BOURN C of E PRIMARY ACADEMY

IT ACCEPTABLE USE AND ONLINE SAFETY POLICY

Finance/Premises/IT

May 2018

1. Introduction

1.1. The internet and email are now indispensable tools for all School teaching staff, managers, administrators and pupils. The use of these exciting and innovative technology tools in school and at home has been shown to raise educational standards and promote pupil achievement yet while they offer huge potential benefits to improving work efficiency and effectiveness if properly applied, they also pose significant risks for the School.

1.2. This acceptable use/online safety policy provides staff at Bourn Primary with guidance on how to make best use of these technologies whilst understanding the potential dangers. It also gives guidance on how pupils should be using the internet/email at school and how they are taught about online safety. It applies to all users of the School's IT systems.

1.3. A further purpose of this policy is to describe the safeguarding measures in place for adults and children in the School including:

- the ground rules we have developed in the School for using the internet and online technologies;
- how these fit into the wider context of our other school policies;
- the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.

1.4. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using technology, media and information resources, is one the School shares with parents and carers. At Bourn Primary Academy, we feel that the most successful approach lies in a combination of site filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

2. Technology at Bourn Primary Academy

2.1. The School's IT infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN) and the Local Authority's Education ICT Service.

2.2. This infrastructure helps to ensure that staff and pupils rarely encounter material which is inappropriate or offensive. If or when they do, the School's Acceptable Use Agreements and Online Safety education programme ensure that they are equipped to deal with any issues in the most appropriate way.

2.3. Technologies regularly used by pupils and adult stakeholders include:

Staff:

- Laptops and desktops.
- Tablets (iPads).
- Cameras and video cameras, visualisers.
- Internet, E-mail, "its Learning" Learning Platform, the school website, SIMS and confidential pupil information.

Pupils.

- Laptops and desktop PCs,
- Tablets (iPads),
- Cameras and video cameras, visualisers.
- Internet (including the school website).
- Other peripherals such as programmable toys, dataloggers, control technology equipment.

Others on school premises:

- Limited access to School systems such as filtered internet access using a visitor account.

2.4. Whilst we recognise the benefits of individual pupil accounts on our School network, we prefer to use year group accounts for ease of access. All members of staff have individual, password-protected accounts to the School network. Visitors to the school can access part of the network using a generic visitor account and password.

2.5. The School's network can either be accessed using a wired or wireless connection. The wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the Computing Subject Leader.

2.6. School staff (unless expressly approved by the Head Teacher) and pupils are not permitted to connect personal devices to the School's wireless network and the wireless key is not given to visitors to the school. Staff personal devices can only be connected in exceptional circumstances and solely for the purposes of school business. They connect to a restricted wireless service.

3. Teaching and Learning Using Online Technologies

3.1. The internet is a part of everyday life for education, business and social interaction. Benefits of using online technologies in education include:

- access to world-wide educational resources;

- access to experts who would otherwise be unavailable;
- access to anytime – anywhere – learning;
- collaboration across schools, networks of schools and services.

4. Online Safety Issues

4.1. While children and young people need support to keep them safe online, the risks associated with the use of technology are not just restricted to them. Online safety issues can also affect adults who work or are associated with the School; for example, school and personal data being entered on web/social networking sites, fraudulent email traps or cyberbullying. It is impossible to eliminate risk completely. It is therefore essential, through good educational provision to manage the risk and deal with any threat to safety. Some of the dangers include:

- access to illegal, harmful or inappropriate images or other content;
- unauthorised access to / loss of / sharing of personal information;
- the risk of being subject to grooming by those with whom they make contact on the internet;
- the sharing or distribution of personal images without an individual's consent or knowledge;
- inappropriate communication or contact with others, including strangers;
- cyber-bullying;
- access to unsuitable video or internet games;
- an inability to evaluate the quality, accuracy and relevance of information on the internet;
- plagiarism and copyright infringement;
- illegal downloading of music or video files;
- the potential for excessive use which may impact on the social and emotional development and learning of the young person.

5. Safeguarding Children Online

5.1. The School recognises that different users will be expected to use the School's technology systems in different ways, appropriate to their age or role in School. We acknowledge the need to:

Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children.

