Self Review Form – a tool used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark
LGfL	London Grid for Learning – the Regional Broadband Consortium of Local Authorities – is the provider of broadband and other services for schools and other organisations in the London area
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol