The Bliss Charity School
ICT/E-Safety Policy

Mission Statement
The Bliss Charity School aims to provide a caring, secure and enriching experience; each child is encouraged to develop strong personal, academic, physical and creative skills for lifelong learning.

Sections

SECTION 1

ICT at The Bliss Charity School

What is Information and Communications Technology?
Information and communication technology (ICT) prepares pupils to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology. Pupils use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and with discrimination. They learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of people, communities and cultures. Increased capability in the use of ICT promotes initiative and independent learning; with pupils being able to make informed judgements about when and where to use ICT to best effect, and consider its implications for home and work both now and in the future."
*(*National Curriculum for England DfE/QCA 1999)

We believe that Information and Communications Technology (ICT) is about providing children with the ability to adapt to change. It provides access to all subjects and is a highly motivational medium. We interpret the term 'information communication technology' to include the use of any equipment which allows users to communicate or manipulate information (in the broadest sense of the word) electronically.

ICT appeals to children because it is new and fun. It gives them access to a world of information and prepares them for the technological age. It also provides additional methods of communication for a range of purposes.

At The Bliss Charity School, we believe that ICT enhances teaching because it motivates, is enjoyable and reduces teacher workload.

Why is ICT special in our school?
ICT gives all children access to education. All children at The Bliss Charity School will have access to the ICT resources. ICT at our school will be imaginative, enjoyable, varied and cutting edge. ICT will be used in all subjects where its use will enhance the learning objectives. It will support and aid learning throughout the curriculum.

Our aims for ICT are to enrich learning for all pupils and to ensure that all staff develop confidence and competence to use ICT to effectively enhance all subjects throughout the primary curriculum.

Entitlement
The Bliss Charity School uses the Rising Stars scheme of work, 'Switched On Computing', and this is adjusted to ensure that it fits in with our cross-curricular planning. Laptops and ipads are timetabled for use in conjunction with classroom computers to ensure that all children have access to a computer between two or three children and can practice the skills learnt in ICT lessons – a minimum of once a week. Where possible, ICT will be taught as part of an integrated curriculum in accordance with the schools agreed long term curriculum mapping. Where a lesson includes ICT skills as well as those of another subject, the planning will indicate both sets of objectives. In some instances, it may not be possible to fully integrate ICT with other subjects and so some units or objectives may need to be taught as discrete units.

The integration of ICT with other subjects is important because it highlights the important uses of particular ICT skills in other subjects and parts of life.

Some links with other subjects have been identified by matching the appropriate ICT unit with suitable subjects in our long term planning maps. ICT is used wherever it enhances the learning objectives being taught. We feel that ICT can be used in all subjects and where used effectively, it enhances the learning experience.

Learning and Teaching
In ICT lessons, teachers make clear the ICT objectives and discuss success criteria with children. Teachers use the interactive whiteboard to demonstrate the objective before allowing children to demonstrate on the whiteboard and practice the skills in individually differentiated activities. At the end of the lesson, the plenary allows the teacher to evaluate learning objectives and success criteria with children. The plenary also allows opportunities to discuss how these skills may be used in other lessons and on other occasions.

Learning support assistants are involved with the teacher in planning the ICT activities and supporting children to either advance their skills further or to give children access.

When working on the computers, laptops or ipads children work in pairs or threes. On some occasions, children will work in mixed ability pairs, while on other occasions children will work with other children of a similar ability to avoid dependence on more able peers. When necessary for assessing pupil progress, children work individually to give a clear picture of their individual capabilities.

Access to ICT
All computers are linked to the printer/copier in the office via the school wireless system. Each class has digital cameras. The computers are linked together using the Easi Server system. Each class also has additional sockets to enable additional computers to be used in the room.

To enable whole class use of computers, 15 laptop computers, are stored in a trolley and a converted cupboard where they are charged overnight. Each class has a timetabled ICT session. When they are not timetabled, other classes may book in to use some or all of the computers in other lessons.

The school also has two sets of ipads, stored in their own charging case/trolley. Each class has timetables use of the ipads during their ICT slot. When they are not timetabled, other classes may book in to use some or all of the ipads in other lessons.

All teaching staff have their own laptop for use both in school and at home. Each classroom is equipped with an interactive whiteboard and interactive pens for use with the whiteboard.

Inclusion
All pupils, regardless of race or gender, shall have the opportunity to develop ICT capability. The school will promote equal opportunities for computer usage and fairness of distribution of ICT resources. Children with a computer at home are encouraged to use it for educational benefit and parents are offered advice about what is appropriate using the school website.

The school will monitor the level of access to computers in the home environment to ensure no pupils are unduly disadvantaged. Groupings for computer usage will generally follow the same pattern as for all lessons. It is appropriate to match pairs of equal ability, rather than have a more able ICT users always guide a less able pupil. This generally leads to passivity and dominance. However it is appropriate to plan to have peer tutors for some lessons where the objectives also enable the more able user to learn by specifically teaching.
Positive images of computer use by people of both sexes will be promoted. The school recognises the advantages of the use of ICT by children with special educational needs.
Using ICT can:

- address children's individual needs
- increase access to the curriculum
- enhance language skills

Staff will structure their teaching materials to match a learning difficulty. If the situation arises, the school will endeavour to buy appropriate resources to suit the specific needs of the child.

Assessment and Recording
The statutory requirements are that progress is reported to parents annually. Teachers report ICT progress to parents in the annual reports issued in July, commenting on progress throughout the year.

We keep a portfolio of pupil work on the school computer system to demonstrate use of ICT throughout the school. Each pupil has their work stored in an individual folder, which at the end of the year is moved up to the next class as a continuing record of ICT achievement. This enables class teachers to see the level of work produced by each child in their class.

ICT work will be marked in accordance with the school policy for marking. Where it is not necessary for work to be printed out, teachers will give verbal feedback to pupils in the place of written comments.

Monitoring and Review
Monitoring is carried out by the Headteacher, the ICT subject leader and the ICT Governor, in the following ways:

- Informal discussion with staff and pupils
- Collection of class ICT files stored on computer
- Looking at the work in children's individual folders
- Classroom observation
- Collection and scrutiny of medium and short term planning for ICT
- Collection and scrutiny of medium and short term planning for other subjects to observe cross-curricular use of ICT
- Questionnaires to pupils, staff, parents and governors where appropriate

Health and safety/ Security
When setting up and using the laptops, all wires and cabling will be placed around the outside of the room, with no overhanging wires which may represent a tripping hazard.

Children will also be made aware of the correct way to sit when using the computer and the need to take regular breaks if they are to spend any length of time on computers. Children and staff are made aware that they will not look directly into the beam of the overhead projector to avoid risk of serious and permanent damage to their eyes.

The Health and Safety at Work Act (1 January 1993), European Directive deals with requirements for computer positioning and quality of screen. This directive is followed for all administration staff. Whilst this legislation only applies to people at work we seek to provide conditions for all children which meet these requirements.

The school has an alarm system installed throughout. Each computer system has individual security against access to the management system. The files and network system are backed up regularly. The virus checker is updated regularly.

Internet Safety
This policy contains an 'Acceptable Use' section which outlines our practice with regards to safe use of the internet.

Home school links
The school website at www.bliss.northants.sch.uk is maintained by Mrs Howard in the office.

The website also has a curriculum page which informs parents of the areas taught in each subject throughout the school year, with some useful links to websites provided.

Other methods of enhancing home school links via the website are:

- The school newsletter is available from the 'parents/newsletters page.
- Events are photographed and details added.
- Governor information page showing updates from governor meetings.
- Displays are photographed and shown in the gallery section.
- The school council minutes can be accessed from the homepage.
- Policies, the prospectus and other documents can be accessed from the website.

The use of the website will be monitored by the Subject Leader to ensure that it is updated regularly.

A letter is sent out to parents, when their child starts school, to ask for permission for photographs of their children to appear on the website – only those who are permitted are allowed to appear. When naming children, only first names and the initial letter of the surname (if needed) will be used. Addresses and other details of children will not be shown on the website.