**UKCCIS (The UK Council for Child Internet Safety) – June 2008*

6. Staff Use of the School's Internet Service

6.1. The School wishes to encourage the use of email and internet by staff in support of their work. Use of these facilities should be appropriate to the work, standards and ethos of the School.

6.2. The use of the School's internet and email systems is not provided as a right to any of the users and may be withdrawn from any user, adult or pupil, who does not conform to this Acceptable Use Policy.

6.3. The School is responsible for authorising the use of its internet or email facilities and monitors their usage.

6.4. Any member of staff who commits a serious offence in the use of the School's internet service may be subject to the School's staff disciplinary procedures.

6.5. Illegal activity using the School's internet service will be reported to the police as necessary.

6.6. Staff should not use the School's email and internet system for personal use during school time, except where specifically authorised by a member of the Senior Management Team.

6.7. Staff or administrative users will protect the School from computer virus attack or technical disruption by not downloading from the internet any programs or executable files other that by agreement with the School's IT technician.

6.8. Staff should protect their passwords to the School's IT systems by not sharing them, by not using obvious passwords which are easy to deduce or by leaving them in an insecure place.

6.9. Staff are not to procure goods or services directly over the internet, except by specific agreement with the Head Teacher.

6.10. If a member of staff sees any unacceptable site or material as a result of an innocent internet query, unsolicited pop-up window or in any other way, it must be reported immediately to the line manager and to Education ICT Service on 0300 3000000. Action can then be taken to block the site or material.

6.11. Staff should at all times abide by the copyright laws in respect of documents and materials downloaded from the internet.

6.12. Staff should be aware of the ethos, standards, equalities and ethnic mix of the School and should not access any internet material, or work with the internet, in any way that infringes or offends these.

7. Staff Email Acceptable Use Statements

7.1. Users of the Local Authority's email service must conform with the Council email code of practice at all times.

7.2. Staff are to check email regularly - ignoring messages is discourteous and confusing to a sender.

7.3. The laws of the land apply equally to electronic messages and documents as they do to paper documents, including the laws relating to defamation, copyright, obscenity, fraudulent misrepresentation, freedom of information, and wrongful discrimination. The content of an email or attachment must never infringe the law of the land and, if sent from the School, should be in accordance with the values and ethos of the School. Sending an email from a School email account is similar to sending a letter on School letter-headed paper.

7.4. Staff are to make sure that their email address is included on any contact information put onto paper-based letters or documents.

7.5. All email communication between staff and members of the School community on School business must be made from an official School email account. Staff and volunteers must never give out their personal details, such as home/mobile phone numbers, home address or personal email address.

7.6. Any email received by a member of staff which is regarded as illegal or offensive should be reported to the Head Teacher immediately.

7.7. To safeguard against computer viruses, staff are not to open external emails or attachments that look in any way suspicious but rather are to report these to the School's IT Co-ordinator for checking.

7.8. Unless a member of staff is specifically authorised to do so, no email should be sent to any supplier that could be interpreted as creating a contract in any way. NOTE: Within the law, a user could send an email containing certain wording which may form a legally binding contract with a supplier.

7.9. Attachments in emails containing files with extensions of "exe", "com" or "bat" are not to be opened, unless it is absolutely certain that the file has come from a trusted source. All such files must be thoroughly virus checked before they are opened.

7.10. Staff are not to attempt to read another person's email.

7.11. See the Data Protection & Record Management Policy for further comments on the safe use of email.

8. Use of School laptops and other media outside of School

8.1. The use of School laptops and School software at home for personal reasons should be limited and appropriate and is at the discretion of the Head Teacher. Usage outside School is limited to teachers, the School Business Manager and, when necessary, the IT technician.

8.2. Staff may not remove or copy sensitive or personal data from the School unless the medium (hard drive, usb stick or other storage device) is encrypted.

8.3. Staff using a School laptop or other device off the School site, at home or elsewhere, are still bound by the School's Acceptable Use Policy. The misuse of such devices for activity not agreed to by the School may be breaking the law under the Computer Misuse Act (1990).

9. Use of Cloud Storage

9.1. Staff should not store any School data in the cloud unless agreed to by the Head Teacher or the IT Technician. Note that School information about children must, by law, be saved only on computers residing in the European Union, and this requirement must be carefully assessed if cloud storage is chosen.

