

'What we learn with pleasure we never forget'

ONLINE SAFETY POLICY

Date Written: October 2017

Date of Review: July 2018

Headteacher.....

Date.....

Chair of Governors.....

Date.....

Introduction

The schools Online-Safety Policy covers the safe use of internet and electronic communications technologies. The internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to use technology safely, respectfully and responsibly; to locate, retrieve and exchange information using ICT and to use software or design, write and debug programs that accomplish specific goals.

The policy highlights the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It also provides safeguards and rules to guide staff, pupils and visitors in their online experiences.

Computer skills are vital to access life-long learning and employment. Our School has a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. We provide pupils with as safe an internet environment as possible, and teach them to be aware of, and respond responsibly to possible risks.

The schools Online-safety policy operates in conjunction with others, e.g. Behaviour, Anti-Bullying, Acceptable Use of ICT, Teaching and Learning, Data Protection, and Safeguarding Children.

Effective Practice in Online-Safety

Online-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A clear understanding of the Online-Safety Policy;
- Secure, filtered broadband from Suffolk County Council (E2BN) with secure firewall and antivirus software;
- A school network that complies with the National Education Network standards and specifications.

Core Principles of Internet Safety

Guided educational use

Significant educational benefits result from curriculum internet use including access to information from around the world and the ability to communicate widely and to publish easily. Curriculum internet use should be planned within a regulated and managed environment. Directed and successful internet use will also reduce the opportunities for activities of dubious worth.

Risk assessment

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks - to become 'internet wise'. Our school is fully aware of the risks, perform risk assessments and implement a policy for internet use. Pupils know how to respond if they come across inappropriate material or are contacted inappropriately online.

Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of internet and other communication technologies such as mobile phones. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

Regulation

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. For instance, un-moderated chat rooms, social media platforms and live video chat-rooms present immediate dangers and are banned. Fair rules prominently displayed at the point of access help pupils make responsible decisions.

Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. Strategies are selected to suit the school situation and their effectiveness monitored.

- There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

Teaching and learning

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to our primary age pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are taught in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

Managing Internet Access

Information system security

- The School's ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Pupils are unable to send emails to anyone outside of the school's domain but are taught how to identify suspicious emails from both known and unknown recipients.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. In the main, group photographs will be used rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Work can only be published with the permission of the pupil and parents/carers.
- Parents should be clearly informed of the school policy on image taking and publishing.

Social networking and personal publishing

- Pupils will not access social networking sites, but will be educated in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Managing filtering

- The schools' broadband provider is E2BN, who is recommended by SCC.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online-Safety Lead (Mr Head).
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are effective.

Managing 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 senior leadership team are aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during school time.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All staff must read the Acceptable Use Policy and sign to say they will adhere before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources form before being allowed to access the internet from the school site.
- Key Stage 2 have access to the Internet for independent research which is supervised by an adult.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor SCC can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the Online-safety policy is appropriate and effective.

Handling Online-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a safeguarding nature will be dealt with in accordance with school safeguarding procedures. (Our School's Online-Safety Policy has a flowchart of responses to an incident of concern.)
- Pupils and parents will be informed of the complaints procedure (see school's complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Communications Policy

Introducing the Online-safety policy to pupils

- Online-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in Online-Safety will be developed (with reference to the materials from SCC).
- Online-Safety training will be embedded across the curriculum.
- The schools E-Cadets (peer ambassadors) help to raise awareness and promote online safety within school.

Staff and the Online-Safety policy

- All staff will be referred to the School Online-Safety Policy and its importance explained.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user and that passwords must remain secret.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.
- All staff will sign the Schools Acceptable ICT use.

Parents' and carers' support

- Parents' and carers' attention will be drawn to the School Online-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of Online-safety resources for parents/carers.

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Any Parents / Carers wishing to access the internet via the Family Information Point must sign the schools Acceptable Use Policy.

