Cedars Primary School E-safety Policy

Using new learning technologies effectively and safely

Reviewed October 2023 by Jemma Vaisnys

OVERVIEW

Our E-safety Policy has been written by the Computing Co-ordinator. It has been agreed by the senior leadership team and approved by Governors. It will be reviewed annually. Technology is commonplace and its effective use is an essential life skill. Unmediated access to a range of resources brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. A policy is required to help ensure acceptable use were the safety of pupils and staff is safe guarded. E-Safety depends on staff, school governors, advisors, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and associated communication technologies.

The resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information, which has sometimes not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times they will be able to move beyond these to sites unfamiliar to the teacher.

There is therefore the possibility that a pupil may access unsuitable material either accidentally or deliberately. The purpose of this policy is to:

- Establish the ground rules we have in school for using the Internet.
- Describe how these fit into the wider context of our behaviour and PHSE policies.
- Demonstrate the methods used to protect the children from sites containing unsuitable material.

Safety Audit

This self-audit should be taken our every year.

Has the school an e-Safety Policy that complies with Becta guidance?	**yes**
Date of latest update: **October 2023**	
The Policy was agreed by governors on: **October 2023**	
The Policy is available for staff and on: **School Website and Staff Shared**	
And for parents on: **School Website**	
The Designated Child Protection Coordinator is: **Mrs N Truman**	
The e-Safety Coordinator is: **Mrs Vaisnys**	
Has e-safety training been provided for both students and staff?	**Children throughout the year across EYFS/Computing curriculum**
Do all staff sign an ICT Code of Conduct on appointment?	**Yes and every September for staff**
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	**Yes**
Have school e-Safety Rules been set for students?	**Yes**
Are these Rules displayed in all rooms with computers?	**Yes – Posters should be seen in all areas**
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access	**Yes**
Has an ICT security audit been initiated by SMT, possibly using external expertise?	**Crystal**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Yes**

Teaching and learning

As the children's access and understanding expands, so should the guidance and rules to ensure safe access use of the internet

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Pupils will be taught how to evaluate Internet content appropriate to their age.

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what Internet use is responsible and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation appropriate to their age group.
- Sanctions for inappropriate use of the internet will be explained to the children.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly with Crystal.
- Virus protection is updated regularly by Crystal.
- Security strategies will be discussed with Blackburn with Darwen and Crystal.

Managing filtering

- The school will work with the LA, DCSF, Internet Service Provider and Crystal to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator and the LA will be informed so that they can take appropriate action.

Staying safe

The school will ensure that pupils and parents are aware of e-safety issues. A list of useful addresses and resources is included in this document.

- The school internet access is designed expressly for pupil use and includes appropriate filtering.
- Pupils may only use approved digital methods of communication on the school system e.g. not forwarding chain letters.
- Pupils will be taught to tell an adult immediately about any offensive communications they receive or any inappropriate content they may encounter using digital technology.
- Pupils and staff will use equipment responsibly.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location or arrange to meet anyone without specific permission.
- Pupils and parents will be advised that the unsupervised use of social network spaces outside school is inappropriate for pupils.

Published content

Any information that can be accessed outside the school's intranet should be classed as published whether in electronic or paper format.

- Electronic communication sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- General contact details should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Staff and pupils using digital cameras, video recorders or sound recorders will ensure that they inform others before recording them and always use equipment in a respectful manner, these should never be taken off school premises on unsecure devices and without prior permission from a member of the senior leadership team.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- If parents deny permission or permission is stopped due to a safe guarding issue, photographs of these children should never be used.
- Pupils' full names will not be used anywhere, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs or video of pupils are published.
- Where pupil's work is published the school will ensure that the child's identity is protected.