10. Social Contact and Social Networking

10.1. Staff must not post material which damages the reputation of the School or which causes concern about their suitability to work with children and young people. Those who post material which could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct.

10.2. School staff will not invite, accept or engage in communications with parents or children from the School community on any social media channels, including networking sites or blogs, whilst in employment at Bourn Primary Academy.

10.3. Staff should not accept any current pupil of any age or any ex-pupil of the School under the age of 18 as a friend, subscriber or similar on any personal social media account. If a pupil seeks to establish social contact, or if the contact occurs, the member of staff should exercise their professional judgment in making a response and be aware that such social contact in person, by phone or on the internet, could be misconstrued and may place the member of staff in a very vulnerable position. A member of the Senior Management Team should be made aware of any such communications or connections.

10.4. If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported to the Head Teacher.

10.5. Members of the School staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.

10.6. Staff must avoid posts or comments that refer to specific, individual matters related to the School and members of its community on any social media channels.

10.7. Staff are also advised to consider the reputation of the School in any posts or comments on any social media channel. Parents and students may access staff profiles online and could, if they find offensive information and/or images, complain to the School.

10.8. Staff should always make sure that they log out of any social media website after using it, particularly when using a machine that is shared with other users. Accounts can be hijacked by others if the user remains logged in – even if the browser was closed and the machine switched off.

11. School Mobile Phone

11.1. The School mobile phone should be used on any trip outside School and should be the only phone used when conducting School business with pupils and parents outside School.

11.2. The phone should not be used for anything but School business.

12. Community/Third-Party Use of the Internet

12.1. As part of its role as a community school, the School can, at its discretion, allow third parties to make use of its IT equipment.

12.2. This usage will be limited to internet access only, making all School-specific data such as curriculum resource and pupil work unavailable to them. The School email system will also be unavailable.

12.3. If a third-party user sees any unacceptable site or material as a result of an innocent internet query, unsolicited pop-up window or in any other way, the screen should be removed from view by switching off the monitor but leaving the computer on to preserve the offending internet address. It should be immediately reported to the Computer Subject Leader or member of the Senior Management Team straight away.

12.4. Third parties are expected to keep private any account details the School provides them with.

12.5. Third parties may not install software onto the School's computers.

12.6. Third parties may not remove any of the School's IT equipment from the School premises.

12.7. If there is any doubt as to best practice when using the School's IT equipment and / or accessing websites, third-party users must first contact the Head Teacher or IT Technician for clarification.

12.8. All third-party users will be supplied with a copy of this document.

13. Online Safety Curriculum

13.1. In line with recommendations in the e-safety briefing for Ofsted Inspectors (Sept 2012), the School has a range of age-related teaching and learning opportunities to help the pupils to become safe and responsible users of new technologies. These opportunities include:

- regular whole school assemblies;
- specific activities during Safer Internet Day (traditionally held in February);
- age-related classroom activities using the ThinkUKnow materials;
- related work in PSHE lessons;
- posters and reminders in and around the school and on the desktop screens of pupil laptops, PCs and tablets.

14. Keeping Pupils Safe Online

14.1. Members of staff constantly monitor pupils' use of the internet and other technologies. Our programme for Online Safety education is evidenced in teachers' planning either as discrete or embedded activities.

14.2. Staff will explicitly teach the importance of online safety to the children during Computing and PSHE lessons and refer to key points as part of the teaching throughout the year, using age-appropriate language. Messages involving Risks and Rules and Responsibilities are taught and/or reinforced as detailed in the school's Acceptable Use Agreements.

14.3. Younger pupils will not be able to use the internet unsupervised.

14.4. Online Safety is of the highest priority for pupils, and the county broadband supplier, E2BN, applies filters to Bourn Primary pupil connections in order to remove inappropriate material. However, there are still opportunities for inappropriate material to remain undetected by these filters, and vigilance by teachers is paramount.

The statements below represent a series of best practices teachers should use to minimise the likelihood of incidents.

14.5. When preparing internet material for pupils to view, teachers should be aware that, because their accounts are filtered for inappropriate content, this can occasionally mean that online material accessible using a teacher account (and considered safe) may not be available to pupil accounts.

