St. John the Evangelist CEVA Primary School

E-SAFETY POLICY

June 2015

This policy should be implemented as part of the overall strategy of the school and operated within the context of our vision, aims and values as a Church of England school. The policy was devised after consultation with staff, parents and pupils.

The e-safety committee will oversee this policy. Members of the committee are:
Catherine Cowell (Head Teacher)
Ann Tossell (Computing Subject Leader and E-Safety coordinator)
Julie Rawlinson (School Business Manager)
Rob Lewis (E-Safety Governor)
One Parent Representative
Two Pupil Representatives

This policy also comes under the safeguarding umbrella.

This policy will be reviewed annually

Signed:

Dated:

Contents

Policy

Appendices

1. INTRODUCTION

E-Safety encompasses both the security of data held by the school and the safety of users whilst exploiting the potential of new technologies. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The E-safety Policy has been developed to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

(a) The core E-Safety policy

The school has designed this policy, building upon the South West Grid for Learning E-**Safety** template Policy and additional government / Local Authority guidance. Further details on the South West Grid for Learning (SWGfL) policy and North Somerset's guidance can be found at the following addresses:

http://thelearningexchange.org.uk/e-safety-home/

http://www.swgfl.org.uk/Staying-Safe

(b) End-to-End E-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff, students and community users; encouraged by education and made explicit through publicised policies.
- Sound implementation of E-Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the South West Grid for Learning Consortium including the effective management of the filtering and monitoring system.
- National Education Network standards and specifications.

2. Definitions and statutory guidance

Members of the school community include staff, pupils, volunteers, parents/carers, governors, visitors and community users who have access to and are users of school ICT systems, both within and outside of the school premises.
The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents and associated behaviour in accordance with this policy and anti-bullying policies and will inform parents/carers of incidents of inappropriate E-Safety behaviour that take place out of school. Incidents will be recorded in the school's E-Safety Incident Log and the appropriate procedure will be followed (see E-Safety incident flow chart Appendix B).

3. Roles and Responsibilities

(a) Governors

The board of Governors is responsible for the approval of the E-Safety policy and for reviewing the effectiveness of the policy. Governors should take part in E-Safety training/awareness sessions. One of the board should undertake the role of 'E-Safety Governor'.

The responsibilities of this person include:

- Meeting regularly with the E-Safety Co-ordinator
- Monitoring of the E-Safety Incident Log
- Regular review of the filtering/change control log
- Reporting on relevant areas to the board of governors

(b) Head teacher

The Head teacher is responsible for ensuring the safety (including E-Safety) of members of the school community.

The head teacher and the Computing Subject Leader should also be aware of the procedures to be followed in the event of a serious E-Safety allegation.

(c) E-Safety co-ordinator

It is the responsibility of the E-Safety co-ordinator to:

- Attend the E-Safety committee meetings
- Take day-to-day responsibility for E-Safety issues and take a leading role in
- establishing and reviewing the school's E-Safety policies and supporting
- documentation
- Ensure that all staff are aware of the procedures that need to be followed in the
- event of an E-Safety incident occurring
- Provide training and advice for staff and remind staff to change passwords every 90 days
- Liaise with the Local Authority
- Liaise with school ICT technical staff
- Receive reports of E-Safety incidents and create a log of incidents to inform future
- E-Safety developments
- Meet regularly with the E-Safety Governor to discuss current issues, review incidents
- logs and the filtering/change control logs
- Attend relevant meetings
- Report regularly to the Senior Leadership Team.

(d) ICT Technician

The ICT Technician is responsible for ensuring that:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack
- The school meets the E-Safety technical requirements outlined in the SWGfL Security Policy, the Acceptable ICT User Statement and any relevant Local Authority E-Safety Policy and guidance
- Users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Informs SWGfL of issues relating to the filtering applied by the Grid
- Use of the network is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety co-ordinator and Head teacher.

(e) Child Protection (Designated Person)

The Designated Person for Child Protection should be trained in E-Safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying.

(f) <u>Teaching and support staff</u>

Teaching and support staff are responsible for ensuring that they:

- have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
- have read, understood and signed the school Staff Acceptable User Agreement
- report any suspected misuse or problem to the E-Safety co-ordinator for investigation
- ensure digital communications with pupils and parents should be on a professional level and only carried out using official school systems

(g) <u>Pupils</u>

All pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable User Agreement, which they will be expected to sign before being given access to the school system. According to age related expectations of understanding, pupils are expected to:

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying
- Understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

(h) <u>Parents and Carers</u>

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children.

The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, website and information about national and local E-Safety campaigns.

Parents and carers will be responsible for:

Endorsing (by signature) the Pupil ICT Acceptable User Agreement. Copies of the E-Safety policy and Agreement, are available to view on the School Website.

All users of the school network will conduct their use line with the principles laid down in the following sections:

PASSWORD Guidelines and Procedures
MOBILE PHONE Guidelines and Procedures
ICT ACCEPTABLE USER Guidelines and Procedures
Permitted use of technologies and devices

4. Training

It is essential that all staff receive E-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal E-Safety training will be made available to staff. An audit of the E-Safety training needs of all staff will be carried out annually
- All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Acceptable User Agreements.
- Governor training - invited to staff training and offered LA/external awareness raising events.

5.Teaching and Learning

(a) Curriculum

- E-Safety is a focus in all areas of the curriculum, wherever electronic technologies are used, and staff reinforce E-Safety messages in the use of ICT across the curriculum. In addition, E-Safety is taught as an explicit part of the Computing Curriculum, following a structured and progressive scheme of work
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, (e.g. on social networking sites).

(b) Learning

(i) Why Internet use is important

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

(ii) The internet can enhance learning

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

(iii) Pupils will be taught how to evaluate internet content

- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

6. Managing Internet Access

(a) <u>Information system security</u>

- School ICT systems capacity and security will be reviewed regularly by the ICT technician
- Virus protection will be updated regularly by the ICT technician
- Security strategies will be discussed with LA advisors and with the South West Grid for Learning.