Curriculum Management
The Subject Leader will facilitate the use of Information and Communication Technology in the following ways:

- By updating the policy and scheme of work;
- By ordering/updating resources;
- By providing INSET so that all staff are confident in how to teach the subject and have sufficient subject knowledge;
- To keep staff abreast of new developments;
- By taking an overview of whole school planning to ensure that opportunities occur for pupils to develop an information and communication technology capability and that progression is taking place;
- By supporting staff in developing pupils' capability;
- By attending appropriate courses to update knowledge of current developments, and by keeping links with the LA Advisory Team for Information and Communication Technology;
- By contributing to the School Improvement Plan on an annual basis
- By management of the technician's job book.
- Making sure all staff understand system for logging faults and use of the Internet/email
- Monitoring the curriculum
- Maintaining records of software licences and their deployment.

Provision of technical support
The Bliss Charity School receives technical support from Easipc on a four weekly basis. Jobs for the technician are recorded in a book in the office, the ICT Subject Leader also asks all staff for any additional jobs the day before the technician comes into school. Easipc also support the school with differential filtering.

Maintenance and repair cycle
Our school has a three year planned cycle for the replacement of hardware and software, to ensure that our technology is kept up to date.

Copyright and licensing
All software is used in strict accordance with the licence agreement. Licence documents are stored together in the school office.

Personal software is not loaded onto school computers – new software is purchased with the appropriate licence.

Refer to the Copyright Designs and Patents Act 1988 and the 1991 European Software Directive for more details.

SECTION 2

Acceptable use policy – general

Sections of this policy has been developed by the Children and Young People's Service in consultation with Education Welfare - CYPS, Northamptonshire Police, the Northamptonshire Safeguarding Children's Board, Governors, Parents/Carers and Children, and in partnership with Professional Associates.

What is an AUP (Acceptable Use Policy)?
An Acceptable Use section sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard adults, children and young people within our school. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate development within ICT. At present the internet technologies used extensively by young people in both home and school environments include:

- Websites
- Social Networking and Chat Rooms
- Gaming
- Music Downloading
- Mobile phones with wireless connectivity
- Email and Instant Messaging
- Learning Platforms
- Video Broadcasting

Despite there being significant educational and social benefits associated with the use of these technologies, there are risks which need to be emphasised to all users and steps taken to safeguard against them. The policy will also provide support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies beyond the school or educational setting. It explains procedures for any unacceptable use of these technologies by adults, children or young people.

Why have an AUP?
The use of the internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children access these technologies.

The risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or any mobile device.
- Viruses.
- Cyber-bullying.
- Sexting the sending of indecent personal images, videos or text via mobile phones for private viewing. Can potentially be widely distributed and publicly viewed.
- On-line content which is abusive or pornographic As part of the Every Child Matters agenda set out by the government, the Education Act 2004 and the Children's Act, it is the duty of schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of on-line technologies. This policy aims to explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also informs as to how children and young people are educated to be safe and responsible users capable of making good

judgements about what they see, find and use. The term 'e-safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

1.0 Aims

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school or other educational settings.
- To provide safeguards and rules for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

2.0 Roles and responsibilities of The Bliss Charity School

2.1 Governors and Headteacher

It is the overall responsibility of the Headteacher (Shaun Carter) with the Governors to ensure that there is an overview of e-Safety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:

- The Headteacher is the designated e-Safety Leader to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of who holds this post within the school.
- Mrs Morse and Mrs Newton have been trained as Higher Level E-Safety Officers.
- Time and resources will be provided for the e-Safety Leader and staff to be trained and update policies, where appropriate.
- The Headteacher is responsible for promoting e-Safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Headteacher will inform the Governors at the Curriculum meetings about the progress of or any updates to the e-Safety curriculum (via PSHE or ICT) and ensure Governors know how this relates to child protection. At the Full Governor meetings, all Governors are to be made aware of e-Safety developments from the Curriculum meetings.
- The Governors **MUST** ensure Child Protection is covered with an awareness of e-Safety and how it is being addressed within the school, as it is the responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.
- The e-Safety Governor is Graham Hotchkiss and he will challenge the school about having an AUP with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including:

Challenging the school about having:

- Firewalls
- Anti-virus and anti-spyware software
- Filters
- Using an accredited ISP
- Awareness of wireless technology issues
- A clear policy on using personal devices.

Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures (see the Allegation Procedure – Section 12 Safeguarding Children's Board)

2.2 E-Safety Leader

It is the role of the designated e-Safety Leader **Mrs Dani Newton,** to:

- Appreciate the importance of e-safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe ICT learning environment within the school.
- Ensure that the AUP is reviewed annually, with up-to-date information available for all staff to teach e-Safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-a-lone PC, staff/children laptops and the learning platform.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people and also how to make requests to change filters.
- Report issues and update the Governors on a regular basis.
- Liaise with the PSHE, Child Protection and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.
- Transparent monitoring of the internet and on-line technologies
- Keep a log of incidents in the behaviour folder, including e-safety concerns, for analysis to help inform future development and safeguarding, where risks can be identified. These concerns will also be stored on SIMS. Refer to Appendix B and Section 12 of the Allegation Procedure from the NSCB to ensure the correct procedures are used with incidents of misuse (website in Appendices).
- Work alongside the ICT Leader, to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised Ensure there is regular monitoring of internal e-mails, where:
    - Blanket e-mails are discouraged
    - Tone of e-mails is in keeping with all other methods of communication
    - Report overuse of blanket e-mails or inappropriate tones to the Headteacher and/or Governors.

2.3 Staff or adults - people who hold a position of power and trust

It is the responsibility of all adults within the school or other setting to:

- Understand that they hold a position of power and trust and therefore act accordingly.
- Ensure that they know who the Designated Person for Child Protection is within schools (Shaun Carter, Olivia Thompson, Sharon Simpson, Sue Caller and Lynn Adey) so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it will be reported immediately to the Headteacher/Safeguarding lead. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately. (Following the Allegation Procedure, Section 12, NSCB.)
- Be familiar with the Discipline, Anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the Headteacher/Safeguarding lead immediately, who will then follow the Allegations Procedure, Section 12, NSCB, where appropriate.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the e-Safety Leader.
- Alert the e-Safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people will know what to do in the event of an incident.

- Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Have read the Acceptable Use Policy for School Based Employees to show that they agree with and accept the rules for staff using non-personal equipment, within and beyond the school environment, as outlined in appendices.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998.
- Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- School bursars will need to ensure that they follow the correct procedures for any data required to be taken from the school premises.
- Report accidental access to inappropriate materials to the e-Safety Leader and Mrs Howard in the office who will report it to Exa helpdesk in order that inappropriate sites are added to the restricted list.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school/educational setting's network.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the internet or other technologies using the NCC accident/incident reporting procedure in the same way as for other non-physical assaults.
- When teaching an email lesson, teacher must spot check at least three emails to ensure that the content is appropriate.

2.4 Children and young people

Children and young people should be:

- Responsible for following the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school or setting for the first time.
- Taught to use the internet in a safe and responsible manner through ICT, PSHE or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

3. Appropriate and Inappropriate Use

3.1 By staff or adults

- Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.
- They have a password to access a filtered internet service and know that this will not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.
- All staff will receive a copy of the Acceptable Use Policy, (Appendix C) which then need to be signed, returned to school.
- The Acceptable Use Rules will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations.
- The acceptable use will be similar for staff to that of the children and young people so that an example of good practice can be established.
- All staff equipment will be audited annually by EasiPC.

In the event of inappropriate use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher/safeguarding lead immediately and then the Allegations Procedure (Section 12, NSCB) and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

3.2 By Children or Young People

Acceptable Use are outlined in the Appendices. These detail how children and young people are expected to use the internet and other technologies within school. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The Bliss Charity School encourages parents/carers to support the rules with their child or young person. This is shown by signing the Acceptable Use Rules together so that it is clear to the school or setting that the rules are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the internet beyond school.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free. File-sharing via e-mail, weblogs or any other means on-line will be appropriate and be copyright free when using the learning platform in or beyond school.

In the event of inappropriate use

Should a child or young person be found to misuse the on-line facilities whilst at school, or in a setting, the following consequences will occur:

- Any child found to be misusing the internet by not following the Acceptable Use Rules may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the rules may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.
- A letter may be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, e.g. use 'Hector Protector', for example, (dependent on age) so that an adult can take the appropriate action.

Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing on-line technologies will also be addressed by the school.

Children will be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

The report history will be accessed monthly by EasiPC and monitored for inappropriate use.