14.6. Focused search tasks should be used rather than very open research tasks for younger pupils, to ensure that accidental access to inappropriate websites is reduced.

14.7. Should pupils be asked to perform any "open searches", these should be checked in advance to minimise the opportunities for any mis-spellings by the children, which may cause inappropriate material to be found.

14.8. Searches for images may return inappropriate results, as pictures are not easy to filter accurately. These searches should be thoroughly tested first, certainly beyond the first page of results.

14.9. Sites known to be child-safe or those saved to "Favourites" should be used whenever possible, to reduce accidental access to other sites.

15. Pupil Use of School Internet and Email – Online Safety

15.1. Within Online Safety, pupils should be taught and know:

- what to do if they accidentally find an unsafe site while using the internet;
- not to use any personal information such as their real name or address at any time when emailing or using the internet (e.g. at home or School) and the reasons why this could be unsafe;

- to involve teachers, parents and carers whenever they are communicating with people they do not know;
- to use the internet responsibly and to speak to their teacher, parents or carers if they feel unsure or unsafe;
- that web sources could be unreliable and inaccurate, to check their information against other sources and not to rely on just one information source.

16. Online Bullying

16.1. Pupils should be made aware of the existence of online bullying and that, if they feel they are the victim of online bullying, they should approach a parent/carer or a member of staff to let them know.

16.2. Should it become clear that a pupil is behaving inappropriately online, this behaviour will be dealt with as described in the Positive Behaviour Policy.

17. Responding to Online Safety Incidents

17.1. It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an Online Safety incident occurs or they suspect a child is at risk through their use of technology. It is important that responses to Online Safety incidents are consistent with responses to other incidents in School. This may mean that serious actions have to be taken in some circumstances.

17.2. If an Online Safety incident occurs, Bourn Primary Academy will follow its agreed procedures for dealing with incidents including internal sanctions and involvement of parents (for IT, this may include the deactivation of accounts or restricted access to systems as per the School's Acceptable Use Agreements). Where the School suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed.

17.3. If a pupil finds an unsafe site during lesson time, the screen should be removed from the children's view, either by switching off the monitor or by removing the entire device. In either case, leave the computer on so that a note can be made of the web address. In the first instance this should be reported to the Computing Subject Leader straight away. The Computing Subject Leader will pass this to the child protection Designated Person if appropriate. Appendix B gives an overview of this procedure. The Computing Subject Leader should arrange for an email to be sent to the IT Service informing them of the site so that future access can be prevented.

18. Dealing with Incidents and Seeking Help

18.1. If a concern is raised, refer immediately to one of the designated persons for child protection – the Head Teacher, Deputy/Assistant Head or, if necessary, the Chair of Governors.

18.2. It is their responsibility to:

Step 1: Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator

Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate. If in doubt they should consult the Education Child Protection Service helpline.

Step 3: Ensure that the incident is documented using the standard child protection Log of Concern form.

18.3. Depending on the judgements made at steps 1 and 2 the following actions should be taken:

Staff instigator – follow the standard procedures for Managing Allegations against a member of staff. If unsure seek advice from the Local Authority Designated Officer or Education Officer.

Staff victim – Seek advice from your Human Resources (HR) provider and/or Educational Child Protection Service.

Illegal activity involving a child – refer directly to Cambridgeshire Constabulary – 0845 456 4564 – make clear that it is a child protection issue.

Inappropriate activity involving a child – follow standard child protection procedures. If unsure seek advice from Education Child Protection Service helpline.

18.4. Equally, if the incident involves or leads to an allegation against a member of staff, the School will follow the agreed procedures for dealing with any allegation against a member of staff (see Statement of Procedures for Dealing with Allegations of Abuse Against Teachers and Other Staff and Volunteers).

19. Pupils' Acceptable Use Agreement

19.1. Appendix A of this document – Bourn Primary Academy Pupil Acceptable Use Agreement / e-Safety Rules and Pupil e-Safety Recommendations - is intended for Bourn Primary pupils and should be discussed by class teachers with their classes.

20. Pupils' Personal Mobile Phones

20.1. While at school pupils are not allowed to use any forms of electronic communication other than those offered by the School, which are currently email and the internet.

