E-Safety and Acceptable Use

Evolve Church Academies Trust

Approved by:	[Name]	**Date:** [Date]
Last reviewed on:	[Date]	
Next review due by:	[Date]	

The designated people responsible for Child Protection are Oliver Johnson (Evole Executive Headteacher), Mrs Kathryn Crawford (Head of School – St Loys and Chacombe), Mrs Sandra Prewer (Head of School – Culworth) and Mrs Clare Law (Head of School – Boddington). Refer to the appropriate personnel for the relevant school within Evolve.

The designated member responsible for internet safety (the e-Safety leader) in the schools is the DSL

The designated Director of **Evolve Church Academies Trust** responsible for safeguarding is John Moffit

The Internet has now long been considered to be an essential part of modern life. In addition, the school has a duty to provide pupils with quality Internet access as part of their learning. This e-safety policy considers the use of both the fixed and mobile internet, PCs, laptops, webcams, digital video equipment, mobile phones, camera phones, I-pads, personal digital assistants and portable media players. It will be revised to incorporate new and emerging technologies. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use.

Aims

The aims of this e-Safety Policy are to:

- Emphasise the need to educate staff and children about the pros and cons of using new technologies both within and outside the schools, so that they have the necessary skills and knowledge to become responsible digital citizens.
- Provide safeguards and rules for acceptable use to guide all users, whether staff of pupil, in their online experiences
- Ensure that adults are clear about procedures for misuse of any technologies both within and beyond the schools and to understand that internet use in the schools is a resource and a privilege and should be treated respectfully.
- 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
- Provide guidance to staff and pupils about the acceptable use of mobile technologies, both the schools' and personal items that are brought into the schools.

- Ensure that pupils benefit from all learning opportunities offered by the internet resources provided by the schools in a safe and controlled manner.

The Trust's Vision for Digital Education

We strive to develop the learning environment to provide a range of ICT opportunities and tools. This will empower our children to make relevant and safe choices and be flexible as they develop their personalised learning, in line with our schools' vision. We aspire to provide children with the necessary skills to enable them to succeed to a high level in an ever increasingly technology driven world.

Purpose Of Internet Use

The purpose of Internet use in the schools is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the schools' management information and business administration systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers are required to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed ICT capability is now seen as an essential life-skill. Internet access is an entitlement for pupils as part of the curriculum. The schools have a duty to provide pupils with quality Internet access as part of their learning experience.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- exchange of curriculum and administration data with the LEA and DCSF.

Assessing the risks

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 the schools to ensure that children and young people are protected from harm both within and beyond the schools environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of on-line technologies.

- Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which may be unsuitable. We recognise that it is important to adopt strategies for the safe and responsible use of the Internet. In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The schools will take all reasonable precautions to ensure that users access only appropriate material.

- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Head Teacher will ensure that the ICT policy is implemented and compliance with the policy monitored by the member of staff responsible for e-safety.

We will make every effort to safeguard against all risks. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. Any incidents that may arise will be dealt with according to the provisions of the Child Protection Policy and in accordance with the procedures of the LSBCN to ensure children are protected.

Roles and responsibilities

1.1 Governors and Head Teacher

It is the overall responsibility of the Head Teacher with the Governor body of each school to ensure that there is an overview of e-Safety (as part of the wider remit of Child Protection) across the schools with further responsibilities as follows:

The Head Teacher has designated an 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 schools.

Time and resources are provided for the e-Safety Leader and staff to be trained and update policies, where appropriate.

The Head Teacher is responsible for promoting e-Safety across the curriculum and has an awareness of how this is being developed, linked with the school's development plan.

The Head Teacher is to 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 will ensure Child Protection is covered with an awareness of e-Safety and how it is being addressed within the schools.

The e-Safety Governor will ensure that the schools have an ICT Policy with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including:

- Firewalls
- Anti-virus and anti-spyware software
- Filters
- Using an accredited ISP (internet Service Provider)
- Awareness of wireless technology issues
- Policy on using personal devices.

The E-safety governor will ensure that any misuse or incident is dealt with in accordance with the Child Protection Policy and LSCBN procedure.