(b) <u>Children and E-mail</u>

- Pupils may only use approved E-mail accounts on the school system
- Pupils must immediately tell a teacher if they receive offensive E-mail
- Pupils must not reveal personal details of themselves or others in E-mail communication or arrange to meet anyone without specific permission
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted
- Pupils will be advised to only open attachments from known and safe sources or to check with the teacher if in doubt.

(c) <u>Published content and the school website</u>

- The contact details on the website should be the school address, E-mail and telephone number. Staff or pupils' personal information will not be published
- The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

(d) <u>Publishing images and work by pupils</u>

- Photographs that include pupils will be selected carefully
- Pupils' full names will not be used anywhere on the website or blog, particularly in association with photographs.

(e) <u>Social networking and personal publishing</u>

- The school will block/filter access to social networking sites
- Pupils will be advised never to give out personal information of any kind that might identify them or their location
- Pupils and parents will be advised of the possible risks arising from the use of social network sites outside school, to which primary aged pupils can be exposed.

(f) <u>Managing filtering</u>

- The internet is monitored for all users.
- The school will work with the Local Authority, the Department for Education and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved
- If staff or pupils discover an unsuitable website, it must be reported to an adult, who will consult the E-Safety co-ordinator
- The ICT technician, the Computing co-ordinator and the E-Safety co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

(g) <u>Managing emerging technologies</u>

- Emerging technologies will be examined to ensure the security of existing systems and for educational benefit before use in school is allowed.

7. PASSWORD Guidelines and Procedure

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access
- No user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies)
- Access to personal data is securely controlled in line with the school's Data Protection Policy
- Logs are maintained of access by users and of their actions whilst using the system.

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including E-mail

Responsibilities

The management of the password procedures will be the responsibility of the Computing subject leader, ICT technician and the E-Safety co-ordinator.

All adults and pupils will have responsibility for the security of their username and password. Adults and pupils must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Passwords for new users and replacement passwords for existing users will be allocated by the ICT Technician and the E-Safety co-ordinator.

Adult users will change their passwords every 90 days, while pupils will change their passwords every year.

Training / Awareness

Members of staff will be made aware of the school's password procedures:

- At induction
- Through the school's E-Safety policy and password procedures
- Through the Staff Acceptable User Agreement.

Pupils / students will be made aware of the school's password procedures:

- In ICT, PSHE or E-Safety lessons
- Through the use of posters
- Through the Pupil Acceptable User Agreement.

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the E-Safety co-ordinator and will be reviewed, at least annually, by the E-Safety Committee.

All users will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames.

The following rules apply to the use of passwords:

- Never reveal your password to anyone
- Do not use any part of your username within the password
- Never write your password down in a shared place
- Passwords shall not be displayed on screen, and will be securely hashed
- Requests for password changes should be made in person to the School Business Manager, ensuring that the new password can only be passed to the genuine user.

The following rules apply to the use of passwords for adults:

- Passwords must be changed every 90 days
- Adult passwords should be a combination of upper and lower case characters and numbers and must be a minimum of eight characters

Computers and laptops will be screen locked when leaving a room.

The “administrator” passwords for the school ICT system, used by the ICT technician, Computing Subject Leader and E-Safety co-ordinator must also be available to the Head teacher or other nominated senior leader and kept in a secure place e.g. school safe (A school should never allow one user to have sole administrator access).

Audit/Monitoring/Reporting/Review

The E-Safety co-ordinator and ICT Technician will ensure that full records are kept of:

- User Ids and requests for password changes
- User logons
- Security incidents related to this policy.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by the E-Safety Committee at regular intervals with a minimum of once a year. The policy will be reviewed annually in response to changes in guidance and evidence gained from the logs.

8. MOBILE PHONE Guidelines and Procedures

Introduction

This policy outlines the appropriate use of mobile phones on our school site.
The widespread ownership of mobile phones among young people requires that school administrators, teachers, pupils, and parents take steps to ensure that mobile phones are used responsibly at school.

Pupils

We recognise that many students and their families own a mobile phone. We also recognise that some parents/guardians request that their child/ren bring a mobile phone to school for safety/security reasons. Our core business of teaching and learning needs to be conducted in an environment free from unnecessary distractions or disruptions. Therefore the school strongly discourages the possession of mobile phones in school by students. There are no reasons why a student needs to have in their possession, or use, a mobile phone during the school day. Parents are reminded that in cases of emergency the school office remains a vital and appropriate point of contact. This ensures your child is reached quickly and assisted in any appropriate way.

The school is prepared to allow mobile phones on the premises but only within the parameters of the policy as stated below.

Responsibility

It is the responsibility of pupils who bring mobile phones to school to abide by the guidelines outlined in this document.

- The decision to provide a mobile phone to their child/ren should be made by parents or guardians.
- Parents should be aware if their child/ren takes a mobile phone to school.
- Parents/guardians may revoke approval at any time.
- Pupils must hand the mobile phone in to the school office upon arrival and collect it at the end of the day.

Sanctions

Students who fail to follow these guidelines will have their phones confiscated. The phone will only be handed back to the parent/guardian. The school may revoke the right for student to bring a mobile phone onto the school grounds.

It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. The school may consider it appropriate to involve the police.

Staff

It is the responsibility of staff who bring mobile phones to school to abide by the guidelines outlined in this document.

- During teaching time, while on playground duty and during meetings, mobile phones will be locked in lockers, and switched off or put on ‘silent' or ‘discreet' mode. Mobile phone use is not permitted during teaching time, while on playground duty and during meetings.
- Staff may take personal mobile phones on educational visits to enable contact to be kept with school.
- Mobile phones can only be used in the designated zones during school hours.
  These zones are:
  School office
  Staff room
  Head teacher’s office.
- Any individual bringing a personal device into the setting must ensure that it contains no inappropriate or illegal content.
- Any breach of these procedures could lead to the e-safety committee being informed and consequently disciplinary action according to the schools procedures.