Managing emerging technologies

- The educational benefit of emerging technologies and any potential risks will be considered before it is used in school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

POLICY DECISIONS

Authorising Internet access

- All staff and volunteers must read and sign the 'ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Children and parents must sign the ICT user agreement every year before any access to ICT resources is granted.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Blackburn with Darwen LA can accept liability for the material accessed, or any consequences of Internet access. Any inappropriate access whether intentional or unintentional will be reported to the e safety co-ordinator and to the LA where necessary.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and where appropriate inform the LA.
- Any complaint about staff misuse must be referred directly to the headteacher.
- Complaints of a child protection nature must be dealt with immediately in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure on request.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all rooms and discussed with the pupils during the first ICT lesson of the year. ICT user agreements will be signed with the children during this lesson and returned from home, once signed by parents.
- Pupils will be informed that network and Internet use will be monitored and can be monitored and traced to the individual device or login.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that internet traffic may be monitored and traced to the individual device or login. Discretion and professional conduct is essential.
- The school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.
- All staff must read and sign the ICT user agreement every year.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy on the school's website

Appendix 1

Sexting Protocols

Introduction

'Sexting' is one of a number of 'risk-taking' behaviours associated with the use of digital devices, social media or the internet. It is accepted that young people experiment and challenge boundaries and therefore the risks associated with 'online' activity can never be completely eliminated. However, Cedars Primary School takes a pro-active approach to help students to understand, assess, manage and avoid the risks associated with 'online activity'.

The school recognises its duty of care to its young people who do find themselves involved in such activity as well as its responsibility to report such behaviours where legal or safeguarding boundaries are crossed.

There are a number of definitions of 'sexting' but for the purposes of this policy sexting is simply defined as:

- Images or videos generated by children under the age of 18, or of children under the age of 18 that are of a sexual nature or are indecent.
- These images are shared between young people and/or adults via a mobile phone, handheld device, computer, 'tablet' or website with people they may not even know.

Aim

Cedars Primary School will not tolerate 'sexting', it is inappropriate and illegal amongst young people and can have extremely damaging and long-lasting consequences. This policy has been created in order to provide a guide for parents, staff and pupils as to how the school will proceed and what steps will be taken should an incident of sexting be reported or suspected.

Legal Implications for Pupils

Sexting potentially breaches several civil laws concerned with the creation, possession and distribution of child pornography and indecent images. These are images which show partial (where breasts or genitals are exposed) or full nudity and/or feature sexual acts being performed. It is illegal for pupils to make and/or share images such as these, even if they are images of themselves, which have been taken personally or with consent.

Pupils who engage in sexting (to any extent) are at risk of receiving a police caution and/or being placed on a register for sexual offenders for a period of several years (which can have serious ramifications in adulthood with regards to employment, travel etc.).

Sexting can also (in some cases) be viewed as a crime under the Malicious Communications Act. Sexting is therefore identified as unacceptable behaviour and the possession of pornography is prohibited in school.

The misuse of IT, such as sexting, inappropriate comments on social networking, being the object of cyber-bullying and online grooming are all potential welfare concerns and identified as such in our Safeguarding Policy.

Our Duty

As staff, we have a responsibility to work with parents and carers in ensuring that all pupils are fully aware of the dangers and possible repercussions of sexting. In school, this information will be communicated to pupils through vertical tutoring, in assemblies and through parental information. Sexting incidents are often complicated as they potentially involve a large number of pupils and those involved could be victims or perpetrators or both. Depending on the specific circumstances and gravity, the incident will be investigated as a safeguarding/pupil wellbeing issuer.

Protocol

Where an incident of sexting is reported or suspected at Cedars Primary School

- If “sexting” is reported by the victim or deemed to be a Child Protection matter, then it must be treated as a disclosure of a Child Protection matter and referred to the Pupil Wellbeing Officer.
- Parents and carers will be notified and the incident will be reported to the police, as appropriate.
- Pupils will be sanctioned in accordance with our Behaviour Policy. Sexting is a serious offence and dependent on motive, intent, pressure or coercion, those involved may be issued with fixed term or, in extreme cases, even permanent exclusion.
- Pupils may also be required to attend workshops to ensure that they understand legality, consequences and to work through specific scenarios.
- Pupils may also be subject to interview by the Police and confiscation of their electronic devices.

Guidance for staff if you suspect that an offence has been committed

- If you suspect that “sexting” has taken place or you become aware of indecent images circulating in school or a pupil refers an incident of “sexting” to you, then you must refer it straight away to the Headteacher or the Pupil Wellbeing Officer.