1.2 e-Safety Leader

It is the role of the designated e-Safety Leader (DSL) to:

Establish and maintain a safe ICT learning environment within the schools.

Ensure that the Acceptable Use Policy 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.

Report issues and update the Head Teacher on a regular basis.

Liaise with the PSHE, Child Protection and ICT Coordinators 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.

Ensure transparent monitoring of the internet and on-line technologies. Boddington and Culworth Schools uses filtering systems and staff will be watchful at all times.

Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified.

Work alongside the ICT Coordinator and ICT technician, 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 minimize issues of virus transfer.

1.3 Staff and any other adults working in the schools

It is the responsibility of all adults within the schools to:

Ensure that they know who the designated person for Child Protection is within the schools or other setting, so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Head Teacher. In the event of an allegation made against the Head Teacher, the Chair of Governors must be informed immediately.

Be familiar with the Behaviour, 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 Head Teacher immediately.

Alert the e-Safety Coordinator to any new or arising issues and risks that may need to be included within policies and procedures.

Ensure that children are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Ensure that children 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.

Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff using non-personal equipment, within and beyond the school environment.

Use electronic communications in an appropriate and legal way.

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.

Report accidental access to inappropriate materials to the e-Safety Leader.

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 schools/educational setting’s network.

1.4 Children and young people

Children will be:

- Involved in the review of Acceptable Use Rules through the schools council and through work with their class teacher, in line with this policy being reviewed and updated.

- Responsible for following the Acceptable Use Rules whilst within the schools as agreed.

- Taught to use the internet in a safe and responsible manner through the curriculum.

- 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).

2. ***Appropriate and Inappropriate Use***

2.1 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.

All staff receive a copy of the Acceptable Use Policy annually and a copy of the Acceptable Use Rules, which are then signed, returned to the schools and kept under file with a signed copy returned to the member of staff. The Acceptable Use Rules are displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

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 Head Teacher immediately. The Head Teacher will implement the policies in the Child Protection procedure in accordance with LSCBN procedures.

A copy of the Acceptable Use Rules is on display in each classroom and attached to the laptop trolleys.

We encourage parents/carers to support the rules with their children. They are asked to sign a copy of the Acceptable Rules (APPENDIX 2) together so that it is clear to the schools that the rules are accepted by the child with the support of their parents/carers. This is also intended to provide support and information to parents/carers when children may be using the internet beyond the schools.
Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed.

2.2 By children

In the event of inappropriate use

- Any child found to be misusing the internet by not following the Acceptable Use Rules will have a letter sent home to parents/carers explaining the reason for suspending the child'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 is deemed to have misused technology against another child or adult.

In the event that a child **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 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 deliberately misusing on-line technologies will also be addressed by the schools. See appendices.

Children are 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.

3 The curriculum and tools for learning

3.1 Internet use

We aim to teach children how to use the internet safely and responsibly. They are also taught, through ICT and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. We aim to teach the following concepts, skills and competencies by the time the children leave Year 6:

- Internet literacy
- making good judgments 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 in terms of personal information

- where to go for advice and how to report abuse

E-Safety lessons and resources are also found at www.thinkuknow.co.uk for Key Stage 1 and 2.

These skills and competencies are taught within the curriculum so that children have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner. Children 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 – We will ensure 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 the schools
- identifying information, e.g. I am number 8 in the Culworth and Boddington etc. FootballTeam

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

3.2 Pupils with additional learning needs

We strive to provide access to a broad and balanced curriculum for all learners and recognize the importance of tailoring activities to suit the educational needs of each pupil. Where a child 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.

3.3 E-mail use

Children have access to emails 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.

Staff and children should use their school issued e-mail addresses for school business only.

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

3.4 Mobile phones and other emerging technologies

We will continue to consider carefully how the use of mobile technologies can be used as a teaching and learning tool within the curriculum, taking into consideration the following areas of concern:

- 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 the schools filtering and allow access to inappropriate or potentially harmful material or communications.