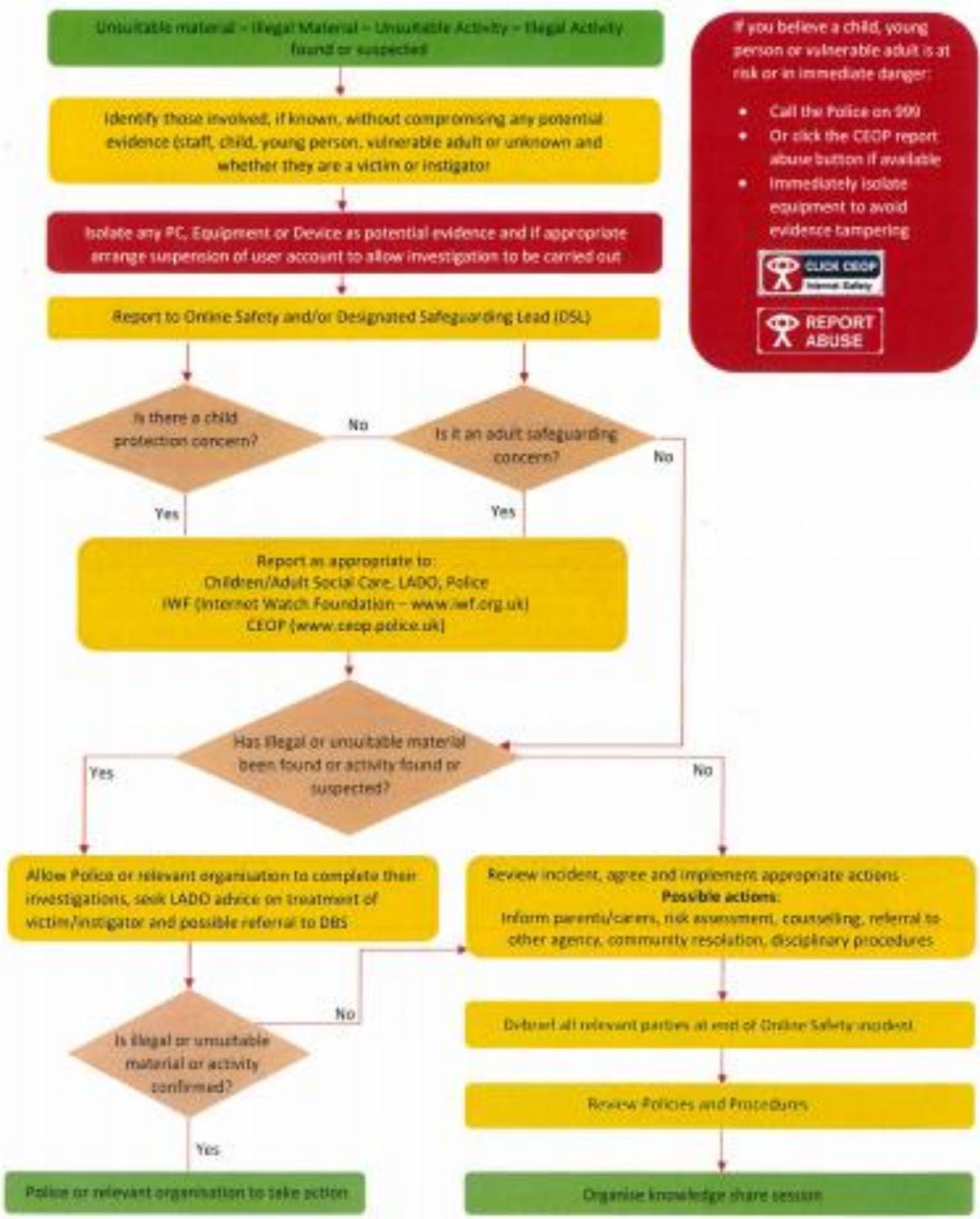
Appendix 1: Internet use

| Possible teaching and learning activities Activities | Key Online-safety issues | Relevant websites |
|---|---|---|
| Using search engines to access information from a range of websites. | Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with. | Google |
| Exchanging information with other pupils and asking questions of experts via e-mail or blogs. | Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. | Gmail education Pupils are only able to email within the domain |
| Publishing pupils' work on school and other websites. | Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils' work should only be published on "moderated sites" and by the school administrator. | Making the News SuperClubs Plus Headline History National Education Network Gallery Thimble Wix.Com Google Apps |
| Publishing images including photographs of pupils. | Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not | Making the News SuperClubs Plus Learninggrids Museum sites, etc. Digital Storytelling BBC - Primary Art National Education Network Gallery |

