Bessacarr Primary School

E- Safety Policy

Introduction

The Internet is regarded as an essential part of learning. Used as a resource it is a vital part of children's learning. The curriculum requires pupils to learn how to locate, retrieve, and exchange information using ICT.

There are many devices used throughout school to access the Internet, including iPads, Laptops and Desktop computers amongst others. Schools Internet access is strictly filtered, but when accessing the Internet outside of school, children's access may not be filtered.

This policy will highlight how school effectively handles e-safety and will act as guidance on how parents can manage Internet safety outside of school. It will act alongside our ICT, Safeguarding, Data Protection, Bullying, Twitter and Mobile Device policies.

What is E-Safety?

E-Safety applies to accessing the Internet through various electronic devices such as iPads and wireless technology. It highlights the need to educate children and young people about the benefits and risk of using the Internet and provides safeguards and awareness for users to enable them to control their online experiences. Quite simply it is the safe and responsible use of technology.

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

- Responsible use of ICT by all staff and pupils
- Sound implementation of e-safety policy in both administration and curriculum, including secure network design and use.
- Safe and secure broadband from ACS including the effective management of content filtering.

<u>Designated Staff</u>

Bessacarr Primary has designated staff to deal with all e-safety issues:

Mr Daniel Smeaton – E-safety coordinator

Mrs Jo Howe – Inclusion leader/parent support

Mrs Sarah Cairns – Executive Head Teacher

Why is Internet use important?

- The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Use of the Internet is an integral part of the curriculum, whether used as a learning tool or for set tasks.
- Bessacarr Primary relies upon the Internet for the following:
- Phone system
- Registration/attendance
- Result tracking and recording
- School dinners
- Signing in
- Text to parents
- Remote access
- Remote backup
- Social media
- Learning platform (I am Learning)
- Behaviour systems
- Teaching resources

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes 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.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

- KS1 and KS2 Pupils will be asked to sign an 'Acceptable ICT Use Agreement'.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to Mr Smeaton or ACS.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils do not have access to personal e-mails in school.
- Every member of teaching and admin staff has their own school e-mail address. Staff are advised to use this for work related activities.
- The forwarding of chain letters is not permitted.
- The use of personal e-mails in school time and from school machines is advised against.

Social Networking

- Pupils are advised that when using sites out of school, to never give out personal details of any kind which may identify them or their location.
- Pupils are advised not to place personal photos on any social network space.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others by using the sites built in privacy settings.
- Pupils are aware of the CEOP button and what it should be used for.
- We use the 'Alright Charlie' (Blast) materials where age appropriate.
- Bessacarr Primary is active on social media through our Twitter accounts, these are administered by the school and all staff follow set guidelines highlighted in our Social Media policy.

Filtering

Bessacarr Primary will work in partnership with ACS to ensure filtering systems are as effective as possible.

Our Internet is fully filtered and is administered by Mr Daniel Smeaton.

Managing Emerging Technologies

- Emerging technologies will be examined by staff for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Children are not allowed to bring mobile phones to school.
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will use the school phone, where contact with pupils and parents is required.
- In accordance with our mobile device policy, staff are allowed to use their mobile phone for Twitter purposes as long as all photos are deleted before they leave school at the end of the day.

Published Content and the School Web Site

- The contact details on the Website are the school address and telephone number. The main email contact is Mr

Daniel Smeaton. Staff or pupils personal information will not be published.

- Mr Daniel Smeaton will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images

- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- Written permission from parents or carers will be obtained via a letter signed during induction before photographs of pupils are published on the school Website.
- Posts on any of our school Twitter accounts will not use pupils' full names.
- Staff may take photos of children on personal mobile devices as long as they adhere to the mobile device policy and all images are deleted before they leave the building.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.

- Virus protection (Sophos) will be installed and updated regularly.
- Security strategies will be discussed with ACS.

Protecting Personal Data

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

Assessing Risks

- The school will take reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Doncaster Metropolitan Borough Council can accept liability for the material accessed, or any consequences of Internet access.
- Bessacarr Primary will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by Mr Daniel Smeaton and Mrs Jo Howe.