The use of mobile phones by children is not allowed at the schools. In exceptional circumstances, the Head Teacher may sanction the use of a mobile phone by a child only with the written request from a parent/carer, outlining the reasons. Permission will be signed by the Head Teacher and a log kept of such use. Staff are allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers to contact children under any circumstances.**

(i) Personal mobile devices

⍰ Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, will be subject to the same procedures as taking images from digital or video cameras.

- Staff should 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 the schools, authorisation must be sought from the Head Teacher and the activity supervised by a member of staff at all times.
- The schools are not responsible for any theft, loss or damage of any personal mobile device.

(ii)School/educational establishment 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 should be used to conduct school business outside of the school's environment. The Head Teacher may give permission for staff to use their own personal mobile devices for the school's business. A record will be kept. Where personal devices are used for school business, images will be transferred to the schools' systems as soon as possible and deleted from personal equipment at that time.

3.5 Video and photographs

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 the schools there is access to a variety of equipment. The e- Safety leader will maintain a list of such equipment.

Children must seek permission from their teacher before uploading any images and teachers must check for inappropriate content.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to the schools website. Photographs should only ever include the child's first name. Photographs will be stored in a central location on the schools network.

4. Web 2.0 Technologies

4.1 Managing Social Networking and other Web 2.0 technologies

- We control access to social networking sites through existing filtering systems.
- Pupils are not permitted to give out personal details or information which could identify them or their location (e.g. mobile phone number, home address, the schools name, groups or clubs attended, IM and email address or full names of friends.)
- Pupils 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, the schools 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.
- We are aware that social networking can be a vehicle for cyberbullying. Pupils are encouraged to report any incidents of bullying to the schools allowing for the procedures, as set out in the anti-bullying policy, to be followed.

4.2 Social networking advice for staff

All staff are expected to abide by professional standards.

5. Safeguarding measures

5.1 Filtering

The schools use an Internet filtering system provided by our IT providers.

Children should use a search engine that is age appropriate such as AskJeeveskids or Yahooligans. Links or feeds to e-safety websites are provided.

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

For older children, 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 to report an incident if they feel they cannot talk to a known adult.

CEOP (Child Exploitation and On-line Protection Centre) training for Year 6 Primary children is annual and part of the PSHE curriculum for raising awareness on staying safe and being responsible.

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

8. Parents

8.1 Roles

Each child receives a copy of the Acceptable Use Rules (APPENDIX 2) on an annual basis or first-time entry to the schools which needs to be read with the parent/carer, signed and returned to the schools confirming both an understanding and acceptance of the rules.

It is expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

The Schools keep records of the signed forms.

8.2 Support As part of the approach to developing e-safety awareness with children, We offer parents the opportunity to find out more about how they can support the schools in keeping their child safe and find out what they can do to continue to keep them safe whilst using on-line technologies beyond the schools. The schools promotes 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.

9. Links to other policies

9.1 Behaviour and Anti-Bullying Policies

Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs. We have an up to date Anti- bullying Policy which includes any cyberbullying issues.

9.2 Managing allegations and concerns of abuse made against people who work with children. Allegations made against a member of staff should be reported to the designated person for child protection within the schools or educational setting immediately. In the event of an allegation being made against a Head Teacher, the Chair of Governors should be notified immediately. The Child Protection Policy will be followed in accordance with the LSCBN policy.

9.3 PSHE

The teaching and learning of e-Safety is embedded within the PSHE curriculum to ensure that the key safety messages about engaging with people are the same whether children are on or off line.

9.4 Health and Safety

Refer to the Health and Safety Policy and procedures of the schools 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.

9.5 School website

The uploading of images to the school's website is subject to the same acceptable rules as uploading to any personal on-line space. Permission will be sought from the parent/carer prior to the uploading of any images. (APPENDIX 2)

9.6 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, staff are encouraged to report incidents to the Head Teacher and unions, using the reporting procedures for monitoring.

10 Review

This policy will be reviewed annually by the Policies Committee.

Appendices

Staff Procedures Following Misuse by Staff

The Head Teacher will ensure that these procedures are followed, in the event of any misuse of the internet, by a member of staff.

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 the schools and Local Authority/Regional Broadband Consortium 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 the schools.