9. School Website Guidelines and Procedures

THE SCHOOL WEBSITE

The school has established clear policies to ensure that its website is effective, and does not compromise the safety of the pupils or staff:

- The Head teacher is responsible for the overall content of information on the school website.
- Content: Considerations must be given to the following: - layout, format and style, colour, font type and size.
- Protocol: Considerations must be given to the following: - honesty, information must not be misleading, be politically correct, must not be offensive, conform to copyright, avoid using underline, be consistent – e.g. when linking to different areas, allow for modem V Broadband (timings) and download times (Compact pages, amount of graphics make sure they are JPG/GIF files and compressed).
- The School Business Manager will be responsible for loading and maintaining and publishing the school website.
- The website will be checked regularly to ensure that there is no content that compromises the safety of pupils or staff.
- Publication of pupil images will only be used with parental permission.
- Publication of adult images will only be used with their permission.
- Pupils' names will not be used.
- Ensure the school is not infringing the intellectual property rights of others through any of the materials available via its website. Copyright may apply to text, images, music or video that originates from other sources.
- Is compliant with the Date Protection Act 1998

10. Photographic Images of Children

Introduction

The use of images of children and young people has become more of an issue over recent years with concerns over members of the public misusing the images themselves or gaining access to the children and young people pictured. The issue has been further complicated with the advancement of mobile phone and internet technology.

There is no national policy available at the moment to instruct schools and LAs on the best procedures to adopt. North Somerset schools have requested specific guidance with regard to the use of images in publications and on websites and the procedures regarding the use of video recording equipment by parents / carers.

This document provides guidance on the appropriate use of images of children in education, including schools, youth and community, pupil referral units etc. It covers still, video and electronic photographic images wherever they are used. The guidance is for staff in educational establishments and in North Somerset Council (NSC) who wish to use images of children and young people in education.

This guidance does not differentiate between images for use in publications and those for use on the internet. This is because whilst the school prospectus is designed to be a hard document, it could easily be made available over the web. It is therefore difficult to monitor which images have been approved for which purpose.

Schools need to make full and proper use of photographic images while meeting the law and preserving the safety of children. Concerns focus on issues around rights of privacy, child protection and copyright ownership. These guidelines address these issues and give advice on good practice.

Typical Uses of Photographs

- Key skills for PE.
- Performing arts including dance and movement, concerts, drama performances, parent evenings.
- Sports days and sports fixtures and the use of photographic equipment by parents and carers and children from the other school.
- Media including newspapers and television especially when some editors require children's names when publishing photographs.
- Displays in school of children's activities.
- Publications by the establishment and by the LA.
- Establishment and LA web-sites.
- Staff training and professional development activities.
- Site security / CCTV videos.

Governing Body

On behalf of the Governing Body, the Health and Safety Governor with the Head teacher should ensure that the policy is adhered to.

Ownership

Human Rights legislation and the Data Protection Act 1998 give people new rights and it is the right to 'privacy' that is the issue when using photographs. The Council and schools must take steps that respect the rights of people in photographs.

Schools should not display images of pupils or staff on websites, in publications or in areas of the school used by the public outside of school hours without consent of the person concerned or their legal guardian. The definition of a public area includes places where visitors to the school have access.

The Copyright, Designs and Patent Acts 1988 moved the ownership of copyright to the photographer (or their employer) and away from the person commissioning and paying for the photographs, unless there is an agreement otherwise.

Good Practice
The following advice represents good practice in the use of photographic images involving children.

1. When taking a picture the school or LA must obtain the consent of the person in the picture or from their parent or carer.
2. If using a photo from the media or commissioning a photograph, have a signed agreement.
3. Use the image in its intended context. Examples of this not happening are:
   - When a picture taken by a national newspaper of a child accepting an award was used by the National Front in a story with a completely different story angle.
   - When a photo of the public boarding a bus to launch a rural transport initiative is used to illustrate a story attacking rural transport shortages.
4. Follow the commitment made in the consent forms:
   - If names must be used, give only first name;
   - Not to use the photograph out of context;
   - Not to use the photograph to illustrate sensitive or negative issues.

5. When photographing children:
   a) Ensure that parents and carers of young people have signed and returned the school consent form for general photography. Any images going beyond the school or LA need additional specific consent
   b) Ensure all children are appropriately dressed.
   c) Avoid images that only show a single child with no surrounding context of what they are learning or doing.
   d) Photographs of three or four children are more likely to also include their learning context.
   e) Do not use images of a child who is considered very vulnerable, unless parents / carers have given specific written permission.
   f) Avoid naming young people. If one name is required then use the first name only where possible.
   g) Use photographs that represent the diversity of the young people participating.
   h) Report any concerns relating to any inappropriate or intrusive photography to the Head teacher.
   i) Remember the duty of care and challenge any inappropriate behaviour or language.
   j) Do not use images that are likely to cause distress, upset or embarrassment.

6. Annually review stored images and delete unwanted material.

Parental Permission
Use of images of children requires the consent of the parent / carer. Permission should always be obtained by using the Information Sheet, when a child joins the school. The form covers both the school and LA when using the photographs in publications and on web-sites. As part of the updating of the Information Sheet, ask parents if they wish to change their permission.

When a parent does not agree to their child being photographed, the Head teacher must inform staff and make every effort to comply sensitively.
For example, if a child whose parents have refused permission for photography is involved with a sports event, e.g. a football match, it may not be appropriate to photograph the whole team. Careful liaison with parents is therefore essential. With discussion it may be possible to agree other options. The parent may

accept a team photograph if names are not published or they may be prepared to relent if it affects the whole team.

When photographic images are transmitted or shared beyond the school e.g. television broadcasts specific permission should be obtained.

Inter-School Fixtures
Apply these guidelines to inter-school events. If a vulnerable child is involved, it will be necessary to liaise with a member of staff from the other establishment so that they are aware of the wishes of the parents or carer of the child and seek the cooperation of the parents of the opposing team.

Teacher Training/ All Students and Portfolios
During training and with newly qualified staff, colleagues need to compile portfolios with photographs of children during lessons. Staff should act responsibly in compiling these images. The Class Teacher should oversee the compiled images in order to monitor their appropriateness.

Displays in Schools
Still photographs shown on displays and video clips available during open / parents' evenings should depict children in an appropriate way. They should not display images of children in inappropriate or revealing clothing so appropriate levels of integrity and decency are maintained. Do not use photographs or images likely to cause embarrassment.