- Although all staff are by law permitted to search pupils without their consent if they have a reasonable suspicion that they may have prohibited items in their possession, such as pornography, you may put yourself at risk of allegations by attempting to deal with this issue or by viewing indecent images yourself, so this is an investigation that should be carried out by the Headteacher or Pupil Wellbeing Officer.
- DO NOT search, copy, print images that do come to your attention. Switch off or put in flight mode so phone cannot be remotely wiped, secure phone and seek advice. Staff do not want to inadvertently implicate themselves simply by viewing such material.
- If you are in any doubt whatsoever, seek immediate advice from the Headteacher or Pupil Wellbeing Officer and refer the issue on.

Appendix 2

Sexting Referral Protocol

Considerations – risk assessment

- Vulnerability of the child
- Coercion
- How shared and where
- Impact on children
- Age of the children

5 points for referral:

1. Adult involvement
2. Coercion or blackmail
3. Extreme or violent
4. Under 18
5. Immediate risk of harm

Initial disclosure
This could come from a pupil directly, a parent, a pupil's friend. Treat as a child wellbeing issue and follow its referral protocol. DO NOT share/look at material yourself.

Initial review
At this initial stage the Pupil Wellbeing Officer and the Head teacher review the information and consider the 5 points for immediate referral.

Risk assessment/Dealing with the incident
Consider the risk of harm and at any point if there are 'causes for concern' you should refer to police/social care.

Police/social care referral
Refer to local arrangements for dealing with incidents and contact local services.

Management in school
Ensure parents are informed and the incident recorded following all child protection and safeguarding procedures.

Appendix 3

ICT Risk Protection and Breach Protocol

CRYSTAL - IT Protection and role

- Crystal to ensure that SOPHOS is loaded on the server, regularly updated and deployed.
- Crystal to ensure that no machine is running Microsoft software that is not supported by current updates as notified by Microsoft.
- Crystal to ensure Microsoft updates are up to date and deployed.

The Web Filter detects and/or blocks access to inappropriate material on the Internet based on our extensive, education-specific URL database with more than one billion entries, as well as your own custom allow and block lists. It categories based on subject matter and age-appropriateness, providing easy review and administration.

WIFI

The Wi-Fi in the school is very secure, as it uses WPA2 with AES encryption to ensure that nobody can unlawfully gain access to the wireless network, this means that to gain access to the network somebody would have to physically plug into a network port in the school.
At this point the user would be able to access only a very limited portion of the network, as all of the files are stored in encrypted containers which can only be accessed with the correct user level privileges, for example, a pupil only has access to folders such as pupil shared, pupil home drives etc, whereas a teacher will have access to their own home drive, staff shared and pupil shared. Only Admin Staff can access the administrative folders and only SEN staff can access the SEN folders, this compartmentalisation ensures that files and folders are accessed only by those who have the rights to be able to access them.

Areas of Possible threats

- Any equipment being brought in from outside should only be allowed to be used with permission from the Head.
- **Supply teachers** should seek the permission from the head to use own equipment in school
- **Students** should not be using electronic equipment from home in school.
- **Training** by outside companies doing presentations or demonstrations must be checked before use.
- **Contractors**, Door entry/CCTV etc using equipment to set up their systems. (they are not allowed to load Sophos)
- **Staff** - Wi-Fi on phone. Staff should not have access to Wi-Fi on their personal mobile devices.