4 The curriculum and tools for Learning

4.1 Internet use – also see Internet section

The Bliss Charity School will teach children and young people how to use the internet safely and responsibly. They will also be taught, through ICT, metacognition and P4C/SEAL lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies will have been taught by the time they leave Year 6:

- Internet literacy
- making good judgements about websites and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger

- access to resources that outline how to be safe and responsible when using any on-line technologies
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading information – know what is safe to upload and not upload personal information where to go for advice and how to report abuse
- how to stay safe online

The Rising Stars ICT Scheme of Work, 'Switched On Computing', is used to teach internet and e-mail lessons from Years 1 to 6. E-Safety lessons and resources can also be found at www.thinkuknow.co.uk for KS1 and KS2. These skills and competencies are taught within the curriculum so that children and young people have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner. Children and young people should know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information such as:

- full name (first name is acceptable, without a photograph)
- address
- telephone number
- e-mail address
- school
- clubs attended and where
- age or DOB
- names of parents
- routes to and from school
- identifying information, e.g. I am number 8 in the Youth Football Team

Photographs will only be uploaded on the approval of a member of staff or parent/carer and will only contain something that would also be acceptable in 'real life'. Parents/carers should monitor the content of photographs uploaded. Images of children and young people will be stored according to policy.

4.2 Pupils with additional learning needs

The Bliss Charity School strives to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

4.3 E-mail use

The school have e-mail addresses for children to use, as individuals as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.

Individual email accounts can be traced if there is an incident of misuse whereas class email accounts cannot, especially for older users.

Staff, children and young people to use their school issued email addresses for any communication between home and school only. A breach of this may be considered a misuse.

Parents/carers are encouraged to be involved with the monitoring of emails sent, although the best approach with children and young people is to communicate about who they may be talking to and assess risks together.

4.4 Mobile phones and other emerging technologies **– also see iPad section**

The Bliss Charity School carefully considers how the use of mobile technologies can be used as a teaching and learning tool within the curriculum with the following areas of concern to be taken into consideration:

- *inappropriate or bullying text messages*
- *images or video taken of adults or peers without permission being sought*
- *'happy slapping' – the videoing of violent or abusive acts towards a child, young person or adult which is often distributed*
- *Sexting- the sending of suggestive or sexually explicit personal images via mobile phones*
- *Wireless internet access which can bypass school filtering and allow access to inappropriate or potentially harmful material or communications.*

Children may bring mobile phones or PDA devices to school in exceptional circumstances but may not use them during school hours. They will be left in the office. We have considered the increased incidents of bullying and misuse which have been reported where students are allowed to use them in school. Where inappropriate usage of said technologies does occur, a virtual paper trail may be traceable, even if the message received is sent anonymously.

(i) Personal mobile devices –

- Staff are allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers to contact children and young people under any circumstances.**

- Staff must ensure that there is no inappropriate or illegal content stored on the device and will be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras (see 7.6 for further details)
- Staff will be aware that games consoles such as the Sony Playstation, Microsoft Xbox and other such systems have Internet access which may not include filtering. Before use within school, authorisation will be sought from the Headteacher and the activity supervised by a member of staff at all times.
- The school is not responsible for any theft, loss or damage of any personal mobile device.

(ii) School issued mobile devices –

The management of the use of these devices is similar to those stated above, but with the following additions:

Where the establishment has provided a mobile device to a member of staff, such as a laptop, PDA or mobile phone, only this equipment will be used to conduct school business outside of the school environment. It will also be policy to ensure that children and young people understand the use of a public domain and the consequences of misuse. Relevant curriculum links will be made to highlight the legal implications and the involvement of law enforcement.

Other technologies which schools and settings use with children and young people include:

- photocopiers
- fax machines
- telephones

4.5 Video and photographs **– see AUP of cameras and video equipment**

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in school there is access to cameras in each class and a spare available in the office.

It is not appropriate for staff to use their personal mobiles or other personal equipment. All images are stored on the school network not on individual teacher's laptops.

It is also highly recommended that permission is sought prior to any uploading of images to check for inappropriate content.

The sharing of photographs via weblogs, forums or any other means on-line will only occur after permission has been given by a parent/carer or member of staff.

Any photographs or video clips uploaded will not have a file name of a child, first name only, especially where these may be uploaded to a school website.

Group photographs are preferable to individual children and young people and will not be of any compromising positions or in inappropriate clothing. Photographs are stored on the Public (P drive) which can be viewed by anyone in school on the network system and they will be removed to archive at the end of the school year.

4.6 Video-conferencing and webcams (including Skype)

The use of webcams to video-conference will be via Exa Broadband which is a filtered service. Publicly accessible webcams are not used in school. Taking images via a webcam will follow the same procedures as taking images with a digital or video camera.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Rules.)

5. Web 2.0 Technologies

5.1 Managing Social Networking and other Web technologies

Social networking sites have emerged in recent years as a leading method of communication proving increasingly popular amongst both adults and young people alike. The service typically offers users both a public and private space through which they can engage with other online users, and express themselves creatively through images, web content and their own personal profile page. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with young people, there are a number of risks associated which must be addressed. With this in mind, both staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook, MySpace and Bebo.) In response to this issue the following measures have been put in place:

- The school controls access to social networking sites through existing filtering systems.
- Students are advised against giving out personal details or information which could identify them or their location (e.g. mobile phone number, home address, school name, groups or clubs attended, IM and email address or full names of friends.)
- Students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos which could reveal personal details (e.g. house number, street name, school uniform)
- Pupils are advised on social networking security and recommendations made for privacy settings to be activated to ‘Friends only’ for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- The staff remind children and parents of the age restrictions associated with social media.
- The school is aware that social networking can be a vehicle for cyberbullying. Pupils are encouraged to report any incidents of bullying to the school allowing for the procedures, as set out in the anti-bullying policy, to be followed.
- The Parents' Code of Conduct also set out action that may be taken in the event of placing 'Defamatory, offensive or derogatory comments regarding the school or any of the pupils/parent/staff, at the school on Facebook or other social sites'.

5.2 Social networking advice for staff **– Pupil/Teacher Relationships**

Social networking outside of work hours, on non school-issue equipment, is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice will be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff will not engage in personal online contact with students outside of Headteacher authorised systems (e.g. school email account for homework purposes)
- Staff will ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students)

6. Safeguarding measures

6.1 Filtering

Staff, children and young people are required to use the personalised learning space and all tools within it, in an acceptable way.

Exa Networks broadband connectivity has a filter system, SurfProtect, which is set at a level so that inappropriate content is filtered and tools are appropriate. **All** filtering is set to 'No Access' within any setting and then controlled via the IP address.

Local Control – controls access to websites and provides the option to add to a 'restricted list'. In the event that the site level is not set to 'No Access', the Headteacher approves access for staff.

Anti-virus and anti-spyware software is used on all network and stand alone PCs or laptops and is updated on a regular basis.

A firewall ensures information about children and young people and the school cannot be accessed by unauthorised users.

Links or feeds to e-safety websites are provided on the school website.

Hector Protector is used as a screen cover so that anything accidentally accessed can be covered whilst an adult is informed.

For older children and young people, the Report Abuse button is available should there be a concern of inappropriate or malicious contact made by someone unknown. This provides a safe place for children and young people to report an incident if they feel they cannot talk to a known adult.

CEOP (Child Exploitation and On-line Protection Centre) training is regular and part of the ICT curriculum for raising awareness on staying safe and being responsible. A link to the www.thinkukknow.co.uk website is part of the skin layout for further advice and information on children's or young people's personal on-line spaces.

6.2 Tools for bypassing filtering

Students and staff are forbidden to use any technology designed to circumvent, avoid or bypass any school or educational setting's security controls (including internet filters, antivirus solutions or firewalls.) as stated in the Acceptable Use Rules.

Violation of this rule will result in disciplinary or in some circumstances legal action. Please refer to the 'Staff Procedures Following Misuse by Staff/Children and Young People' sections of this document.

7. Monitoring

The ICT Co-ordinator will monitor the ICT curriculum to ensure relevant coverage and progression, paying particular attention to E-Safety. In addition within the co-ordinating role, lessons are observed, policies are amended, training provided and resources are audited.