Children Photographing Each Other
This practice can occur extensively during offsite activities particularly during residential periods. Staff should maintain the supervision and management control specified in the Offsite Activities Guidelines 2003. There may be incidents where children take inappropriate photographs, perhaps showing friends and other children inappropriately dressed. Staff should endeavor to discourage this practice, but ultimately parents are responsible for monitoring their child's use of cameras and subsequent use of their images involved.

Newspapers
Photo opportunities: When a newspaper is invited to celebrate an event, the school will make every effort to ensure that only children who have parental permission are photographed and that if required only first names are used.

Use of Internet/Intranet Sites
Many schools will have an internet/intranet facility. The Head teacher should know good practice and ensure that the school only uses appropriate images that follow this guidance. For example, if a child has successfully completed a gymnastics award, it would be appropriate to show the child in a tracksuit rather than leotard.

Mobile Phones
The use of mobile phones as cameras of photographic and or video capabilities should not be permitted anywhere.

Close Circuit Television (CCTV)
Increasing numbers of school are installing such equipment for the following uses:

- As a method of controlling access.
- An aid to site management in monitoring incorrect parking, manoeuvring vehicles, delivery arrivals etc.
- Pupil behaviour issues / bullying. As a behavioural tool during breaks and lunch times it can be used to identify hot spots of inappropriate behaviour.
- As an aid to members of staff with particular responsibility for behaviour management.

- To monitor personal safety for site supervisors, caretakers, cleaners etc.
- To monitor site safety and security.
- As an effective deterrent for crime.
- As a means of crime reduction and discouraging trespass.

Types of Recorders

Cameras: -

Several types of cameras are used, notably:
Fixed-Wide angle lens.
Dome cameras (rotary) with 360 degrees capacity.
Corner mounted cameras with 270 degrees capacity.
Manually operated pan tilt-zoom lenses. These have infinitely variable distance and angle capabilities and so can zoom onto individuals. It is therefore crucial that authorised and designated staff only have access to the equipment and that occasional and periodic monitoring of the images saved is undertaken by a senior member of management. Images should be destroyed after the designated period.

Camera Sitings: -

Every effort should be made to avoid inappropriate images and cameras should not be sited in toilets, changing rooms or other sensitive areas. Camera sitings should be carried out in conjunction with advice from the local authority.

Out of School Hours: -

Cameras may record inappropriate activities taking place on the school site, without the school's knowledge. If they are of a criminal nature, consideration should be given by a senior member of the management team to referring the information to the police.

Again images should be erased in accordance with the procedures above.

While CCTV can be an extremely effective and useful crime reduction / deterrent device, careful use of the images and control by competent responsible staff is considered crucial.

11. Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.

Training is available through SWGfL BOOST which includes unlimited webinar training on this subject and covers clear reporting guidance, including responsibilities, procedures and sanctions, risk assessment, including legal risk: (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development)

School staff should ensure that:

No reference should be made in social media to students / pupils, parents / carers or school staff

They do not engage in online discussion on personal matters relating to members of the school community

Personal opinions should not be attributed to the school or local authority

Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Social media sites will be checked regularly for any reference to the school’s name.

12. Cyber-bullying

Introduction

Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself including, but not limited to:

- Bullying by texts or messages or calls on mobile phones
- The use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, chat rooms, blogs, social networking sites including, amongst others, Facebook and Youtube
- Using e-mail to message others
- Hijacking/cloning e-mail accounts

Staff

Cyber-bullying is a serious issue and while all bullying is damaging, cyber-bullying is invasive of privacy at all times and may also be a criminal act. School staff have a responsibility to educate pupils both in the proper use of telecommunications and about the serious consequences of cyber-bullying through PSHE and e-safety lessons. In addition, all staff have a responsibility to respond to reports of cyber-bullying or harassment by reporting any incidents to the Designated Person for Child Protection and/or the E-safety Coordinator as appropriate. The school will support victims of cyber-bullying and will use the full range of sanctions available to punish any member of the school community who perpetrates cyber-bullying.

Pupils

Pupils who believe they, or someone else is the victim of cyber-bullying, must speak to an adult as soon as possible. This person could be a parent/guardian, teacher or other responsible adult. Where possible the evidence should be preserved in order to follow up on the incident. Children should be aware that incidents carried out at home, which have an impact on members of the school community, may also be dealt with as if they had occurred within school.

13. Filtering and safety of school infrastructure and network

The school takes responsibility for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It also will ensure that the relevant people named in the above sections are effective in carrying out their e-safety responsibilities.

Specifically:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- All users have clearly defined access rights to school technical systems and devices.
- All users are provided with a username and secure password. Users are responsible for the security of their username and password
- Administrator passwords for the ICT system, used by the Network Manager are also available to the Headteacher and kept in a secure place
- The School Business Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- The school has provided differentiated user-level filtering, allowing different filtering levels for different groups of users – staff / pupils
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An system is in place for users to report any actual / potential technical incident / security breach to the relevant person
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. All staff laptops are encrypted. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Temporary logins for "guests" (eg, visitors and governors) onto the school systems gives access to the internet only and not the school network.
- Staff are issued with a school laptop and / or ipad and sign a user agreement. The device remains the property of the school and is returned to school at the end of their employment.
- When devices become obsolete, all data is wiped in line with current guidance and the hard drive destroyed and disposed of separately from the device.
- Staff are not permitted to download or install new programmes or executable files. They are able to allow updates to existing software (eg adobe)
- There is no need for staff to store data on a memory stick. On the rare occasion where it may be necessary, an encrypted memory stick must be used and appropriate precautions taken (eg School Business Manager)
- When data needs to be sent via the internet, the school currently use the North Somerset email system, RM easymail or AnyComms+, all of which are secure systems. Correspondence from outside the authority is password protected wherever possible.

14. Electronic Devices

The school provides a laptop and / or ipad for all teaching staff and certain additional staff who may require access to school information in order to work at home. It should not be necessary for staff to use personal devices in order to work at home. All data or information of a personal or sensitive nature must only be stored on school devices and should only be accessed on school devices.

There is therefore no need for teachers or other staff to use their own devices in the classroom and they should not be brought in to school. This includes laptops, ipads, cameras and similar devices. Mobile phones may only be used in staff designated areas.