20.2. Any use of privately-owned communication media, for example mobile phones, is expressly forbidden and as such is not covered by this policy. However, if there are special circumstances where children may be allowed to bring in devices with a communications facility as part of their learning (e.g. tablets) then express permission must be sought from the parents of those children on a case-by-case basis.

21. Photography

21.1. Parental permission is sought at the start of the academic year to allow photographs, or examples of pupils' work, to be published on the School website or other instances in the public domain. Where there are specific circumstances e.g. magazine or newspaper publication, permission will be confirmed on a case-by-case

basis. Efforts should be made to ensure that parents understand the implications before giving permission.

21.2. On no account should either first names or surnames be attached to photographs of children which are published online. Care must be exercised that the filename or metadata of a photograph (e.g. janesmith.jpg) does not inadvertently identify a child.

21.3. The members of staff maintaining the School website should ensure that all images on the website, but especially those of children, are of low resolution.

21.4. Guidelines for parents/carers taking photographs are made clear at events. Images taken by parents/carers are for personal use only and are not to be published online.

21.5. **Press Coverage**

21.5.1. Press coverage is encouraged where this builds confidence, pupil esteem or positive images in the community but the School, staff, pupils and children are reminded they have a right to refuse publication of an item if it is not in the best interests of the School or the individual or will breach privacy.

21.5.2. The School will ensure specific parental consent is gained in advance for any events to which the press is invited to photograph individual pupils.

21.5.3. The School will refuse to allow images to be taken by journalists/others who attend the School without invitation.

21.5.4. Head Teachers are within their rights to not give full pupil names or personal information to go with photographs of pupils for the media.

21.5.5. The School will not sign blanket consent forms from media; instead specific details of photographs being taken and used should be insisted upon.

22. Online Safety – Information for Parents/Carers

22.1. Parents/carers should be made aware of the risks of internet and email usage in order that they can take precautions at home. The School now holds two-yearly Safer Internet events to coincide with the national Safer Internet Day. These sessions allow parents to understand the risks posed by a range of internet-enabled hardware, including phones, PCs and gaming consoles.

22.2. Furthermore, the School regularly advises parents and carers about the importance of online safety by making information available through accessible channels such as newsletters and the School website. A dedicated page on computer safety can be found here:

http://www.bournschool.co.uk/pupils/online-safety/

23. References

- Safeguarding and Child Protection Policy
- Prevent Policy
- SRE Policy

- Positive Behaviour Policy
- Anti-bullying Policy
- Data Protection and Record Management

Appendix A

Bourn Primary Academy Pupil Acceptable Use Agreement / e-Safety Rules

- ✓ I will only use IT in School for School purposes.
- ✓ I will only use my class email address or my own School email address when emailing.
- ✓ I will only open email attachments from people I know, or whom my teacher has approved.
- ✓ I will not tell other people my IT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all IT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a School project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe
- ✓ I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the School community
- ✓ I know that my use of IT can be checked and that my parent/ carer contacted if a member of School staff is concerned about my e-Safety.
- ✓ I know that I'm not permitted to carry a mobile phone in School and if I come to School with a mobile phone, it must be switched off and handed into the School office at the start of the day. It will remain there until I leave the School, even if I attend After-School activities.
- ✓ If I have a phone or other mobile device on me during the day, it will be confiscated and my parents will be informed.