| | | |
|---|--|---|
| | <p>refer to the pupil by name.</p> <p>Staff must ensure that published images do not breach copyright laws.</p> | |
| <p>Communicating ideas within chat rooms or online forums.</p> | <p>Only chat rooms dedicated to educational use and that are moderated should be used.</p> <p>Access to other social networking sites should be blocked.</p> <p>Pupils should never give out personal information.</p> | <p>SuperClubs Plus</p> <p>FlashMeeting</p> <p>Class Dojo</p> |
| <p>Audio and video conferencing to gather information and share pupils' work.</p> | <p>Pupils should be supervised.</p> <p>Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.</p> | <p>FlashMeeting</p> <p>National Archives "On-Line"</p> <p>Global Leap</p> <p>JANET</p> <p>Videoconferencing Advisory Service (JVCS)</p> |

Appendix 2: Internet Safety Incident Flowchart

Online Safety Reporting Flowchart



If you believe a child, young person or vulnerable adult is at risk or in immediate danger:

- Call the Police on 999
- Or click the CEOP report abuse button if available
- Immediately isolate equipment to avoid evidence tampering




Carlton Colville Primary School

Internet User Agreement KS1

We have computers with access to the Internet which helps us with our learning. The following rules have been written to make sure I stay safe when using technology. By using ICT in school, I agree that I will follow these rules. These rules could also apply at home to keep me safe.

The Golden Rule - I will think before I click

- S** **SAFE** - I will only use the internet when an adult is with me.
 - I will not tell anyone any personal details like my phone number or last name.
 - I will keep my password secret, but I can tell my parents.
- M** **MEETING** - I will never agree to meet or web-chat with any online friends.
 - I will log off properly before closing the lid of laptops or walking away from computers.
- A** **ACCEPT** - I will not open any emails without my parents' permission.
 - I will not download or install any games from the Internet without my parents' permission.
- R** **RELIABLE** - I understand that some people online pretend to be someone else. Sometimes they pretend to be children, when they're actually grown up.
- T** **TELL** - I will tell a trusted adult if I come across something online that upsets me or I find something that I know I shouldn't have access to.
 - I will practice good netiquette and be polite when talking to people or writing online.

I won't put drinks on the table when using ICT.

I will be careful when carrying or using equipment.

I will only buy things online with my parents' permission.

September 2017

1) I won't keep online secrets from my parents.

2) I know that my parents want to make sure I'm safe and I will listen to them when they ask me not to do something because I know there is a reason.

3) I will help teach my parents more about computers and the Internet.

I understand the above rules and agree to keep them. I understand that if I break the rules, my access to the internet may be stopped.

PUPILS NAME: _____

CLASS: _____

Parental Agreement

I have discussed the agreement with my child and give permission for Internet access on these terms.

I understand the school has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported or unsafe behaviour.

I will support the school by promoting safe use of the internet and digital technology at home. I will inform the school if I have any concerns.

Signed _____ Parent/Carer Date: _____

Signed _____ Child Date: _____

September 2017

Carlton Colville Primary School

Internet User Agreement KS2

We have computers with access to the Internet which helps us with our learning. The following rules have been written to make sure I stay safe when using technology. By using ICT in school, I agree that I will follow these rules. These rules could also apply at home to keep me safe.

When using the internet I will follow the SMART rules:

S

SAFE - I will not give my name, address, telephone number, school, or my parents' name, address or telephone number to anyone I meet online. I will use a nickname as my username when online.

- I will not fill out any form online that asks me for any information about myself or my family without asking my parents first, even if it is from something I know.

M

MEETING - I will never agree to meet or web-chat with any online friends unless my parents say it's ok and they are with me.

A

ACCEPT - I will check who has sent me an email before opening it and I will not accept or open files that I do not recognise or feel are suspicious.