- Any complaint about staff misuse will be referred to the Executive Headteacher or Head of School.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure which can be found on the school website.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Pupils will be informed that Internet use will be monitored.
- Children will be taught about the dangers of the Internet through e-safety assemblies.
- KS2 children will sign an acceptable use policy

Staff

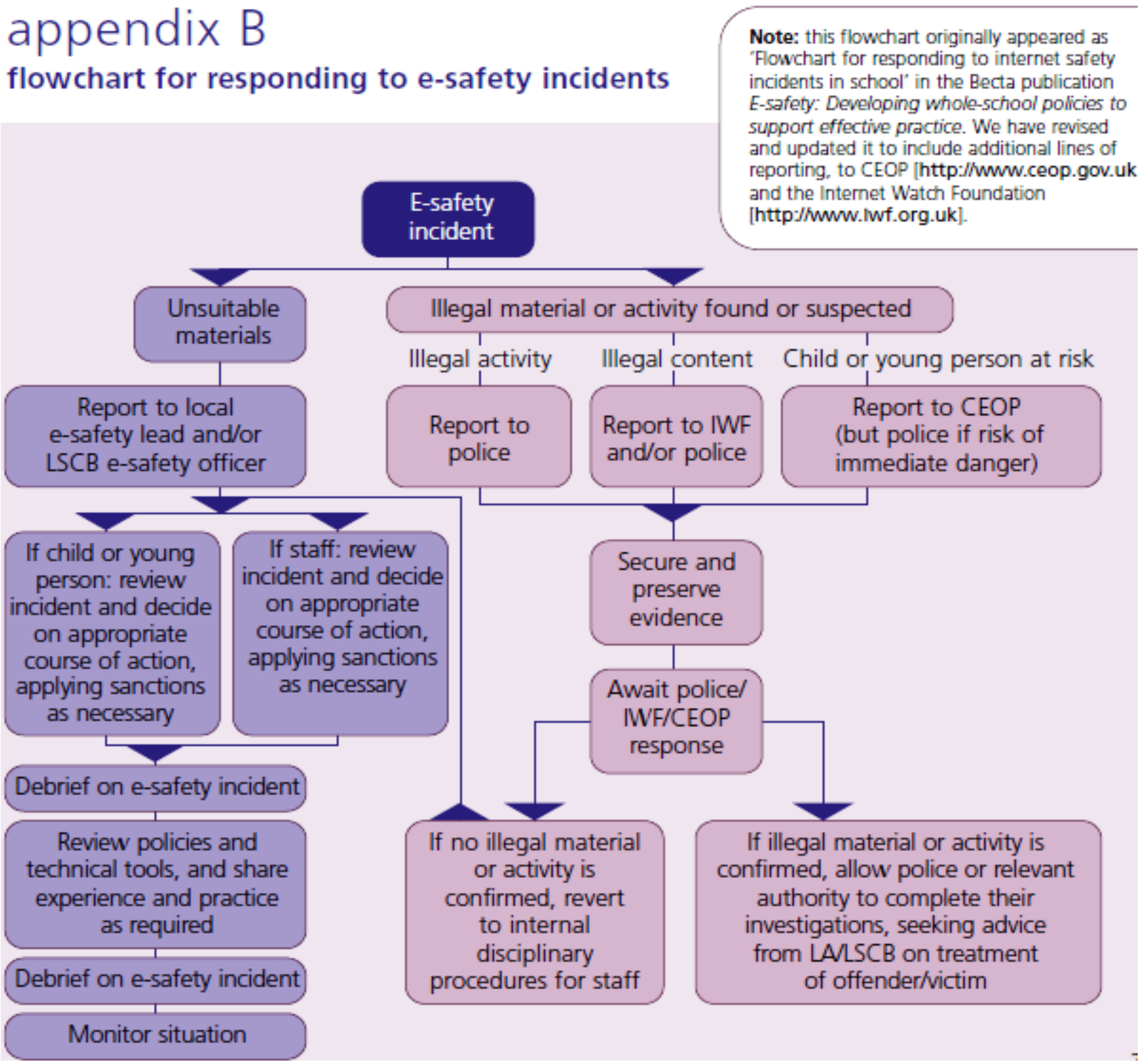
- All staff will be given the School e-Safety Policy and its importance explained.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will be trained in e-safety.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school Website and through E-Safety workshops.
- Regular newsletters will be sent out alerting parents to new dangers.