8. School library

The computer in the school library will be protected in line with the school network.
Where software is used that requires a child login, this ought to be password protected so that the child is only able to access themselves as a user. Children and young people will be taught not to share passwords.
The same acceptable use rules apply for any staff and children and young people using this technology.

9. Parents

9.1 Roles

Each child or young person receives a copy of the Acceptable Use Rules on first-time entry to the school which need to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules.

It will be expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.
School keeps a record of the signed forms.

9.2 Support

As part of the approach to developing e-safety awareness with children and young people, the Bliss Charity School tries to offer parents the opportunity to find out more about how they can support the school in keeping their child safe and find out what they can do to continue to keep them safe whilst using on-line technologies beyond school.

We try to promote a positive attitude to using the World Wide Web and therefore want parents to support their child's learning and understanding of how to use on-line technologies safely and responsibly.

This information is shared via an annual E-Safety training and as part Safer Internet Day (SID) in February. We ensure that skills around internet use are offered as part of the follow-up training for parents/carers so they know how to use the tools their children and young people are using. Part of this evening will provide parents with information on how the school protects children and young people whilst using the learning platform facilities, such as the internet and E-mail. It will also be an opportunity to explore how both parents and the school can teach the children how to be safe and responsible internet users and how this can be extended to use beyond the school environment.

The Appendices of this section detail where parents/carers can go for further support beyond the school. The school endeavours to provide access to the internet for parents/carers so that appropriate advice and information can be accessed where there may be no internet at home, subject to arrangement.

10. Links to other policies

10.1 Discipline and Anti-Bullying Policies

Please refer to the Discipline Policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs. The Bliss Charity School will have an up to date Anti-bullying Policy which will include any cyberbullying issues.

People will not treat on-line behaviours differently to off-line behaviours and will have exactly the same expectations for appropriate behaviour. This is a key message which will be

reflected within Behaviour and Anti-bullying Policies as it is only the tools and technologies that change, not the behaviour of children, young people and adults.

10.2 Managing allegations and concerns of abuse made against people who work with children

Please refer to the Allegation Procedure, Section 12 LSCB, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff will be reported to the designated person for child protection within the school or educational setting immediately. In the event of an allegation being made against a Headteacher, the Chair of Governors will be notified immediately.

10.3 Health and Safety

Refer to the Health and Safety Policy and procedures of the school/setting and the County Council for information on related topics, particularly Display Screen Equipment, Home working and Accident/Incident reporting procedures. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

10.4 School website **– www.bliss.northants.sch.uk**

The uploading of images to the school website will be subject to the same acceptable rules as uploading to any personal on-line space. Permission ought to be sought from the parent/carer prior to the uploading of any images. We consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

10.5 External websites

In the event that a member of staff finds themselves or another adult on an external website, such as 'Rate My Teacher', as a victim, schools/settings are encouraged to report incidents to the Headteacher and unions, using the reporting procedures for monitoring. The Parents' Code of Conduct also deals at length with the misuse of social networking sites.

10.6 Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of on-line technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body

10.7 Staff Procedures Following Misuse by Staff

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the internet, by an adult:

A. An inappropriate website is accessed inadvertently:

- Report website to the e-Safety Leader if this is deemed necessary.
- Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned or restricted list. Change Local Control filters to restrict locally.
- Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:

- Ensure that no one else can access the material by shutting down.
- Log the incident.
- Report to the Headteacher and e-Safety Leader immediately.
- Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
- Inform the LA/RBC filtering services as with A.

C. An adult receives inappropriate material.

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Headteacher immediately.

- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice e.g. police.

D. An adult has used ICT equipment inappropriately:

- Follow the procedures for B.

E. An adult has communicated with a child or used ICT equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately, if necessary.
- Report to the Headteacher and Designated Person for Child Protection immediately, who will then follow the Allegations Procedure and Child Protection Policy from Section 12, NSCB.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions.
- If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and Designated Safeguarding Lead immediately and follow the Allegations procedure and Child Protection Policy.
- Contact CEOP (police) as necessary.

F. Threatening or malicious comments are posted to the school website (or printed out) about an adult in school:

- Preserve any evidence.
- Inform the Headteacher immediately and follow Child Protection Policy as necessary.
- Inform the RBC/LA/NSCB and e-Safety Leader so that new risks can be identified.
- Contact the police or CEOP as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this will be reported to the Headteacher.

- Staff Procedures Following Misuse by Children and Young People

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:

- Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
- Report website to the e-Safety Leader if this is deemed necessary.
- Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned list or use Local Control to alter within your setting.
- Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:

- Refer the child to the Acceptable Use Rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Decide on appropriate sanction.
- Notify the parent/carer.
- Inform LA/RBC as above.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately.
- Report to the Headteacher and Designated Person for Child Protection immediately.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate misuse the Headteacher must follow the Allegation Procedure and/or Child Protection Policy from Section 12, NSCB.
- Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or about a child in school:

- Preserve any evidence.
- Inform the Headteacher immediately.
- Inform the RBC/LA/NSCB and e-Safety Leader so that new risks can be identified.
- Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:

- Preserve any evidence.
- Inform the Headteacher immediately.

N.B. There are three incidences when you must report directly to the police.

- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found.
They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine.
Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.
• www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

Procedures need to be followed by the school within Section 12 of the Allegations Procedure and Child Protection Policy from the Northamptonshire Safeguarding Children's Board guidance.

All adults to know who the Designated Safeguarding lead is: Shaun Carter with Olivia Thompson, Sharon Simpson, Sue Caller and Lynn Adey. It is important to remember that any offensive images that may be received will never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Acceptable Use Rules for Staff, Governors and Visitors

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

I know that I should only use the school equipment in an appropriate manner and for professional uses.

I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet or send them via E-mail.

I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.

I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.

I will report accidental misuse.

I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Person for Child Protection or e-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.

I know who my Designated Person for Child Protection is.

I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should use the school E-mail and phones (if provided) and only to a child's school E-mail address upon agreed use within the school.

I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher and/or e-Safety Leader.

I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.

I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Leader.

I will adhere to copyright and intellectual property rights.

I will only install hardware and software I have been given permission for.

I accept that the use of any technology designed to avoid or bypass school filtering systems is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures for staff misuse.

I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using on-line technologies.

Signed…….Date…….

Name (printed)…….

SECTION 3

Acceptable use of schools-based employees

1. Policy Statement
In order to create a safe teaching and learning environment, effective policies and procedures which are clearly understood and followed by the whole school community are essential. This Acceptable Use section sets out the roles, responsibilities and procedures for the safe and appropriate use of all technologies to safeguard adults, children and young people within a school or educational setting. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate developments within ICT.

The purpose of the Acceptable Use section is to clearly identify for the whole school community:

i) the steps taken in school to ensure the E-Safety of pupils when using the internet, e-mail and related technologies,

ii) the school's expectations for the behaviour of the whole school community whilst using the internet, e-mail and related technologies within and beyond school ,

iii) the school's expectations for the behaviour of staff when accessing and using data.

2. Scope of policy
The policy applies to all school based employees, including individuals working in a voluntary capacity. All schools are expected to ensure that non-employees on site are made aware of the expectation that technologies and the internet are used safely and appropriately. The Acceptable Use Policy will be used in conjunction with the school/educational settings' disciplinary procedures and code of conduct applicable to employees and pupils.

Where this policy is applied to the Head Teacher, the Chair of Governors will be responsible for its implementation.

Where the Governing Body wishes to deviate from this proposed policy or adopt any other policy, it is the responsibility of the Governing Body to arrange consultation with appropriate representatives from recognised trade unions and professional associations.

3. Legal background
All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare. The legal obligations and safeguarding duties of all school employees in relation to use of technologies feature within the following legislative documents which will be referred to for further information:

- The Children Act 2004
- School Staffing (England) Regulations 2009
- Working Together to Safeguard Children 2010
- Education Act 2002
- Safeguarding Vulnerable Groups Act 2009

All safeguarding responsibilities of schools and individuals referred to within this Acceptable Use Policy includes, but is not restricted to the legislation listed above.