- I will not download anything from the Internet and if someone sends me a picture, I will not accept it without my parents' permission.

R

- I will check for viruses whenever I borrow a USB stick from someone.

RELIABLE - I understand that some people online pretend to be someone else. Sometimes they pretend to be children, when they're actually grown up.

T

TELL - I will tell a trusted adult if I come across something online that makes me feel uncomfortable or I find something that I know I shouldn't have access to.

- If someone asks me to do something I am not supposed to or don't want to, I will tell a trusted adult or I will press the report it button on the school website.

- I will not get into arguments online. If someone tries to start an argument with me or says something mean to me I won't answer them and will tell an adult. I will practice good netiquette.

- 1) I will not buy or order anything online without asking my parents permission or give out any credit-card information.

September 2017

- 2) I will ensure that any social media apps that I use are set as private and are not public. I will not stream live online and will check with my parents before uploading content.
- 3) I understand that I am responsible for any messages I send and the search terms I use when using the Internet or on my phone.
- 4) I won't keep online secrets from my parents.
- 5) I know that my parents want to make sure I'm safe and I will listen to them when they ask me not to do something because I know there is a reason.
- 6) I will help teach my parents more about computers and the Internet.

I understand the above rules and agree to keep them. I understand that if I break the rules, my access to the internet may be restricted or withdrawn. I understand that if an incident that happens outside of school is reported to my teacher or a member of staff, my parents will be informed.

PUPILS NAME: _____

CLASS: _____

Parental Agreement

I have discussed the agreement with my child and give permission for Internet access on these terms.

I understand the school has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported or unsafe behaviour.

I will support the school by promoting safe use of the internet and digital technology at home. I will inform the school if I have any concerns.

Signed _____ Parent/Carer Date: _____

Signed _____ Child Date: _____

September 2017

Appendix 4 :

Please visit the schools online safety page for parents to find a comprehensive list of useful website.

If you have any further concerns please do not hesitate to contact the Online Safety Lead (Mr Head) here in school.

Appendix 5 : Useful resources for teachers

BBC Chat Guide Video + "What If..." Discussion Cards
(Available from the 'Teachers Documents Folder' on the School's Intranet)

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/

Becta
<http://schools.becta.org.uk/index.php?section=is>

Chat Danger
www.chatdanger.com

Child Exploitation and Online Protection Centre
www.ceop.gov.uk

Childnet
www.childnet-int.org

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen
www.digizen.org

Kidsmart
www.kidsmart.org.uk

Think U Know
www.thinkuknow.co.uk

Safer Children in the Digital World
www.dfes.gov.uk/byronreview

NSPCC

Appendix 6 : Online-Safety Audit - Also see 360 Self-Evaluation

| | |
|---|------------|
| Has the school an Online-Safety Policy that complies with SCC guidance? | Y |
| Date of latest update: July 2017 | |
| The school Online-safety policy was agreed by governors on: July 2017 | |
| The policy is available for staff in: the office, the staff room and online. | |
| The policy is available for parents/carers at: The office and online | |
| The responsible member of the Senior Leadership Team is: Mr Head | |
| The responsible member of the Governing Body is: James Johnson | |
| The Designated Safeguarding Manager is: Ben Axon | |
| The Online-Safety Lead is: Mr Head | |
| Has Online-safety training been provided for both pupils and staff? | Y |
| Is there a clear procedure for a response to an incident of concern? | Y |
| Are SCC approved Online-Safety materials available to employees? | Y |
| Are employees given the Acceptable Use Policy during induction? | Y |
| Are all pupils aware of the School's Online-Safety Rules? | Y |
| Are Online-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils? | Y |
| Do parents/carers sign and return an agreement that their child will comply with the School Online-Safety Rules? | Y |
| Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced? | Y |
| Has an ICT security audit been initiated by SLT, possibly using external expertise? | Y (NSO) |
| Is personal data collected, stored and used according to the principles of the Data Protection Act? | Y |
| Is Internet access provided by an approved educational Internet service provider which complies with DFE requirements (e.g. SCC)? | Y |
| Is personal data collected, stored and used according to the principles of the Data Protection Act? | Y |