If the Head Teacher suspects that a member of staff may have been using their own devices to store confidential information inappropriately, including data and images, they will be asked to surrender the device for inspection. Any data found will be deleted and disciplinary measures may be taken.

Pupils are not permitted to bring personal devices into school including ipads, laptops, cameras or hand held gaming devices. Pupils are permitted to bring a phone in to school at a parent’s request, providing it is handed in to the office for the duration of the school day.

15. Acceptable User Agreements

Purpose
The purpose of this is to ensure that Staff and pupils (known as Users) understand the way in which the Internet and other electronic devices is to be used. The Policy aims to ensure that the technologies are used effectively for their intended purpose, without infringing legal requirements or creating unnecessary risk. Users should read this policy alongside the other SWGfL policies, Filtering Policy and Email Policy.

Scope
The policy applies to:

- All users and administrators of the SWGfL services and/or infrastructure
- All employees, including contractors and temporary staff
- All Student Teachers
- Parents and helpers
- Pupils

On evidence provided by SWGfL, an employee may be disciplined by their employer, including dismissal. At the same time if your conduct and/or action(s) may be illegal and you may become personally liable in some circumstances.

General Policy
The SWGfL encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. It should not compromise the SWGfL's information and computer systems.

Please read this policy carefully as you will be deemed to be aware of its contents.

Use of Internet Facilities

1. Information accessible via the Internet covers a wide range of interests and activities. For the purposed of this document, Internet usage means any connection to the Internet via web browsing, external email or news groups.
2. Connection to the Internet via the schools network is available to all Users having access to a networked computer.
3. Occasional personal use of the Internet by Employees only is permitted, subject to the restrictions contained in this policy. Any personal use is expected to be in the employee's own time and is not to interfere with an individual's normal job responsibilities. Personal use must not detrimentally affect the job responsibilities of other employees, cause offence, disrupt any system and/or harm the school's reputation.
4. Use of the internet may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources and access to certain websites will be restricted.
5. The distribution of any school information via the Internet is to be subject to same control and scrutiny as for other channels of communication (telephone, mail, face-to-face). The school reserves the right to determine the suitability of information distributed via the Internet.
6. Access to certain sites that are deemed to be excluded under this Policy will be denied by the school. This list will be regularly reviewed and updated.

Monitoring
All the School resources, including access to the Internet are provided solely for school purposes. At any time without prior notice the School maintains the right and ability to examine any systems and inspect and review any and all data recorded in those systems.

Any information stored on a computer, whether the information is contained on a hard drive, computer disk or in any other manner may be subject to scrutiny by the School. This examination supports the performance or internal investigations and the management of information systems as well as helping to ensure compliance with internal policies and the law.

Internet sites that have been visited by users can be traced. Therefore all Users having access to the Internet need to be aware that in order to ensure compliance with this policy, the School employs monitoring software to check on the use and content of the internet sites accessed to ensure that there are no serious breaches of this Policy. The School specifically reserves the right for authorised personnel to access, retrieve, read and delete such Internet access monitoring logs, to assure compliance with this Policy.
This monitoring of usage will be in accordance with the Regulation of Investigatory Powers Act.

SERVICES
There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school, the school will be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY
Users are expected to inform the ICT Technician immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user ID and password, where applicable and must not share this information with other users. Users identified as a security risk will be denied access to the network.

PHYSICAL SECURITY
Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. Laptops should be covered under personal household insurance N.B. household policies do not cover laptops left unattended in cars (not even locked in the boot).

WILFUL DAMAGE
Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and if appropriate legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

MEDIA PUBLICATIONS
Named images of pupils (e.g. photographs, videos, web broadcasting TV presentations web pages etc.) must not be published under any circumstances. Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site.
Pupils work will only be published (e.g. photographs, videos) if parental consent has been given.

DATA SECURITY
All data must be handled in a sensitive and secure manner. Personal data or information should only be accessed and stored on school devices.

16. Policy Decisions

(a) Authorising internet access

- All users of school ICT resources will be required to read and sign an age appropriate Acceptable User Agreement on an annual basis.
- The school will keep a record of all staff and pupils who are granted internet access
- The record will be kept up to date, for instance a member of staff may leave or a pupils access be withdrawn
- Parents will be asked to consent to their child using the internet by signing the Pupil ICT Acceptable User Agreement

(b) Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor North Somerset LA can accept liability for the material accessed, or any consequences of internet access.
- The school will audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

(c) Handling E-Safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff/Head teacher
- Any complaint about staff misuse must be referred to the Head teacher.

(d) Community use of the internet

- The school will advise members of the community using the school's internet that they will need to abide by the school E-Safety rules as displayed in the suite. All users must read and sign the Acceptable User Agreement. Any misuse will lead to withdrawal of access.

17. Communications Policy

(a) Introducing the E-Safety policy to all pupils

- All pupils will sign the Pupil Acceptable User Agreement at the start of each academic year before being granted access to the school network, which will be explained at an age appropriate level.

- Parents will be asked to sign the Pupil Acceptable User Agreement on their child's entry to school and thereafter at the start of each academic year to consent to their child using the internet in school through ticking the consent box on Parent Pay
- E-Safety rules will be posted in all teaching areas including lap and ipad storage and discussed with pupils
- Pupils will be informed that network and internet use will be monitored.

(b) Staff and the E-Safety policy

- All staff will be given the school E-Safety policy and its importance explained
- All staff will sign a Staff Acceptable User Agreement before being granted access to the network

(c) Enlisting parents' support

- Parents attention will be drawn to the school E-Safety policy in newsletters and on the school website
- Adults working with pupils using the internet will be made aware of the school E-Safety Policy
- Regular adult helpers will be expected to sign the Staff Acceptable User Agreement and be invited to attend or take part in E-Safety presentations.