4. Responsibilities
Head Teacher and Governors
The Head teacher and Governors have overall responsibility for e-Safety as part of the wider remit of safeguarding and child protection. To meet these responsibilities, the Head Teacher and Governors will:

- designate an e-Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is

addressed appropriately. All employees, students and volunteers will be aware of who holds this post within school.
- provide resources and time for the e-Safety lead and employees to be trained and update protocols where appropriate.
- promote e-safety across the curriculum and have an awareness of how this is being developed, linked with the school development plan.
- share any e-safety progress and curriculum updates at all governing body meetings and ensure that all present understand the link to child protection.
- ensure that e-safety is embedded within all child protection training, guidance and practices.
- elect an e-Safety Governor to challenge the school about e-Safety issues – Graham Hotchkiss.
- make employees aware of the NSCB Inter-agency Child Protection Procedures at http://www.northamptonshirescb.org.uk/

E-Safety Lead **– Mr Shaun Carter**
The nominated e-Safety lead will:
- recognise the importance of e-Safety and understand the school's duty of care for the-Safety of their pupils and employees.
- establish and maintain a safe ICT learning environment within the school.
- ensure that all individuals in a position of trust who access technology with students understand how filtering levels operate and their purpose.
- with the support of the ICT Subject Leader, ensure that filtering is set to the correct level for employees, young volunteers, children and young people accessing school equipment.
- report issues of concern and update the Headteacher on a regular basis.
- liaise with the Anti-Bullying, Child Protection and ICT leads so that procedures are updated and communicated, and take into account any emerging e-safety issues and technological changes.
- co-ordinate and deliver employee training according to new and emerging technologies so that the correct e-Safety information is being delivered.
- maintain an e-Safety Incident Log to be shared at agreed intervals with the Head Teacher and Governors at governing body meetings.
- with the support of the ICT Lead, implement a system of monitoring employee and pupil use of school issued technologies and the internet when a concern is raised.
- monitoring through collection of devices, or purchase of specialist monitoring software e.g. Securus)

Individual Responsibilities
All school based employees, including volunteers under the age of 18, must:
- take responsibility for their own use of technologies and the internet, making sure that they are used legally, safely and responsibly.
- ensure that children and young people in their care are protected and supported in their use of technologies so that they can be used in a safe and responsible manner. Children will be informed about what to do in the event of an e-Safety incident.
- report any e-Safety incident, concern or misuse of technology to the e-Safety lead (Head Teacher), including the unacceptable behaviour of other members of the school community.
- use school ICT systems and resources for all school related business and communications, particularly those involving sensitive pupil data or images of students. School issued email addresses, mobile phones and cameras must always be used by employees unless specific written permission to use a personal device has been granted by the Head Teacher, for example, due to equipment shortages.
- ensure that all electronic communication with pupils, parents, carers, employees and others is compatible with their professional role and in line with school protocols. Personal details, such as mobile number, social network details and personal e-mail will not be shared or used to communicate with pupils and their families.
- not post online any text, image, sound or video which could upset or offend any member of the whole school community or be incompatible with their professional role. Individuals working with children and young people must understand that behaviour in their personal lives

may impact upon their work with those children and young people if shared online or via social networking sites.
- protect their passwords/personal logins and log-off the network wherever possible when leaving work stations unattended.
- understand that employees, who ignore security advice or use email or the internet for inappropriate reasons, risk dismissal and possible police involvement if appropriate.

5. Inappropriate Use

In the event of staff misuse

If an employee is believed to have misused the internet or school network in an illegal, inappropriate or abusive manner, a report must be made to the Head teacher/Safeguarding lead immediately. The appropriate procedures for allegations must be followed and the following teams/authorities contacted:

- Schools Senior HR Advisory Team
- NSCB (formerly LADO - Local Authority Designated Officer)
- Police/CEOP (if appropriate)

Please refer to the e Safety Incident Flowchart within the accompanying Staff Handbook for further details.

In the event of minor or accidental misuse, internal investigations will be initiated and staff disciplinary procedures followed only if appropriate.

Examples of inappropriate use

Accepting or requesting pupils as 'friends' on social networking sites, or exchanging personal email addresses or mobile phone numbers with students.

Behaving in a manner online which would lead any reasonable person to question an individual's suitability to work with children or act as a role model.

In the event of inappropriate use by a child or young person

In the event of accidental access to inappropriate materials, students are expected to notify an adult immediately and attempt to minimise or close the content until an adult can take action.

Students should recognise the CEOP Report Abuse button (www.thinkuknow.co.uk) as a place where they can make confidential reports about online abuse, sexual requests or other misuse which they feel cannot be shared with employees. The 'Hector the Dolphin' button to also be used to cover the screen from an unsuitable image until an adult can resolve the problem.

6. Policy Review

The Acceptable Use section will be updated to reflect any technological developments and changes to the school's ICT Infrastructure. Acceptable Use Rules for students will be consulted upon by the student body to ensure that all young people can understand and adhere to expectations for online behaviour.

7. Useful Links

NASUWT Social Networking- Guidelines for Members
http://www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNetworking

NUT E-Safety: Protecting School Staff- Guidance for Members
http://www.teachers.org.uk/node/12516

UNISON- Guidance on Social Networking
http://www.unison.org.uk/education/schools/pages_view.asp?did=9786

SECTION 4

Internet policy

1. Introduction.

Usually, the resources used by the children 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 that has not been selected by the teacher. Whilst the children 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.

The problems and issues that have been highlighted by the media, concern all schools. Whilst some of the media interest is hype, there is genuine cause for concern that children might access unsuitable material either accidentally or deliberately.

The purpose of this section of the policy is to:

- establish the ground rules we have in school for using the Internet
- demonstrate the methods used to protect the children from sites containing pornography, racist or politically extreme views and violence.

The school believes that the benefits to the children 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 the children in partnership with parents.

2. Using the Internet for Education

The benefits include:

- access to a wide variety of educational resources including libraries, art galleries and museums,
- rapid and cost effective world-wide communication,
- gaining an understanding of people and cultures around the globe,
- social and leisure use,
- greatly increased skills in Literacy, particularly in being able to read and appraise critically and then communicate what is important to others,
- staff professional development through access to new curriculum materials, experts' knowledge and practice,
- exchange of curriculum and administration data with LA/DfE.

The school intends to teach the children about the vast information resources available on the Internet, using it as a planned part of many lessons.

Initially the children may be restricted to sites that have been reviewed and selected for content. The children will have the opportunity to exchange information via e-mail. They will be taught how to use the address book, how to attach files to an e-mail and how to follow conventions of politeness.

As the children gain experience, they will be taught how to use searching techniques to locate and specific information for themselves. Comparisons will be made between researching from different sources of information, (CD Rom, books, WWW). We hope that the children 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, such as text, photos etc may be "downloaded" from the Internet for use in the children's presentations. Tasks will be set to encourage the children to view web sites and information with a critical eye.

The children will be involved as much as possible with the design, construction and maintenance of the School web site.

3. The children's access to the Internet

This School use Exa Networks broadband connectivity which has a filter system set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child. We will normally only allow children to use the Internet when there is a responsible adult present to supervise. However it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen.

Members of staff will be aware of the potential for misuse, and will be responsible for explaining to the children, the expectation we have of them.

Teachers will have access to the children's e-mails and other Internet related files and will check these on a regular basis to ensure expectations of behaviour are being met.

4. Expectations of the children using the Internet

- The rules are read to the children at the start of each school year.
- At this school we expect all the children to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes the materials they choose to access, and the language they use.
- The children using the World Wide Web are expected not to deliberately seek out offensive materials. Should any of the children encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the Service Provider can block further access to the site.
- The children will only contact people they know or those the teacher has approved.
- They will have been taught the rules of etiquette in e-mail and are expected to follow them.
- The children are expected not to use any rude language in their e-mail communications.
- The children must ask permission before accessing the Internet and have a clear idea why they are using it.
- The children will not access other people's files unless permission has been given.
- Computers will only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet. This to prevent corruption of data and avoid viruses.
- Homework completed at home may be brought in on memory stick or CD but this will have to be virus scanned by the class teacher before use.
- No personal information such as phone numbers and addresses will be given out and no arrangements to meet someone made.
- The children consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.

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.

- Pupils whose work or images appear on the School's website will be identified only by their first names. Should any parent or carer particularly wish their child's name or photograph not to appear on the School's website their wishes will be respected.
- Home information and e-mail identities will not be included, only the point of contact to the School i.e. phone number, School address and e-mail to Head/ Co-ordinator
- Work displayed will be of the highest quality and reflect the status of the School

All the children and their parents/guardians are asked to read and sign an agreement covering the expectations we have of the children using the Internet in school.