Bourn Primary Academy

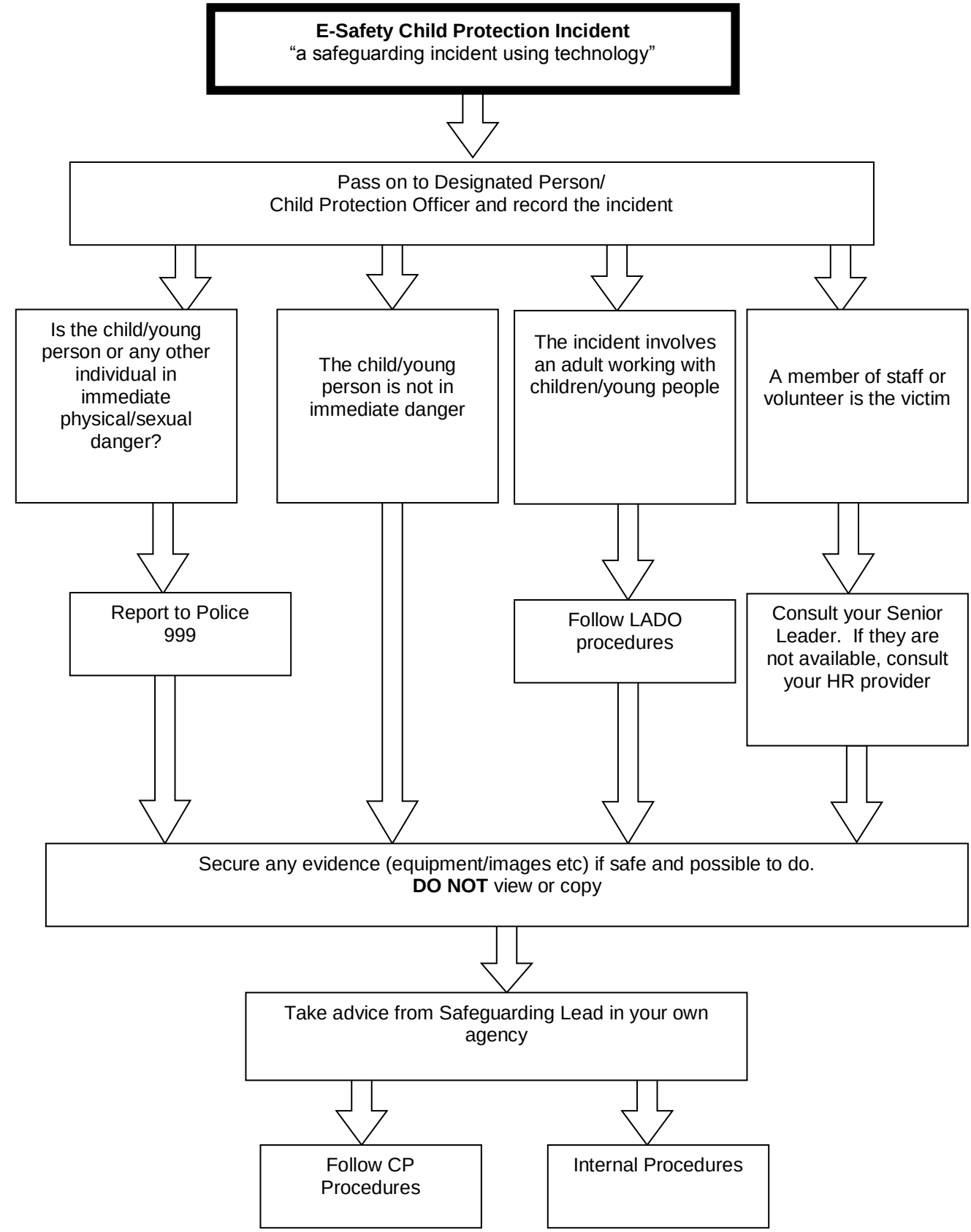
Pupil e-safety recommendations for Parents/Carers

We recommend that Parents/Carers go through these recommendations with their children to assist with their e-safety in and outside School.

- ✓ Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school name, IM address, email address, names of friends, specific interests and clubs etc.
- ✓ Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in photographs which could identify the student or his/her location e.g. house number, street name, school, shopping centre.
- ✓ Pupils are strongly advised to ensure any social media apps they use at home have personal settings set to "Private" and that location services are turned off on any mobile devices. Parents/Carers should help with this, if needed.
- ✓ Pupils should not use an obvious user name and should ensure their privacy is maintained when creating user names.
- ✓ Pupils should be careful of online chat environments even if they exist as part of a game environment and should close connections if they do not recognise an individual who approaches them.
- ✓ If pupils discover unsuitable sites, they should tell their parents/carers immediately, or their teacher if at school.
- ✓ Parents/Carers should make regular checks to ensure that the filtering methods selected on the home router are appropriate, effective and reasonable and should always use their vigilance to ensure pupil safety. The School does the same for the School site.

Appendix B
E-Safety Child Protection Incident – procedure overview

You come across a child protection concern involving technology, then:



Throughout this process, please ensure that all those involved are supported appropriately