Angram Bank Primary School

E-Safety Policy

Approved by Governors on:	
Review Date:	September 2015
Review Date:	September 2016

Contents

Background

Scope of the policy

Roles and responsibilities

Curriculum

Use of digital and video images

Communications

Responding to incidents of misuse

Links to other organisations

This policy is in line with the whole school policy for Child Protection and Safeguarding Children, and the Safeguarding Sheffield Children's Board guidance for schools "E-Safeguarding, Version 9 Sept 15 "(www.safeguardingsheffieldchildren.org.uk).

Background

New technologies have become an integral part of the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which can open up new opportunities for everyone. Children and young people should have an entitlement to safe internet access at all times. A school e-safeguarding policy helps to ensure safe and appropriate use by all users.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Loss of privacy/control of personal information
- Grooming or exploitation by people who they make contact with on the internet
- The sharing/distribution of personal images and personal information without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- Being unable to judge the accuracy, relevance and reliability of information
- Plagiarism (copying a piece of written work or an idea and claiming it as your own) and breach or copyright (the illegal copying or use of creative work e.g. music, video, photographs, documents etc. without the owner's consent)
- Illegal downloading of music or video files
- Hacking into personal profiles, ineffective system security and viruses (giving access to personal and financial information)
- The potential for excessive use which may impact on the social and emotional development and learning of the child or young person

Many of these risks reflect situations in the off-line world and this e-safeguarding policy is used in conjunction with other school policies such as behaviour, anti-bullying and child protection policies.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build resilience to the risks to which pupils may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safeguarding policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people, their parents/carers and all staff to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Scope of the policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, work placement students, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is relevant to incidents of cyber-bullying, or other e-safeguarding incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safeguarding behaviour that take place out of school.

Roles and Responsibilities

Headteacher and Senior Leadership team

The Headteacher has overall responsibility for e-safeguarding all members of the school community through the day to day responsibility for e=safeguarding will be delegated to the E-Safety Co-ordinator. The Headteacher and Senior Leadership Team should be aware of the procedures to be followed int eh event of a serious e-safeguarding incident.

The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-Safety Co-ordinator

The e-safety co-ordinator takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents. They ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place, receive reports of e-safeguarding incidents and create a log to inform future e-safeguarding developments.

Governing Body

Governors are responsible for the approval of the E-Safeguarding Policy and for reviewing the effectiveness of the policy. This will be carried out at least annually at a full Governors meeting. Regular information about e-safety incidents, monitoring reports and any issues will be presented to the Governors. A member of the governing body has taken on the role of E-Safeguarding Governor.

Pupils

Pupils should:

- Read, understand and adhere to the Acceptable Use Policy for pupils, adopting safe and responsible behaviours when online in school and at home.
- Know and understand school policies on the use of mobile phones, digital cameras and hand held devices.
- Know and understand school policies on cyber-bullying.
- Understand the importance of adapting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to report incidents both in and out of school.
- Have a good understanding of research skills and legal issues relating to copying online content.

Parents

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way and in promoting the positive use of the internet and social media. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, Learning Platform and information about e-safety campaigns.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks.

- When using digital images, staff should inform an educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks:

Communication Technologies	Students/Pupils			
	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school			*X	
Use of mobile phones in lessons				X
Use of mobile phones in off duty times				X
Taking photos on personal mobile phones or other camera devices				X
Use of hand held devices eg PDAs, PSPs				X
Use of personal email addresses in school, or on school network				X
Use of school email for personal emails				X
Use of chat rooms/facilities				X
Use of instant messaging				X
Use of social networking sites				X
Use of blogs			X	

*Must be handed in to staff in main office for safe keeping at the start of the day and collected at home time.

When using communication technologies the school considers the following as good practice:

- Users must immediately report the receipt of any email or communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email or communication.
- Any digital communication between staff and pupils or parents/carers (email, chat, Learning Platform etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems.
- Pupils should be taught about email safety issues, such as the risks attached to the use of persona details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse.

If members of staff suspect that misuse might have taken place, it is essential that correct procedures are used to investigate. It is unlikely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Communication Technologies	Actions/Sanctions							
	Refer to class teacher	Refer to Headteacher	Refer to police	Refer to technical support staff for action re filtering/security etc	Inform parents/carers	Removal of network/internet access rights	Warning	Further saction eg detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone/digital camera/other handheld device	X						X	
Unauthorised use of social networking/instant messaging/personal email	X						X	
Unauthorised downloading or uploading of files		X			X		X	X
Allowing others to access school network by sharing username and passwords	X						X	
Attempting to access or accessing the school network, using another student's /pupil's account	X						X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X		X	
Corrupting or destroying the data of other users	X				X		X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X			X			X
Continued infringements of the above, following previous warnings or sanctions		X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X	X		X
Accidently accessing offensive or pornographic material and failing to report the incident	X						X	
Deliberately accessing or trying to access offensive or pornographic material		X			X	X		X

Links to other organsations

http://www.bbc.co.uk/cbbc/curations/stay-safe

https://www.ceop.police.uk/Ceop-Report/

http://www.saferinternet.org/

http://www.kidsmart.org.uk/

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/online-gaming-stay-safe-avoid-risks/

https://www.thinkuknow.co.uk/parents/

http://educateagainsthate.com/parents

http://www.childline.org.uk/Talk/AskSam/Pages/AskSam.aspx

https://www.safeguardingsheffieldchildren.org.uk/

https://www.safeguardingsheffieldchildren.org.uk/welcome/Schools-other-education-settings/Schools-Education-Settings-Policies-Procedures.html

cbbc Stay Safe

ins@fe

internet matters.org
learn about it / talk about it / deal with it

THINK U KNOW .co.uk

SHEFFIELD Safeguarding Children Board

KidSMART

ChildLine 0800 1111

CLICK CEOP Internet Safety
Worried about something you've seen online?
CLICK TO REPORT IT!

safeguarding children