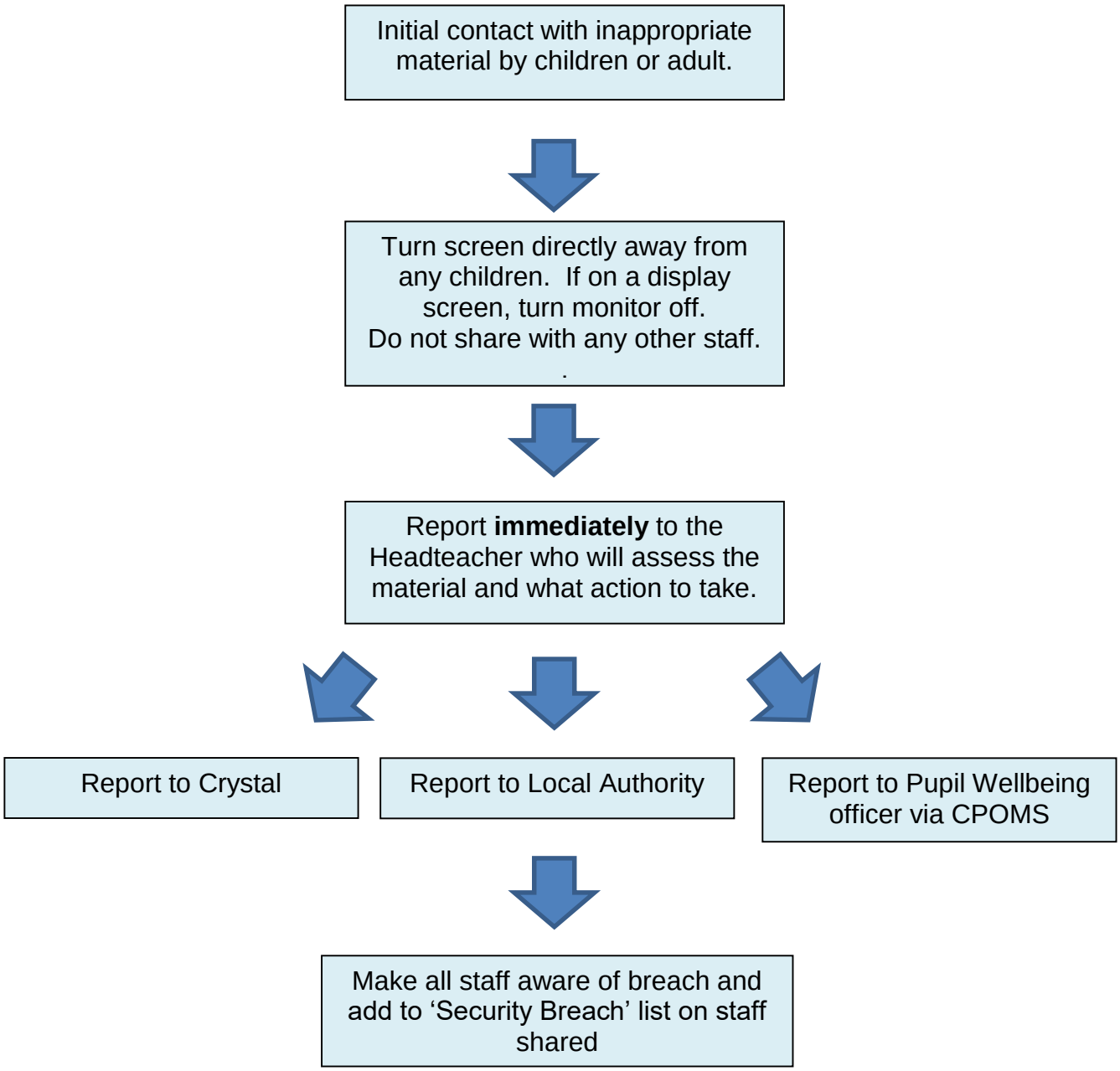
SIMS

- Osmis look after SIMS and do backup & restore.
- The SIMS server has SOPHOS.