SECTION 5

Laptop acceptable use

Computer equipment, software and Internet services provided by The Bliss Charity School for use by teachers in conducting school business is supplied on the following terms and conditions:

1. General
This protocol may be modified from time to time, in response to changing circumstances of an operational, legislative or technological nature.

The Headteacher, ICT coordinator and/or network technician, as part of an audit investigation, may make periodic checks to ensure compliance with these conditions. Where required to do so you must disclose passwords for this purpose.

2. Ownership
The computer equipment, software and services provided are the property of The Bliss Charity School. They are provided on loan to you for the duration of your period as a member of staff at this school. At the end of that period services provided will be terminated and computer equipment and software must be returned to the ICT coordinator in full working condition. If equipment has been lost or damaged whilst on loan, a charge may be made for its replacement or repair.

3. Installation
The equipment and software has been prepared for your use by school technicians. The Bliss Charity School will be responsible for supplying the equipment and any leads necessary to operate the equipment. The machine has been equipped with email software and Internet Explorer 8 for Internet service to your home.

In accordance with Financial Regulations, the equipment shall be marked as School property and shall be recorded in the School Inventory Records.

4. Use of Computer Equipment, software and services
The equipment, software and services are provided for use in respect of school business. In making use of the facilities provided you are required to comply with The Bliss Charity School ICT policy and guidelines with respect to the use of Information Communications Technology.

Private use of the ICT facilities provided is permitted within the guidelines provided above. The Bliss Charity School accepts no liability for any consequences (including financial or other loss), which may arise through private use of the facilities provided.
The Bliss Charity School accepts no liability to support downloaded/installed software for non work related, private use. Any such support requested requiring an IT specialist would incur charges.

You will also note that the security of private information and data is your responsibility. You are advised that simply deleting files does not permanently remove them from a computer.

Where access to the Internet is provided, by using an unfiltered Internet service, you should be aware that the Internet contains potentially offensive material. Northants County Council and The Bliss Charity School accept no liability for any offence, injury or consequences that may result from your use of the Internet and its associated facilities.

You are also reminded of your responsibility of probity (see section 7 below).

Legal Implications
The Bliss Charity School must comply with all UK legislation with respect to the use of ICT. In using The Bliss Charity School facilities you must comply with the following Acts and may be held personally liable for any breach of current legislation as listed below and any future legislation that may be enacted:

- Data Protection Act 1998
- Copyright Designs and Patents Act 1988
- Computer Misuse Act 1990
- Obscene Publications Act 1959
- Freedom of Information Act 2000

It should be noted that:

- There will be no reason to hold The Bliss Charity School information requiring registration under the Data Protection Act on computer equipment provided for your use.
- It is your responsibility to ensure that any personal information held on the computer equipment provided by The Bliss Charity School complies with the provisions of the Data Protection legislation.
- The transmission of personal information contained within electronic mail or as an attachment to electronic mail is also subject to the provisions of the Data Protection Act.
- Waste media (e.g. printed reports, portable disks) must be disposed of with regard to the sensitivity of information concerned and all material making reference to personal data must be disposed of in accordance with The Bliss Charity School AUP and procedures.
- If you hold private information that contains personal details there may be a requirement to register that information.
- The use, or possession, of unlicensed copies or "pirated" versions of software is illegal and is expressly prohibited under the Copyright Designs and Patents Act and The Bliss Charity School AUP.
- Under the Computer Misuse Act 1990, it is an offence:
  (a) To secure computer access to information, data or material where such access is unauthorised, and
  (b) To secure such access with the intent of the commission of a criminal offence.
- The Act also makes it an offence to make any unauthorised modification to the contents of any computer.
- The Obscene Publications Act 1959 makes it an offence to publish an obscene article. Publishing for the purpose of the Act includes distribution or circulation of the article and, in the case of an article containing or embodying matter to be looked at, showing the article.
- Under the Freedom of Information Act 2000 there is a general right of access to all types of recorded information held by public authorities. This will include all information held on your laptop.

5. Computer Security

All media (e.g. flash drives, CDs) of uncertain or unreliable origin must be checked for viruses before use, using The Bliss Charity School's installed antivirus software.

Where a virus is suspected or detected, the matter must be reported to the ICT technician and you must refrain from sending electronic mail and exchanging information via computer media with others, until repair is completed. Virus repair must be undertaken only by an IT specialist. If the source of the virus is not work related then a charge maybe incurred for IT technical support.

Bluetooth capability has been disabled by the technician to prevent unauthorised access to your files and will not be re-activated.

It is your responsibility to ensure that information other than programmes and the operating system held on computer equipment provided by the school is secured (backed-up) on a regular basis.

Where stolen equipment and/or software are recovered; or where it is suspected that equipment or software have been tampered with, they must be tested prior to re-use by an IT specialist.

6. Risk Management and Insurance

The Bliss Charity School maintains insurance on the equipment provided to you, including cover against the perils of theft, accidental damage, malicious damage and fire. Cover for theft is, however, subject to loss arising from forcible entry to or exit from your premises and the standard conditions of cover require that all reasonable care and precaution is taken to try and prevent loss of or damage to the equipment. All computer equipment must be secured from theft or unauthorised use as far as is practical.

If you travel with your laptop or other equipment, it should not be left in an unattended vehicle. There is no cover for losses arising from vehicles, hotel rooms or other unsecured situations. Therefore, you should be especially careful when taking your laptop away from your home, as you will be liable for any such loss.

If you are moving house you are advised to check that the equipment is covered by your removal company's insurance policy.

Any loss of, or damage to, the equipment should be reported as soon as possible to the ICT Co-ordinator in the first instance and any criminal damage should be reported to the Police.

7. Internet access and electronic mail (email)

You are requested to monitor and manage your electronic mail and calendar on a regular basis, preferably daily. You will be provided with an email address to conduct your normal business.

You are reminded that The Bliss Charity School facilities may only be used for lawful purposes. Viewing or transmission of any material, which may be regarded as offensive or in violation of any UK law or legislation, is not permitted. Such material may include copyright material, material judged to be threatening, pornographic, obscene or sexually explicit and material protected by trade secret.

Sending electronic mail, or attaching a file to an email, constitutes processing of personal data if there is any personal data on a living individual within the electronic mail or the attachment. Such processing can only be undertaken if it is permitted under the school's Data Protection notification in the AUP.

Electronic mail should not be used for the transmission of sensitive and confidential information.

Probity

You are reminded of the fact that you are bound by the General Teaching Council's Code of Conduct and Practice for Registered Teachers and that the standards for the regulation of the profession contained within the Code also apply to specific instances, such as the use of the Internet, Intranet or e-mail. You should ensure that your conduct accords with the requirements of the Code.

8. SUPPORT

The laptop is covered by:

- A One Year Warranty including parts and labour on all components including the battery;
- On site support from the school PPT IT technician.

Any computer equipment or software problems which occur during the period of warranty should be reported to the ICT coordinator. In the event that the equipment suffers a complete hardware malfunction, The Bliss Charity School will endeavour to repair/replace the laptop.

9. Health and safety

In the interests of health and safety, you are advised to adhere to the following recommendations for the safe use of personal computer equipment:

- Sit in a chair that gives you good back support to avoid backache;
- Position the screen in front of you to avoid twisting;
- Regularly look away from the screen to reduce eyestrain.

While you have been provided with a “laptop” computer, you should avoid using it on a low table or on your lap as both of these positions will increase strain on your neck and lower back.

If you have any concerns relating to the safe use of your computer equipment, please contact the Headteacher or the ICT coordinator.

10. Indemnity

You shall indemnify Northants Council and The Bliss Charity School against any claims, demands, actions, costs, expenses, losses and damages arising from:

a) any breach by you of any of the conditions of this Protocol;

b) any infringement or alleged infringement of any Intellectual Property Right arising from any use of the equipment combination with any item not supplied by The Bliss Charity School

LAPTOPS FOR TEACHERS

PROTOCOL FOR THE USE OF LAPTOPS BY STAFF OF

The Bliss charity School

SCHEDULE OF EQUIPMENT SOFTWARE AND SERVICES

Equipment Make:

Serial Number (found on underside): .....