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 Head Teacher and e-Safety Leader immediately.
- Head Teacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
- Inform the Local Authority/Regional Broadband Consortium 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 Head Teacher 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, ifnecessary.
- Report to the Head Teacher and Designated Person for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, Local Safeguarding Children's Board Northamptonshire.
- 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 Head Teacher to implement appropriate sanctions.

- If illegal or inappropriate misuse is known, contact the Head Teacher or Chair of Governors (if allegation is made against the Head Teacher) and Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy.
- Contact CEOP (police) as necessary.

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

- Preserve any evidence.
- Inform the Head Teacher immediately and follow Child Protection Policy as necessary.
- Inform the Regional Broadband Consortium/Local Authority/Local Safeguarding Children's Board Northamptonshire 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 should be reported to the Head Teacher.

Staff Procedures Following Misuse by Children

The Head Teacher will ensure that these procedures are followed, in the event of any misuse of the internet, by a child:

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 the schools and Local Authority/Regional Broadband Consortium 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 children's use in the schools.

B. An inappropriate website is accessed deliberately:

- Any child found to be misusing the internet by not following the Acceptable Use Rules will have a letter sent home to parents/carers explaining the reason for suspending the child'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 is deemed to have misused technology against another child or adult.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.

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 Head Teacher 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.
- In the event of illegal or inappropriate misuse the Head Teacher must follow the Child Protection Policy
- Contact CEOP (police) as necessary.

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

- Preserve any evidence.
- Inform the Head Teacher immediately.
- Inform the Regional Broadband Consortium/Local Authority/Local Safeguarding Children's Board Northamptonshire 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 schools or setting:

- Preserve any evidence.
- Inform the Head Teacher immediately.

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

1. Indecent images of children found.
2. Incidents of 'grooming' behaviour.
3. 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 online.

APPENDIX 1
Acceptable Use and e-safety Policy

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 schools 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 that will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

Acceptable Use Rules for Staff, Governors and Visitors

- I know that I should only use the school's 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 about children and young people if uploading to the internet.
- I have read the procedures for misuse in the e-Safety policy so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any misuse that I become aware of to the Designated Person.
- I will report any incidents of concern for children's safety to the Head Teacher, who is the Designated Person for Child Protection in accordance with procedures listed in the Child Protection 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 via personal technologies, including my personal e-mail and should use the school's e- mail and *phones (if provided)* only to a child's school e-mail address upon agreed use within the schools.

- I know that I should not be using the school’s system for personal use unless this has been agreed by the Head Teacher.

- *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 downloadedresources.*

- *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 the e-Safety leader. 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 by the e-Safety leader or Head Teacher.

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

- I know that the schools may monitor use network activity and on-line communications.

- I have been given access to a copy of the e-Safety 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)………………………………………………………………………………………………

School……………………………………………………………………..

APPENDIX 2

e-Safety Acceptable Use Rules Letter to Parents/Carers

Parent agreement

Dear Parent/Guardian

As part of our curriculum we encourage children to make use of educational resources available on the Internet. Access to the Internet enables pupils to conduct research and obtain high quality educational resources from libraries, museums, galleries and other information sources from around the world.

To guard against accidental access to materials which are inappropriate in school we provide an appropriate filtered service. However, it is not always possible to provide 100% assurance that pupils might not accidentally come across material which would not be inappropriate.

Therefore, before they access the Internet we would like all pupils to discuss the attached Elearning Code of Conduct with their parents/guardians and then return the signed form to the school office.