Flowchart for responding to e-safety incidents at Bessacarr Primary



appendix B

flowchart for responding to e-safety incidents

Note: this flowchart originally appeared as 'Flowchart for responding to internet safety incidents in school' in the Becta publication *E-safety: Developing whole-school policies to support effective practice*. We have revised and updated it to include additional lines of reporting, to CEOP [**http://www.ceop.gov.uk** and the Internet Watch Foundation [**http://www.iwf.org.uk**].

E-safety incident

Unsuitable materials

Report to local e-safety lead and/or LSCB e-safety officer

If child or young person: review incident and decide on appropriate course of action, applying sanctions as necessary

If staff: review incident and decide on appropriate course of action, applying sanctions as necessary

Debrief on e-safety incident

Review policies and technical tools, and share experience and practice as required

Debrief on e-safety incident

Monitor situation

Illegal material or activity found or suspected

Illegal activity

Illegal content

Child or young person at risk

Report to police

Report to IWF and/or police

Report to CEOP (but police if risk of immediate danger)

Secure and preserve evidence

Await police/ IWF/CEOP response

If no illegal material or activity is confirmed, revert to internal disciplinary procedures for staff

If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LA/LSCB on treatment of offender/victim

My Acceptable Use Policy

Inside School

I use ICT to help me to achieve my full potential in my learning.

- I will only access the system with my own classes login.
- I will not access other people's files
- I will only use the school devices and connectivity for school learning and home learning (unless I have permission from an adult)
- I will not bring to school any devices, to connect to the network or Internet, from outside school.
- I will ask permission from a member of staff before using the Internet
- I understand that it is not acceptable to post or upload images, of other people without their permission
- I understand that the school may check my computer files and activity and may monitor the Internet sites I visit.

Outside School

- The School advises adult supervision when using the Internet.

- I will never arrange to meet someone or give any personal information over the Internet (name, address, telephone number, name and address of school, bank details)
- I will report any unpleasant material (including on the Internet) or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself
- The messages I send will be polite and responsible

I have read and agree to the terms in this contract.
Signed (child): --

This policy is designed to protect all adults within Bessacarr Primary. Teachers, non-teaching staff and other adults must understand and sign this AUP. The basic principle of this AUP is that the school devices and connectivity may be used only to support teaching and learning and the professional development of the individual. Colleagues must ensure that they fully understand that the consequences of inappropriate activity can be severe and may lead to dismissal and criminal proceedings.

- I will not introduce a device to school systems without the permission of the administrator and ensuring it is free from malware, inappropriate/ illegal content
- I will not use another person's login details without their express permission.
- Adults are advised against the use of personal email for school use.
- Adults are only permitted to use mobile phones in school (including SMS, Bluetooth, wifi) within their own time.
- All adults who are new appointments will be provided with clear guidance on procedures
- The ICT technician is responsible for the procedure of adults who leave the school, e.g. removing files, changing passwords

I have read and understood the Acceptable Use Policy at Bessacarr Primary School and agree to these systems.

Signed:--

Role in school:--

Staff, governor and visitor

ICT Acceptable Use Agreement / Code of Conduct

This policy is in line with DMBC's 'Staff Code of Conduct for Schools and Educational Establishments'.

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr D Smeaton, school e-safety co-ordinator.

- I will only use the school's email/Internet/intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the head or governing body.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

- I will only use the approved, secure email system(s) for any school business.

- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, or accessed remotely. Personal data can only be accessed remotely when authorised by the Head or Governing body.

- I will not install any hardware or software without permission of the administrator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal, or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my line manager or head teacher.