Software:

McAfee Virus Protection Software
Microsoft Windows XP Pro/Vista Pro (delete as appropriate).
Microsoft Office Software – Outlook, Word, Excel and PowerPoint, Publisher (2003)

Subject specific software will be installed as requested ; please list current installed software on Appendix 1

Services:
Internet Explorer 8

DECLARATION

I confirm that I have received the equipment, software and services as specified above and agree to abide by the terms and conditions of use as set out in the attached Protocol for the Use of Laptops by Teachers of:

THE BLISS CHARITY SCHOOL.

Name (please print): ……..

Signed: …… Date: ……..…….

SECTION 6

Ipad acceptable use

The policies, procedures and information within this document applies to all iPads, iPod Touches or any other IT handheld device used in school. Teachers and other school staff may also set additional requirements for use within their classroom.

Users Responsibilities

- Users must use protective covers/cases for their iPad.
- The iPad screen is made of glass and therefore is subject to cracking and breaking if misused: Never drop nor place heavy objects (books, laptops, etc.) on top of the iPad.
- iPads to be returned to the iPad box when not in use.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
- iPads leaving school need to be recorded in the record book except Staff ipads
- Do not subject the iPad to extreme heat or cold.
- Do not store or leave unattended in vehicles.
- Users may not photograph any other person, without that persons' consent.
- The iPad is to be connected to the charger cable at the end of the lesson by an adult only.
- The iPad is subject to routine monitoring by The Bliss Charity School. Devices must be surrendered immediately upon request by any member of staff.
- Users in breach of the Responsible Use Policy may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.
- The Bliss Charity School is not responsible for the financial or other loss of any personal files that may be deleted from an iPad.

Safeguarding and Maintaining as an Academic Tool

- iPad batteries are required to be charged and be ready to use in school.
- Syncing the iPad to iTunes or iCloud will be maintained by a School administrator.
- Items deleted from the iPad cannot be recovered.
- No personal files or apps may be downloaded.
- The whereabouts of the iPad will be known at all times.
- It is a user's responsibility to keep their iPad safe and secure.
- If an iPad is found unattended, it will be given to the nearest member of staff.

Lost, Damaged or Stolen iPad

- If the iPad is lost, stolen, or damaged, the Head Teacher must be notified immediately.
- iPads that are believed to be stolen can be tracked through iCloud.

Prohibited Uses (not exclusive):

Accessing Inappropriate Materials – All material on the iPad must adhere to the ICT Responsible Use section in the policy. Users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.

Illegal Activities – Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity.

Violating Copyrights – Users are not allowed to have music and install apps on their iPad.

Cameras – Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of camera in toilets or changing rooms, regardless of intent, will be treated as a serious violation.

Images of other people may only be made with the permission of those in the photograph.

Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of the Teacher or in the case of staff use; a member of the Senior Leadership team.

Use of the camera and microphone is strictly prohibited unless permission is granted by a teacher.

Any user caught trying to gain access to another user's accounts, files or data will be subject to disciplinary action.

Malicious Use/Vandalism – Any attempt to destroy hardware, software or data will be subject to disciplinary action.

Jailbreaking – Jailbreaking is the process of which removes any limitations placed on the iPad by Apple. Jailbreaking results in a less secure device and is strictly prohibited.

Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.

Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school.

Users will be aware of and abide by the guidelines set out by the School eSafety policy.

The Bliss Charity School reserves the right to confiscate and search an iPad to ensure compliance with this Responsible Use Policy.

SECTION 7

Camera and video equipment acceptable use

The Bliss Charity School will respect parents' wishes and their right to protect their child from the improper use of equipment like cameras and video equipment and the use of photographs on social media / networking sites. Parents will have the opportunity to 'opt out' of use of such equipment but will need to know the importance of such equipment when recording their child's progress. Parents are also bound to respect the privacy rights of other parents and their children and The Bliss Charity School staff in their personal use of social media / networking sites.

All materials stored on systems are confidential, and subject to the provisions of the Data Protection Act 1998. The Bliss Charity School expects the highest standards of confidentiality to be observed.

The following rules and guidance apply to ensure that both employees of The Bliss Charity School, visitors and the work of the school are not compromised.

- Only school cameras will be used to take pictures of the children.
- Cameras will be kept on the premises and used for the setting only.
- Images taken and stored on the camera must be downloaded as soon as possible, ideally once a week.
- Photographs will be used to record a child's progress, for internal use and occasionally used for external publication.
- Photographs and videos will be kept on the school system which is secure.
- Mobile phone use will be restricted to the office and staff room unless agreed with the Headteacher first. No staff member will take photographs of the children on their mobile phones.
- Parents may take personal photographs and videos of their child on the strict agreement that images which include other children and/or staff are not published on the internet, ie Facebook, MySpace, Twitter etc or in any external publications.
- It is the responsibility of all members of staff to be vigilant and report any concerns to the Headteacher or Senior Leadership Team.
- Concerns will be taken seriously, logged and investigated appropriately. The Headteacher or his deputy in his absence, reserves the right to check the image content of a member of staffs mobile phone there be cause for concern over the appropriate use of it.

SECTION 8

ICT/E-Safety Curriculum

Subject content (underlined statements refer to e-safety)

Key stage 1

Pupils should be taught to:

- understand what algorithms are; how they are implemented as programs on digital devices; and that programs execute by following precise and unambiguous instructions
- create and debug simple programs
- use logical reasoning to predict the behaviour of simple programs
- use technology purposefully to create, organise, store, manipulate and retrieve digital content
- recognise common uses of information technology beyond school
- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Key stage 2

Pupils should be taught to:

- design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts
- use sequence, selection, and repetition in programs; work with variables and various forms of input and output
- use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs
- understand computer networks including the internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration
- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

SECTION 9

E-Safety Training

Adults in school
All staff to receive annual E-Safety training from a Higher Level E-Safety Officer. E-Safety training is also included as part of the new staff/ new student teachers induction training.

Parents/Carers
All parents to receive E-Safety training annually in order for their children to be able to access the internet at school. Parents who cannot attend will have to read through the relevant documentation at a separate date, if they wish for their child to access the internet at school.

Children
All children to receive dedicated E-Safety lessons annually during the E-Safety Day (SID) in February. The issue of E-Safety to also be addressed termly through the computing curriculum. Children to also receive an annual visit from the local PCSO (Jen Harrison) who covers issue safety which include E-safety. An annual audit is completed by the ICT Co-ordinator to ensure coverage of E-Safety for all classes.

SECTION 10

Section 10: Preventing Extremism and Radicalisation

BRITISH VALUES
The Department of Education have recently reinforced the need ***"to create and enforce a clear and rigorous expectation on all schools to promote the fundamental British values of democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs."***

PREVENTING RADICALISATION AND EXTREMISM
Radicalisation is defined as the act or process of making a person more radical or favouring of extreme or fundamental changes in political, economic or social conditions, institutions or habits of the mind.

Extremism is defined as the holding of extreme political or religious views.
The Bliss Charity School has a **zero tolerance** approach to extremist behaviour for all school community members. We rely on our strong values to steer our work and ensure the pastoral care of our children protects them from exposure to negative influences.

The Headteacher, Senior Leaders and Emma Howard have received up to date 'Prevent Training' against radicalisation.

The Bliss Charity School is fully committed to safeguarding and promoting the welfare of all its children. As a school we recognise that safeguarding against radicalisation is no different from safeguarding against any other vulnerability. At The Bliss Charity School all staff are expected to uphold and promote the fundamental principles of British values, including **democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs.**

- Children are encouraged to adopt and live out our Core Values, especially when using the internet. These complement the key "British Values" of tolerance, respect, understanding, compassion and harmonious living.
- Children are helped to understand the importance of democracy and freedom of speech, through the SEAL, P4C, metacognition, e-safety lessons during computing and through the elected School Council members.
- Children are taught how to keep themselves safe, in school and when using the internet.
- Children are supported in making good choices from a very young age, so they understand the impact and consequences of their actions on others, especially when using the internet.