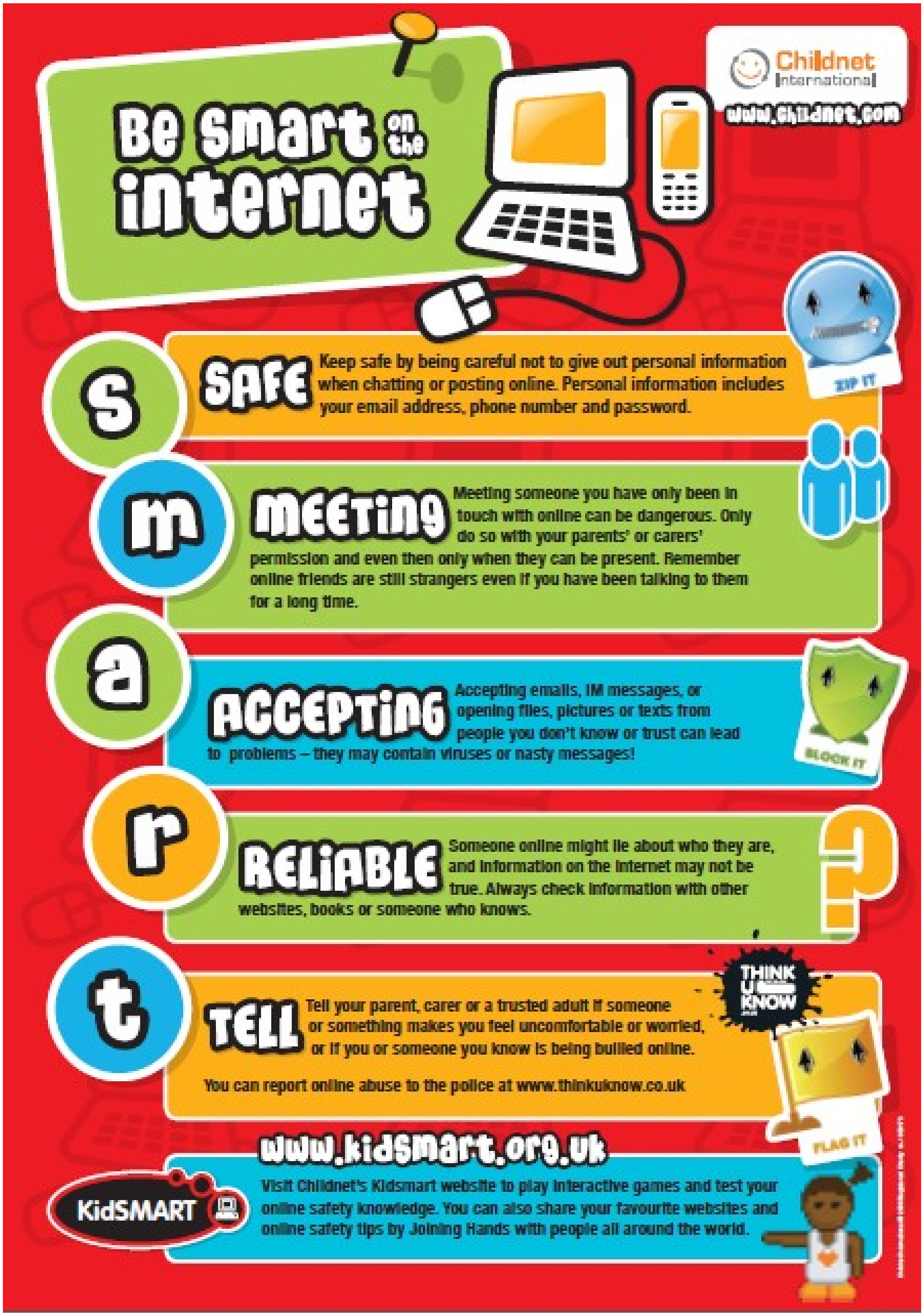
We believe that the educational benefit to pupils from access to the Internet in the form of information resources and opportunities for collaboration, far outweigh the potential disadvantages.

During lesson time teacher will guide pupils towards specific material and educational resources. Where pupils are given permission to access the Internet outside lessons they must agree to access only those sites that are appropriate for use in school and use the e- learning resources appropriately.

Yours sincerely

(insert name)
Headteacher

The federation of Culworth and Boddington Primary Academies E-safety Code of Conduct



Be Smart on the internet

Childnet International
www.childnet.com

S **SAFE** Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.

M **MEETING** Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

A **ACCEPTING** Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R **RELIABLE** Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.

T **TELL** Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

www.kidsmart.org.uk

KidSMART

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Parental consents

Please sign the relevant parts and return to the school office as soon as possible.