What parents can do:

- You should make sure that children know never to give out personal details online or let people they have met contact them by phone or instant messaging. You should also:
- please be aware that moderated chat rooms designed specifically for children are not safe and are often targeted for grooming purposes. Therefore these should only be used under adult supervision.
- try not to be too hard on children if they have given their personal information to a stranger otherwise they may feel scared to talk to you about similar issues in future
- learn the language of chat so you understand what your child is chatting about (children tend to use abbreviations when chatting online)
- sign up to a chat room, forum, blog or Instant Messenger yourself to see how they work and learn the different ways children can chat
- place the computer/laptop/tablet in a family room so your child's online activities can be monitored
- show the same interest in your children's online friends as their real life friends
- ensure that children never arrange to meet online ‘friends’ in person.

- search for appropriate sites for you and your children to access together
- use child-friendly search engines but be aware that not all of them are 100 per cent safe - there have been instances of some advertising pornographic sites
- regularly check the history folder on your browser as it contains a list of previously visited sites - if you find an unsuitable site talk to your child and advise against it.

What to do if you think there is a problem:

No matter what safeguards you put in place, any child using the Internet is at risk of coming into contact with people who may try to take advantage of them. If you think this is happening, you should:

- let your children know that they can tell you if any chat makes them feel uncomfortable, worried or scared - let them know that you won't blame them
- if you suspect an abuser may be grooming your child, or your child is being stalked or harassed, you should contact the local police or Child Exploitation and Online Protection Centre

Blocking unsuitable sites:

Contact your broadband provider, they will be able to set up family friendly access.

Policy on Photographic and Video Images

Introduction

There are many occasions on which it is a good thing to make use of photographs and video images that include children. This is perfectly proper and to be encouraged. However, our school will do all it can to ensure that images are used properly, and that, as in all matters, risks are minimised, and our children kept safe and secure, whether at school or elsewhere. The aim of this policy is to establish the right balance between the proper use of technology and the safety of our children at all times.

Under the terms of the Data Protection Act 1998, all photographs and video images of children and staff alike are classified as personal data. This means that no image can be used for display or for school publicity etc., unless consent is given by or on behalf of the individual concerned.

Parental permission

All parents and carers will be asked to sign a consent form allowing their child to be photographed or videoed while taking part in school activities, and for the image to be used within the school. This form will be given to the parents or guardians of all children joining the school in each successive year. This 'rolling' consent will allow the school to take pictures of pupils engaged in educational activities such as sports events, drama productions, field trips, etc., and to use these pictures internally. Where parents or carers do not give their consent, then the children concerned will not have pictures taken of them.

All pictures taken will be appropriate, and will show children properly clothed for the activity they are engaged in. The school will do all it can to ensure that due sensitivity is shown in the choice and composition of these images.

The Internet

Only appropriate images will be used on the school Internet site, and children will not be identified by their name or address on the school website.

Twitter

Photographs of our children may be used on our Twitter pages, but only children with permission. No surnames will be used.

Mobile phones

We do not allow children to bring mobile phones into school. Adults may bring mobile phones, these can used to take pictures for Twitter, as long as they are deleted once they are uploaded.

Use of digital cameras

There are many ways in which the use of digital images is valuable for children's learning. For example, they may be used in art work or geography or science fieldwork.

Images will be made only as appropriate for school-related activities.

iPad

Staff may use iPads to take pictures in School. But all ipads must remain on School premises.

Children will be taught how to take pictures, but we will discourage them from taking pictures of each other, and they will be supervised by an adult when they have access to a digital camera.

All images of children will be deleted when they leave school.

Media publications

Sometimes, local or national media visit the school to follow up a news story. This is often to do with a notable achievement by a child or a group of children from the school. For example, the school may have raised money for a charity whose representative wants to receive the donation in person. In this situation, where children's images might be made public, the school will inform parents of the event in advance, and allow them to withdraw their child from the event if they so wish. Newspapers normally ask for the names of the children to go alongside the photographs; if parents or carers do not wish this to happen, then the school will not allow the individual to be photographed or filmed by the media concerned.