Appendix A

Further information and guidance on the nature of e-safety and how to encourage safe practice. can be found on:

https://www.**ceop**.police.uk/ (for parents/carers and adults)

www.iwf.org.uk – Internet Watch Foundation (for reporting of illegal images or content)

www.thinkuknow.co.uk (for all children and young people with a section for parents/carers and adults – this also links with the CEOP (Child Exploitation and On-line Protection Centre work)

www.netsmartzkids.org (5 – 17)

www.kidsmart.org.uk (all under 11)

www.phonebrain.org.uk (for Yr 5 – 8)

www.hectorsworld.com (for FS, Yr 1 and 2 and is part of the thinkuknow website above)

www.dcsf.gov.uk (for adults)

http://www3.northamptonshire.gov.uk/councilservices/children/help-and-protection-for-children/Pages/default.aspx or http://www.northamptonshirescb.org.uk/
(Local Safeguarding Children's Board Northamptonshire – policies, procedures and practices, including Section 12 of the Allegations Procedures are available here)

http://www.nen.gov.uk/ (for schools and settings – access to the National Education Network)

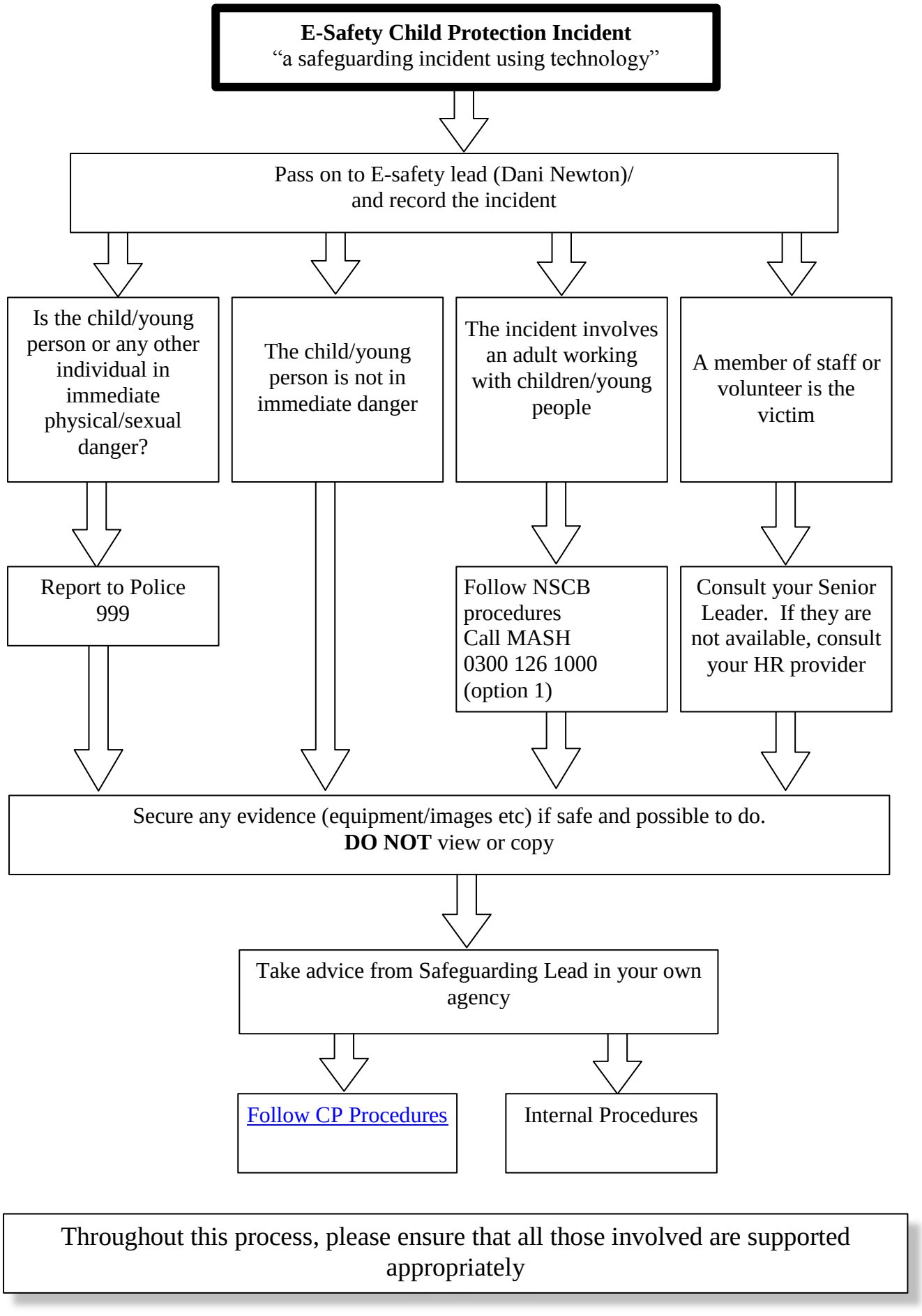
NASUWT Social Networking- Guidelines for Members
http://www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNetworking

NUT E-Safety: Protecting School Staff- Guidance for Members
http://www.teachers.org.uk/node/12516

UNISON- Guidance on Social Networking
http://www.unison.org.uk/education/schools/pages_view.asp?did=9786

Appendix B

You come across a child protection concern involving technology …



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

Appendix C

The Bliss Charity School
Acceptable Use Rules for Staff, Governors and Visitors

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

I know that I should only use the school equipment in an appropriate manner and for professional uses.

I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet or send them via E-mail.

I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.

I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.

I will report accidental misuse.

I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Person for Child Protection or e-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.

I know who my Designated Person for Child Protection is.

I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should use the school E-mail and phones (if provided) and only to a child's school E-mail address upon agreed use within the school.

I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher and/or e-Safety Leader.

I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.

I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Leader.

I will adhere to copyright and intellectual property rights.

I will only install hardware and software I have been given permission for.

I accept that the use of any technology designed to avoid or bypass school filtering systems is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures for staff misuse.

I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using on-line technologies.

Signed…….Date…….

Name (printed)…….

Appendix D

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us.

We can click on the buttons or links when we know what they do. If we see something that we do not think is right, we will either click on Hector on the laptops or press the home button on the Ipads.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

We understand that we should respect everybody, both online and in person.

We know not to give out our personal information online.

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We are trusted to make sensible choices when researching online and know to tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved and we don't open emails from anybody that we don't know.
- 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 understand that we should show respect and tolerance towards everybody, both online and in person

Appendix E

September 2015

Dear Parent/Carer

e-safety Acceptable Use Rules

As part of an enriched curriculum your child will be accessing the Internet and e-mail via Exa Broadband. Exa use a real-time website filtering system.

In order to support the school in educating your child about e-safety (safe use of the Internet), please read the attached internet agreement and rules with your child and then sign and return the slip below.

These rules and internet agreement provide an opportunity for further conversations between you and your child about safe and appropriate use of the Internet and other online tools (eg mobile phones), both within and beyond school (eg at a friends house or at home).

Should you wish to discuss the matter further please contact Miss Connell, ICT co-ordinator.

Yours sincerely

Shaun Carter
Headteacher

I have read through the internet agreement and rules with my child and agree to these safety restrictions.

Signed: _____

Name of child: _____

Class: _____

The Bliss Charity School
Internet Agreement

- I must ask permission before accessing the Internet
- At this school I am expected to be responsible for my own behavior on the Internet, just as I am anywhere else in school. This includes materials I choose to access, and language I use
- When using the World Wide Web I am expected not to deliberately seek out offensive materials. Should I encounter any such material accidentally, I am expected to use the safety button (Hector) and report it immediately to a teacher
- I am expected not to use any rude language in my e-mail communications and contact only people I know or those the teacher has approved. I know that it is forbidden to be involved in sending chain letters
- I will not send e-mails which annoy, insult or attack other people
- I will not access other people's files unless permission has been given
- I will only use the Computers for schoolwork and homework unless permission has been granted otherwise
- **I will not download program files to the computer from the Internet unless a teacher has given me permission**
- I will not bring programs on memory stick or CD Rom in from home for use in school.
- I may bring in Homework, completed at home on a memory stick or CD, but this will have to be virus scanned by the class teacher before use.
- I will not be allowed personal printing, (e.g. pictures of pop groups/cartoon characters) without permission, for cost reasons.
- I will not give out personal information such as phone numbers and addresses and I will not make arrangements to meet someone.
- If I consistently choose not to comply with these expectations I will be warned, and subsequently, I may be denied access to Internet resources.