Seghill First School
E-Safety Policy (including appendices for Acceptable Use Policies)

Seghill First School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology;
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate;
- Ensure the school's Zip it! Block it! Flag it! approach to e-safety alongside the 3c's (Content, contact, conduct) is understood and used throughout school.

Parents will be sent an explanatory letter about the school's approach to e-safety. Parents will also be required to sign an Acceptable Use Agreement (Appendix 1) which will be valid throughout the pupil's time in Seghill First School.

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and Responsibilities

The Governing Body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governor who oversee e-safety is Mr Steve Best.

All governors will:

- Ensure that they have read and understand this policy;
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3).

The Head Teacher

The head teacher, working with senior staff, ICT Technician and Northumberland County Council is responsible for:

- Ensuring that staff understand this policy, and that it is being implemented consistently throughout the school;
- Addressing any online safety issues or incidents;
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy;

- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs);
- Liaising with other agencies and/or external services if necessary;
- Providing termly reports on e-safety in school to the governing board;
- Ensuring appropriate filtering and monitoring systems are in place, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy;
- Implementing this policy consistently;
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2 and 3), and ensuring that pupils follow the school's terms on acceptable use (appendix 1);
- Working with the head teacher to ensure that any online safety incidents are logged (appendix 5) and dealt with appropriately in line with this policy.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Northumberland LA can accept liability for the material accessed, or any consequences resulting from Internet use.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private;
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly;
- Recognise acceptable and unacceptable behaviour;
- Identify a range of ways to report concerns about content and contact.

The safe use of social media and the internet will also be covered in other subjects where relevant.
The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.
We allocate Internet access for staff and pupils on the basis of educational need. It should be clear who has Internet access and who has not.

Authorisation is as individuals and usage is fully supervised. Normally all pupils will be granted Internet access. Parental permission is required for Internet access in all cases as new pupils join Seghill First School. All staff must read and sign the Acceptable Use Policy annually - before using any school ICT resource.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. An e-safety workshop for parents will be offered in the autumn term of every year. This policy will also be shared with parents.

Online safety will also be discussed during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher and then passed to the head teacher.

The school's Zip it! Block it! Flag it! approach will be shared with all parents and displayed throughout the school.

Use of digital and video images

Staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital 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.
- In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital/video images. This is verbally stated at the beginning of every school event.
- Staff and volunteers 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 must not be used for such purposes.
- 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.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Seghill First School works with parents to help them understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Parents will be signposted to a range of useful and informative resources from agencies such as DCSF and Childnet to give practical advice and guidance on cyberbullying.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying:

- We will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others.
- We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Cyber-bullying will be addressed in class through the computing curriculum and PSHE education and also in assemblies.
- Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents of cyberbullying reported to the school will be recorded. The termly report to the governing board will identify any incidents of cyberbullying.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The headteacher will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Acceptable use of the internet in school

- All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1, 2 and 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
- Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
- We will monitor, through Northumberland LA Future Cloud, the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
- More information is set out in the acceptable use agreements in (appendices 1. 2 and 3).

Mobile devices in school

- Pupils are not allowed to bring mobile phones into school. Under certain circumstances exceptions can be discussed with the Head teacher, so that pupil mobile phones can be kept in the school office. Parents must complete the permission slip to acknowledge that the school takes no responsibility for phones which are left in the office.
- Staff are not permitted to use mobile phones during lessons or formal school time. All mobile phones must be turned off and stored securely. They can only be used on site by staff in the staffroom at designated break times during the school day.
- There are dangers for staff if personal phones are used to contact pupils or families and therefore this will only be done when authorised by a senior member of staff.
- All visitors to the school will be required to hand their mobile phone in to the school office whilst on site.

Staff using work devices outside school

- Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.
- Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. USB devices must not be used for any sensitive data.

- If staff have any concerns over the security of their device, they must seek advice from the ICT technician.
- Work devices must be used solely for work activities.

Email

- The staff and governors of Seghill First School will use Google mail, provided by Northumberland LA as a secure email system for any school business.
- All staff and governors must ensure that no personal emails are sent using the school Google mail system.
- When sending emails to more than one person all staff and governors must ensure that they use the BCC to add email addresses rather than revealing email addresses for persons not employed through Northumberland County Council.
- Only the approved email or other school approved communication systems should be used with pupils or parents/carers, and they should only be communicated with on appropriate school business.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputy DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The headteacher logs behaviour and safeguarding issues related to online safety. An incident report log can be found in (Appendix 5).

This policy will be reviewed annually by the head teacher. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Status:	**Statutory**
Reviewed	**20.11.19**
Next Review:	**November 2020**

.

Appendix 1

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.
- I must keep my passwords safe and secure. I will not share it and neither will I try to use someone else's password.
- Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved.
- It is forbidden to be involved in sending chain letters.
- Pupils must ask permission before accessing the Internet.
- School devices should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet.
- No programs on disc, CD Rom or external memory device should be brought in from home for use in school.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.
- I will not bring a mobile phone in to school unless I have permission from the head teacher, in which case the mobile phone will be handed in to the school office.
- I agree that the school will monitor the websites I visit.
- I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
- I will always use the school's ICT systems and internet responsibly.

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2	

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details

- I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree that the school will monitor the websites I visit.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will not store any sensitive data on USB devices.
- I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**