18. Data Protection

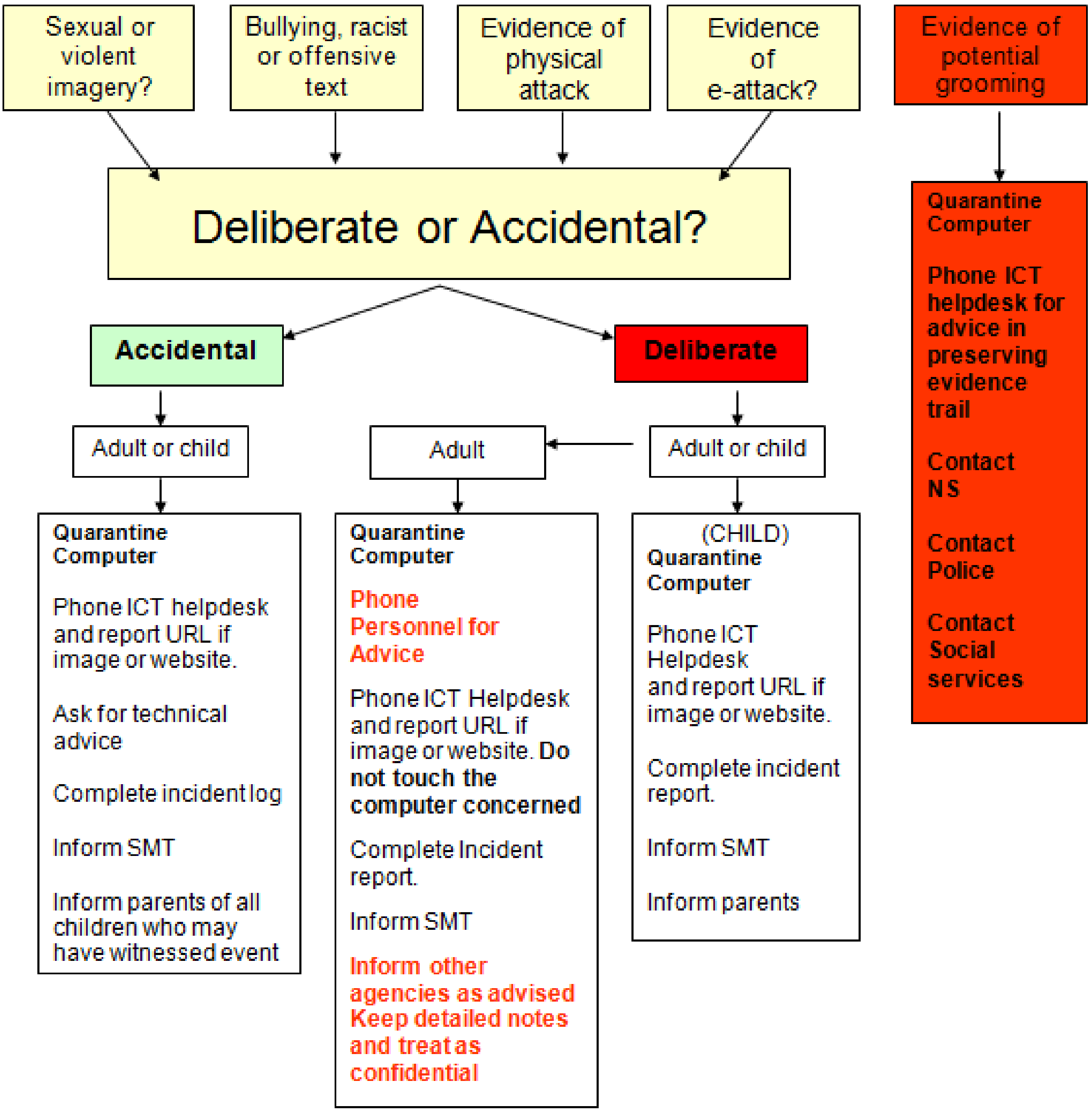
The school operates a data protection policy under the guidance of Information Commission Office. (ICO)

Appendix A
Permitted use of technologies and devices

	Staff & other adults				Students / Pupils			
Communication Technologies	Allow ed	Allowed at certain times tttimes times	Allowed for selected staff	Not allowed	Allow ed	Allowed at certain times	Allowed with staff permission permission	Not allowed
Mobile phones may be brought to school	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x							x
Taking photos on mobile phones				x				x
Use of hand held devices eg PDAs, PSPs	x							x
Use of personal email addresses in school, or on school network		x						x
Use of school email for personal emails		x						x
Use of chat rooms / facilities				x				x
Use of instant messaging				x				x
Use of social networking sites				x				x
Use of blogs		x				x		

Appendix B

E-safety Incident Flow Chart



Sexual or violent imagery?

Bullying, racist or offensive text

Evidence of physical attack

Evidence of e-attack?

Evidence of potential grooming

Deliberate or Accidental?

Accidental

Adult or child

Quarantine Computer

Phone ICT helpdesk and report URL if image or website.

Ask for technical advice

Complete incident log

Inform SMT

Inform parents of all children who may have witnessed event

Deliberate

Adult or child

Adult

Quarantine Computer

Phone Personnel for Advice

Phone ICT Helpdesk and report URL if image or website. **Do not touch the computer concerned**

Complete Incident report.

Inform SMT

Inform other agencies as advised Keep detailed notes and treat as confidential

(CHILD) **Quarantine Computer**

Phone ICT Helpdesk and report URL if image or website.

Complete incident report.

