Angram Bank Primary School

Online Safety Policy

Responsibility	Governors & SLT
Date of last review:	Summer 2021
Date of next review:	Summer 2022

Contents

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 Online Safety (www.safeguardingsheffieldchildren.org.uk).

Introduction

As a school, we understand that new technologies are essential resources for supporting teaching and learning. The internet and other digital devices play an important part in everyday life in an increasingly digital world. Our policy has been designed with this in mind to provide a safe teaching and learning environment for all pupils and staff.

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 offline world and this online safety 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. This online safety policy that follows explains how we intend to do this.

Scope of the policy

This policy applies to all members of the Angram Bank community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the 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 (SLT)

The Headteacher has overall responsibility for online safety all members of the school community through the day to day responsibility for online safety will be delegated to the online safety co-ordinator. The Headteacher and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online incident.

The Senior Leadership Team will receive regular monitoring reports from the online safety co-ordinator.

The designated safeguarding lead should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from sharing of personal data, access to illegal/inappropriate materials, inappropriate on-line contact with adults/strangers, potential or actual incidents of grooming, online-bullying.

Online Safety Co-ordinator

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

Governing Body

Governors are responsible for the approval of the online safety 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 online 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 online safety governor.

Network Manager/Technical staff

Angram Bank Primary School has a managed ICT service provided by an outside contractor. It is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school online safety policy and procedures.
Those with technical responsibilities are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leadership Team, Online Safety Lead for investigation
- That monitoring software/systems are implemented and updated as agreed

Pupils

Pupils:

- Are responsible for using the school digital technology systems in accordance with the school's procedures and expectations
- Know and understand school policies on the use of mobile phones, digital cameras and hand held devices
- Know and understand school policies on anti-bullying including cyber-bullying
- Understand the importance of adapting good online safety practice when using digital technologies out of school and realise that the school's online 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, our learning platform and information about online safety campaigns.

In promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events

- Access to parents' sections of the website/learning platform
- Their children's personal devices in the school/academy (following school's procedures)

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the staff handbook
- They report any suspected misuse or problem to the Headteacher, SLT, Online Safety Lead for investigation
- All digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Students/pupils understand and follow the Online Safety Policy and acceptable use policies
- Students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies in lessons and other school activities
- In lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and taught how to use search engines appropriately and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- A planned online safety curriculum is taught as part of Computing/RHSE lessons and is regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to question and validate the accuracy of information.
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

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 and educate pupils about the risks associated with the taking, using, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- 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.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. See GDPR policy for additional information.

When personal data is stored on any mobile device or removable media the:

- Data must be encrypted and password protected.
- Device must be password protected
- Device must be protected by up to date virus and malware checking software
- Data must be securely deleted from any devices

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- Where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- Will not transfer any school personal data to personal devices
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

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 other mobile devices e.g. tablets, gaming devices				X
Use of personal email addresses in school, or on school network				X
Use of school email for personal emails				X
Use of messaging apps				X
Use of social media			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 personal 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
- Whole class/group email addresses may be used at KS1, while students/pupils at KS2 and above will be provided with individual school/academy email addresses for educational use

Social Media - Protecting Professional Identity

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

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- Clear procedures on what is suitable to be published
- Clear processes for the administration and monitoring of these accounts

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school

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 sanction eg detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal		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 organisations

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

https://www.ceop.police.uk/Safety-Centre/

http://www.saferinternet.org/

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

https://www.nspcc.org.uk/keeping-children-safe/online-safety/

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

http://educateagainsthate.com/parents

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

https://www.betterinternetforkids.eu/en-GB/

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

KidSMART

ChildLine 0800 1111

SHEFFIELD Safeguarding Children Board

CLICK CEOP Internet Safety

Worried about something you've seen online?

CLICK TO REPORT IT!

safeguarding children