Child's name:

E-safety Code of Conduct

As a parent guardian, I have read, discussed and explained the E-learning Code of Conduct to my son/daughter. I understand that if he/she fails to follow this code, his/her individual access may be withdrawn and I will be informed.

Pupil's signature____

Parents/Guardian signature____ Date____________

Permission and Copyright Release

I consent to digital photographs and videos of the child named above, appearing in printedand electronic publications. I understand that the images will be used only for educational purposes and that the identity of my child will be protected. I also acknowledge that the images may also be used in and distributed by other media such as promotional activities.

Parents/Guardian signature____ Date____________

I consent to examples of my child's work being published on the school website or in other media, subject to strict confidentially of personal information.

Parents/Guardian signature____ Date____________

Digital projects in school

I consent to my child taking part in projects in school using digital video and photographs. I consent to my child taking part in the production of and appearing in films. I understand that the films may be made available on the school website or used in other school promotional activities.

Parents/Guardian signature____ Date____________

APPENDIX 3

Further Information and Guidance

The nature of e-safety is evolving. Encourage safe practice. You may want to keep up to date with further supporting documents, information or advice, which can be found on:

- www.parentscentre.gov.uk (for parents/carers)
- www.ceop.co.uk (for parents/carers and adults)
- www.iwf.org.uk (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.bbc.co.uk/cbbc/help/safesurfing (for Yr 3/4)
- www.hectorsworld.com (for FS, Yr 1 and 2 and is part of the thinkuknow website above)
- www.teachernet.gov.uk (for schools and settings)
- www.dcsf.gov.uk (for adults)
- www.digizen.org.uk (for materials from DCSF around the issue of cyberbullying)
- www.becta.org.uk (advice for settings to update policies) and http://www.nextgenerationlearning.org.uk/esafetyandwifi.html (simple tips for parents/adults)
- http://www.safe-child-northants.org.uk (Local Safeguarding Children's Board Northamptonshire – policies, procedures and practices, including Section 12 of the Allegations Procedures are available here)
- www.nen.org.uk (for schools and settings – access to the National Education Network)
- https://enable.lpplus.net/ht/e-Safetyhome (for schools and settings to access e-Safety guidance and support)

Appendices 4

Staff Procedures Following Misuse by Staff

The Head Teacher will ensure that these procedures are followed, in the event of any misuse of the internet, by a member of staff.

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 the schools and Local Authority/Regional Broadband Consortium so that it can be added to the banned or restricted list.

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 Head Teacher and e-Safety Leader immediately.
- Head Teacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
- Inform the Local Authority/Regional Broadband Consortium 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 Head Teacher 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 Head Teacher and Designated Person for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, Local Safeguarding Children’s Board Northamptonshire.
- 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 Head Teacher to implement appropriate sanctions.
- If illegal or inappropriate misuse is known, contact the Head Teacher or Chair of Governors (if allegation is made against the Head Teacher) and Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy.
- Contact CEOP (police) as necessary.

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

- Preserve any evidence.
- Inform the Head Teacher immediately and follow Child Protection Policy as necessary.
- Inform the Regional Broadband Consortium/Local Authority/Local Safeguarding Children's Board Northamptonshire 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 should be reported to the Head Teacher.

Staff Procedures Following Misuse by Children

The Head Teacher will ensure that these procedures are followed, in the event of any misuse of the internet, by a child:

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 the schools and Local Authority/Regional Broadband Consortium 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 children's use in the schools.

B. An inappropriate website is accessed deliberately:

- Any child found to be misusing the internet by not following the Acceptable Use Rules will have a letter sent home to parents/carers explaining the reason for suspending the child'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 is deemed to have misused technology against another child or adult.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.

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 Head Teacher 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.

- In the event of illegal or inappropriate misuse the Head Teacher must follow the Child Protection Policy
- Contact CEOP (police) as necessary.

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

- Preserve any evidence.
- Inform the Head Teacher immediately.
- Inform the Regional Broadband Consortium/Local Authority/Local Safeguarding Children's Board Northamptonshire 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 schools or setting:

- Preserve any evidence.
- Inform the Head Teacher immediately.

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

4. Indecent images of children found.
5. Incidents of 'grooming' behaviour.
6. 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 online.