Inform SMT

Inform parents

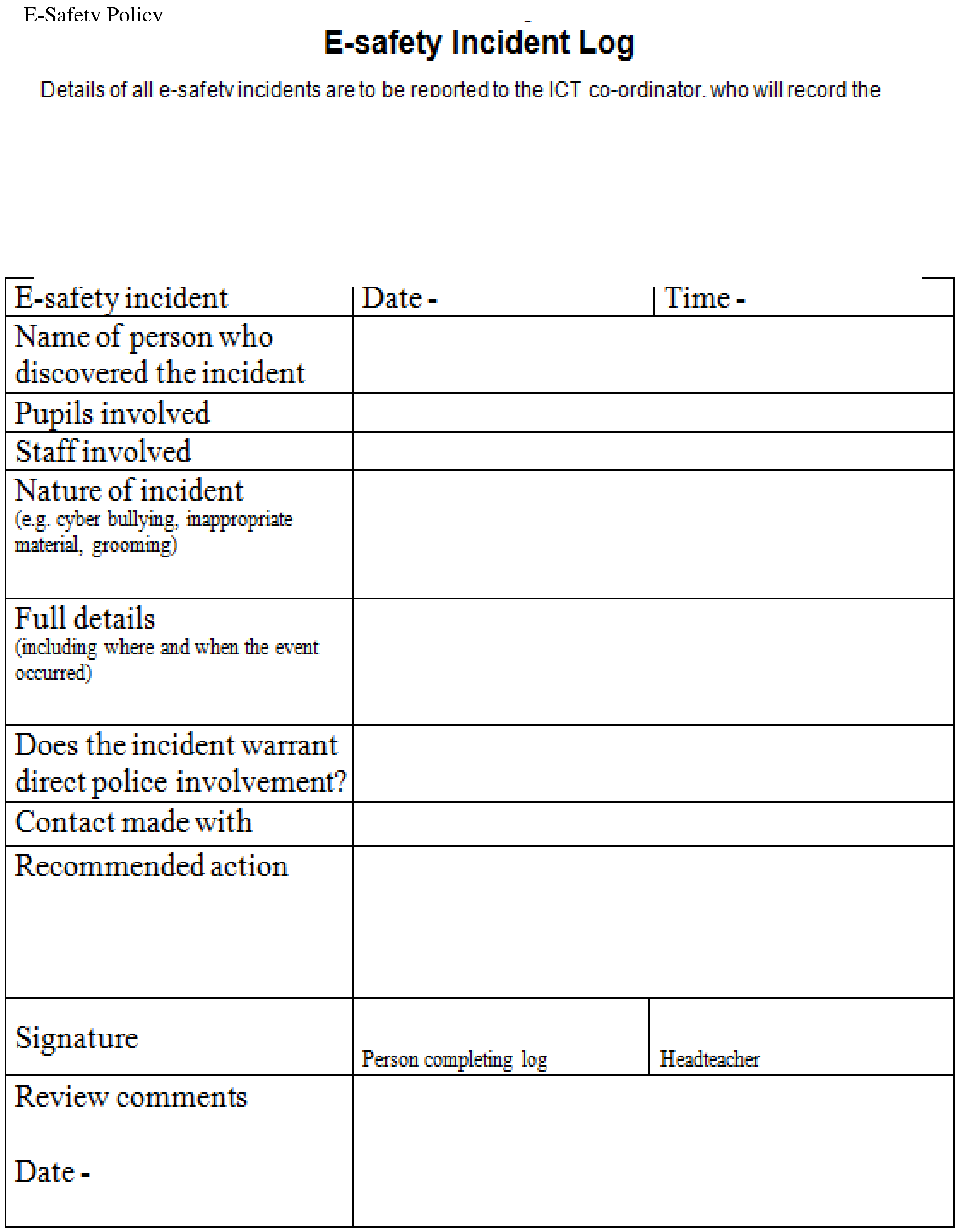
Quarantine Computer

Phone ICT helpdesk for advice in preserving evidence trail

Contact NS

Contact Police

Contact Social services



E-safety Incident Log

Details of all e-safety incidents are to be reported to the ICT co-ordinator, who will record the

E-safety incident	Date -	Time -
Name of person who discovered the incident		
Pupils involved		
Staff involved		
Nature of incident (e.g. cyber bullying, inappropriate material, grooming)		
Full details (including where and when the event occurred)		
Does the incident warrant direct police involvement?		
Contact made with		
Recommended action		
Signature	Person completing log	Headteacher
Review comments Date -		

Appendix C Consent Form for Photography and Images for Adults

St. John the Evangelist Church of England Primary School

Consent Form for Photography and Images for Adults

During your employment at school we may wish to take photographs of activities that involve you. The photographs may be used for displays, publications or on a web-site by us, by the Local Education Authority or by local newspapers.

Photography or filming will only take place with the permission of the Head teacher. When filming or photography is carried out by the news media, names will only be used if there is a particular reason to do so, and home addresses will never be given out. Images that might cause embarrassment or distress will not be used nor will images be associated with material on issues that are sensitive.

Before taking any photographs of you, we need your permission. Please **answer the questions below, sign and date the form and return it to the school office**. You can ask to see images held by the school. You may withdraw your consent at any time by putting this in writing to the Head teacher.

Name (Block Capitals) :	

I understand that:

- the local media may take images of activities that show the school and children in a positive light e.g. Reception Year pictures of new starters, drama and musical performances, sports and prize giving;
- photographers acting on behalf of the school or North Somerset Council may take images for use in displays, in publications or on a website;
- embarrassing or distressing images will not be used;
- the images will not be associated with distressing or sensitive issues; and
- the school will regularly review and delete unwanted material.

Having read the above statement, do you give your consent for photographs and other images to be taken and used? (please tick the appropriate box)		**YES**, I give consent for my pictures to be taken and used
		NO, I do not give permission for my pictures to be taken and used

Signature	
Date (Date/Month/Year):	

Appendix D Consent Form for Photography and Images for Children

St. John the Evangelist Church of England Primary School
Consent Form for Photography and Images for Children

During your child's life at St. John the Evangelist Church of England Primary School we may wish to take film or photographs of activities that involve your child. These may be used for displays, publications by us, by the Local Authority (this may include the School and Authority web-site) or by local newspapers. Photography or filming will only take place with the permission of the head teacher, and under appropriate supervision. When photography is carried out by local newspapers, children will only be named if there is a particular reason to do so (e.g. they have won a prize), first names only will be used and home addresses will never be given out. Images that might cause embarrassment or distress will not be used nor will images be associated with material on issues that are sensitive.

Before filming or taking any photographs of your child, we need your permission - please **sign and date the form below.** You can ask to see images of your child held by the school and you may withdraw your consent at any time.