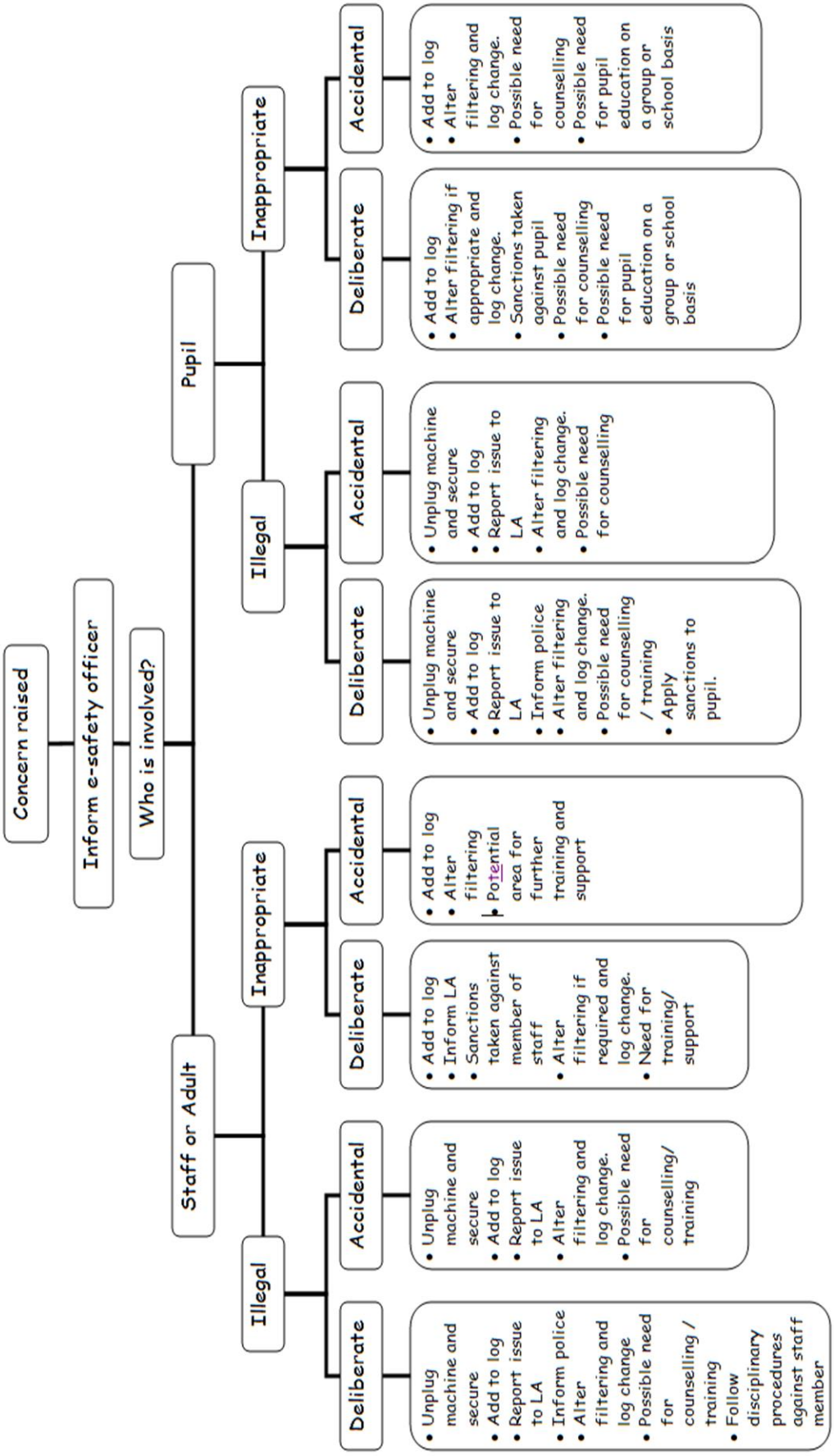
IPADS

Ipads do not have anti-virus. iPhone, iPad and iPod all run on iOS. It is one of the most advanced systems on the market. iOS is secure and stable. You do not need an antivirus to run securely on iOS. Because iOS relies on AppStore. And AppStore has applications that don't have any viruses and are easy to use.

Breach Protocol



Appendix 4 – E-Safety Issues Protocol



Appendix 5

Some Internet and eTechnologies Safety Sites

CEOP (Child Exploitation and Online Protection)

Provides comprehensive information for various groups: 5-7, 8-10, 11-16, Parents and Teachers.

www.ceop.gov.uk

www.thinkuknow.co.uk

BBC: Provides activities, even for very young surfers.

www.bbc.co.uk/chatguide/

www.bbc.co.uk/cbbc/help/safesurfing/

Childnet International: *P*rovides activities and links to a lot of guidance in easy sections.

Jenny's story

Blogging

Lesson Plans and Posters

CD's and support for parents and teachers

Bullying

www.childnet-int.org

National Childrens' Homes: *G*eneral advice on safe Internet use.

www.nch.org.uk

The ***Disney Corporation:*** Has some simple games for younger surfers

www.disney.go.com/surfswell/

BECTA: Provides overall guides and policies for schools and teachers.

www.becta.org.uk

Blackburn with Darwen: The e-learning site has safety and strategy documents.

www.elearningbwd.net

General Advice Sites

www.getsafeonline.org

www.parentcentre.gov.uk

www.gridclub.com