Name of child (Block Capitals) :		
Child's Date of Birth		
Name of person responsible for the child:		
I understand that: • the local press may take images of activities that show the school and children in a positive light e.g. Reception Year pictures of new starters, drama and musical performances, sports and prize giving; • photographers acting on behalf of the school or North Somerset Council may take images for use in displays, in publications or on a website; • embarrassing or distressing images will not be used; • the images will not be associated with distressing or sensitive issues; and • the school will regularly review and delete unwanted material.		
Having read the above statement, do you give your consent for photographs and other images of your child to be taken and used? (please tick the appropriate box)		**YES**, I give my consent for pictures of my child to be taken and used
		NO, I do not give my permission for pictures of my child to be taken and used
Signature of person responsible for the child:		
Relationship to the child:		
Date (Date/Month/Year):		

NB There may be other circumstances, falling outside the normal day to day activities of the school, (e.g. television news) in which pictures of children are requested. The school recognises that in such circumstances specific consent from parent or guardian will be required before photography or filming of children can be permitted. If you have concerns or queries about any of this information, please discuss it with the Head teacher.

St. John the Evangelist Church of England Primary School

Adult ICT Acceptable User Agreement

Responsible use of the Internet

- I will not access or attempt to access any internet sites that may be deemed to be inappropriate including using the Internet for gambling, soliciting, representing personal opinions or revealing confidential information and those relating to illegal activity. Downloading some material is illegal and the police or other authorities may be called to investigate such use. I understand that all sites visited leave evidence in the county network if not on the computer. Common sense needs to apply in deciding which sites are inappropriate.

- I will not visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain: obscene, hateful, illegal and or abusive material relating to any of the groupings (impairment, gender, marital status, ethnic origin, nationality, race or colour, religious belief, sexuality, age, trades union membership) listed in the Equal Opportunities Policy.

- I understand that unacceptable use includes accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety; accessing or creating, transmitting or publishing any defamatory material; receiving sending or publishing material that violates Data Protection Act or breeches the security this act requires for personal data; transmitting unsolicited material to other users (including those on other networks).

- Any personal use will be reasonable in duration and not interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet.

- I understand that E-mail contact will be conducted on a professional basis as a representative of the school. The messages I send will be polite and responsible and will not use language that could be calculated to incite hatred against any ethnic, religious or other minority groups. I understand that my E-mails may be monitored.

- I will respect the ownership of copyright material. I will not upload, download, or otherwise transmit (send, receive, copy, distribute) commercial software or any copyright materials belonging to third parties outside of the school, or to the school itself.

- I will respect the confidentiality of material to which I have access. I will not reveal or publicise confidential or proprietary information which includes but is not limited to: financial information; databases and the information contained therein; personal information on employees and or clients or customers; computer/network access codes and business relationships.

- I will respect the privacy of all users. I will not reveal any personal information (e.g. home address, telephone number) about myself or others users.

E-Safety Policy

- I am aware of the need to protect children using the internet. I will not allow children to gain unsupervised access to the internet or unauthorised access to chat rooms or other unsuitable sites. I will immediately report access to any unsuitable sites to the E-safety coordinator and / or the School Business Manager, whether accessed intentionally or accidentally.

Responsible use of the Network

- I will only access the system with my own login and password, which I will keep secret and log off after each use. If I believe my password has been compromised I will inform the School Business Manager and change my password. If I find a computer left logged on by another user I will log off and log on with my own password before using

- I will not access or attempt to access unauthorised files or network areas. I understand that files saved on the school network may be monitored.

- I will use the computers/devices predominantly to support school work. I will not use the school's equipment for running a private business or enter into any personal transaction that involves the school in any way.

- I will ensure that any removable devices brought in from outside school will have been checked for viruses before connecting them to the school system.

- I will not install or download any software or programme files without the specific permission of the Head Teacher.

- I understand that unacceptable use includes user action that would cause corruption or destruction of other user's data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere

- I understand that all laptops, I-pads and other devices remain the property of the school, and that the Acceptable User Agreement applies to all networks and devices.

- I understand that private data or personal information should only be accessed and stored on school devices and treated with the utmost discretion and sensitivity. I will not store personal data or information on any private device.

- I understand that by signing the Acceptable User Agreement I am confirming that I have read the E-Safety Policy and that I accept the policies, guidelines and procedures contained within.

Print Name	Signature	Date

St. John the Evangelist Church of England Primary School

Pupil ICT Acceptable User Agreement

Responsible use of the Internet

Please read and discuss with your child. Sign below and return so that your child will be allowed access to internet learning in school.

Explanation

As part of the pupils' curriculum enhancement, entitlement and the development of ICT skills, St John the Evangelist CEVA Primary School is providing supervised access to the Internet.

Pupils may be able to exchange electronic mail with partner schools and research information from museums, libraries, news providers and suitable web sites as part of their programme of learning.

We take positive steps to avoid children having access to undesirable materials. At Key Stage 1, access to the Internet will be by teacher or adult demonstration. Pupils will have access to teacher approved materials rather than the open internet. At Key Stage 2, Internet access may be granted to a whole class as part of a scheme of work or to groups of children for research, following a suitable introduction to the rules for responsible Internet use. We also have a firewall system to protect the children. Should you wish to discuss any aspect of Internet use (or to see a lesson in operation) please telephone the Head teacher to arrange an appointment.

Below are the E-Safety Rules that we operate. Further advice may be obtained from national bodies eg CEOP which explain issues further, also covering Internet use at home.

In addition, we advise all parents/carers to read the schools E-Safety policy, paying particular attention to the password and mobile phone sections.

This policy is available on the school website.
Please visit http://www.st-johnevangelist.n-somerset.sch.uk

E-Safety Rules

The school has installed computers/devices with Internet access to help our learning. These rules will keep us safe and help us be fair to others.

- I will only access the system with my own login and password, which I will keep secret
- I will not access files belonging to other people
- I will use the computers/devices for school work and homework
- I will not bring in removable devices from outside school unless I have been given permission
- I will always have permission from a member of staff before using the Internet
- I will only E-mail people I know, or those that my teacher has approved
- The messages I send will be polite and responsible
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission
- I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself
- I understand that the school will check my computer files and will monitor the Internet sites I visit

Pupil's Agreement

- **I have read and I understand the schools E-Safety rules**
- **I will use the computer, network, Internet access and other new technologies in a responsible way at all times.**
- **I know that the network and Internet access will be monitored.**

Pupils Name ………………………………………………………………………… Class ………………….

Parent Signature ……………………………………………………………. Date ……………………