FORSBROOK C.E. (C) PRIMARY SCHOOL

Policy: Online Safety Policy

Adopted:	**October 2020**
Co-ordinator:	**Resources Committee**
Chair of Committee:	**Mrs C Bratt**
Next Review Date:	**October 2021**

Contents

.....

Online Safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and computing environment for Forsbrook Primary School.

> The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school […] to protect and educate the whole school […] community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate. (Keeping Pupils Safe in Education, 2019)

Forsbrook Primary acknowledges the assistance of Sheffield City Council and Kent County Council in providing content for this document.

1. 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

2. Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, *Keeping Pupils Safe in Education* and its advice for schools on *preventing and tackling bullying* and *searching, screening and confiscation*. It reflects existing legislation, *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 'good reason' to do so. This policy takes into account the *National Curriculum computing programmes of study.*

It has been agreed by senior management and approved by governors. The policy applies to all members of the Forsbrook Primary School community (including staff, pupils, volunteers, parents/carers, visitors and governors) who have access to and are users of the school computing systems.

The school's Online Safety Co-ordinator is Rebecca Cotton
The Online Safety Governor is Chris Bratt
The Online Safety Policy and its implementation shall be reviewed annually.

3. Roles and Responsibilities

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the school:

3.1 Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing body will:

- Ensure they read and understand this policy
- Agree to adhere to the terms on acceptable use of the schools ICT systems and the internet (appendix 2)

3.2 Headteacher

The Headteacher will:

- be responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 DSL and Senior Leaders

The above will:

- support the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role.
- be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.
- ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- liaise with any other agencies and/or external services if necessary
- provide regular reports on online safety in school to the Headteacher if necessary and/or governing board

This list is not intended to be exhaustive.

3.4 Online Safety Co-ordinator

The Online Safety Co-ordinator will:

- Take day-to-day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policy / documents.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Provides training and advice for staff.
- Liaise with school ICT technical staff.
- Receive reports of Online Safety incidents and creates a log of incidents as necessary to inform future Online Safety developments.

3.5 Technician

The technician will:

- Ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack and update safety mechanisms to prevent against viruses and malware
- Ensure that filtering and monitoring systems are in place and 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
- Confirm that the school meets required Online Safety technical requirements and any Local Authority/other relevant body Online Safety Policy/Guidance that may apply.
- Ensure that the users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- Make sure 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.
- Confirm that monitoring software are implemented and updated.

3.6 All Staff and Volunteers

All staff and volunteers will:

- Maintain an understanding of this policy
- Implement this policy consistently
- Agree to adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2) and ensure that pupils follow the schools term's on acceptable use (appendix 1)
- Have an up-to-date awareness of Online Safety matters and of the current school Online Safety policy and practices.

- Work with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensure that all incidents of cyber bullying are dealt with appropriately in line with the school behaviour policy
- Ensure that all digital communications with pupils/parents or carers should be on a professional level and only carried out using official school systems.
- Ensure that Online Safety is embedded in all aspects of the curriculum.
- Ensure that security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information. Refer to the social media policy for further guidance.

3.7 Parents

Parents/Carers play a crucial role in ensuring that their pupils understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parent workshops, newsletters, letters, and website information about national/local Online Safety campaigns/literature. Parents/Carers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

Parents are expected to:

- Notify the Headteacher or a member of staff of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further advice and guidance on keeping pupils safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf
- CEOP https://www.ceop.police.uk/safety-centre/

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating Pupils About Online Safety

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience.

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

Pupils will be given clear objectives for Internet use and taught what is acceptable and what is not with reference being made to the Pupil AUP on a regular basis. .

The safe use of social media and the internet will also be covered in other subjects where relevant. All pupils will have digital literacy units that focus on different elements of staying safe online. These units include topics from how to use a search engine, our digital footprint and cyber bullying.

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.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

When pupils are directed to websites as part of home learning they will have been checked for appropriateness by the teacher setting the learning.

5. 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. This policy will also be shared with parents.

Online safety will also be covered in parental workshops.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Cyber-bullying

6.1 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's Social Media and/or behaviour policy.)

6.2 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. Class teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 16 for more detail).

The school also sends information on cyber-bullying to parents via the school website so that they are aware of the signs, how to report it and how they can support children who may be affected.

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 DSL 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.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet

devices, where they believe there is a 'good reason' to do so. This is in line with the school's terms and conditions of pupils bringing and using own devices for education use during distance learning or otherwise.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Policy Central Enterprise (PCE)

The school computing network is monitored using the PCE tool. Policy Central Enterprise detects potentially inappropriate content and conduct as soon as it appears on the screen, is typed in by the user or received by the user. A screen capture is taken of every incident detailing the time and date of capture, machine name, username and reason for capture. A weekly headline summary is produced from the system detailing captures of particular interest to alert the person monitoring the system, (Headteacher, DSL, SLT). These particular violations will be investigated and dealt with in accordance to the Acceptable Use Policy (AUP), behaviour policy and other relevant school policies.

8. Authorised Internet Access.

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to Online Safety and agree to its use:

- The school will maintain a current record of all staff and pupils who are granted 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 and asked to sign and return a consent form for pupil access.

- Only authorised equipment, software and Internet access can be used within the school.

9. E-mail and Communications

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of Online Safety:

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, etc) must be professional in tone and content.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

10. Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils, by permission of the Headteacher, can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office or class teacher at 8:45 and collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.
- All digital communications with pupils/parents or carers should be on a professional level and only carried out using official school systems.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom whilst the pupils are present.
- Staff may use their mobile phones during break times or during the lunch period.
- Parents cannot use their personal mobile phones on school trips to take pictures of the pupils.

11. Digital/Video Cameras

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred to the schools network.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Parents will not use digital cameras, mobile phones or video equipment at school unless specifically authorised by staff.
- The Headteacher or nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.
- All images are stored on the secure school network.
- Digital images are disposed of in accordance with the Data Protection Act.

12. 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.

13. Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Consent from parents will be obtained before photographs of pupils are published on the school Web site. Photographs and videos that include pupils will be selected carefully in accordance with permission given by parents/guardians to appear on the school website and/or social media sites.
- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- Work can only be published with the permission of the pupil and parents.

- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

14. Assessing Risks

The school will take all 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. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

15. Handling Online Safety Complaints

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.

- 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 child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

16. 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 Headteacher and 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.

17. 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
- Social Media policy

Appendix 1: acceptable use policy (pupils and parents/carers)

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
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

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.

Signed (pupil):	**Date:**

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 policy (staff, governors, volunteers and visitors)

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 let the designated safeguarding lead (DSL) and ICT manager 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:**

Appendix 3: online safety training needs – self-audit for staff

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.	

Appendix 4: online safety incident report log

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**

Appendix 5: Possible Actions and Sanctions

	Actions / Sanctions							
Pupils Incidents	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		X			
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		X			X			
Unauthorised / inappropriate use of social media / messaging apps / personal email		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 pupil's account		X					X	
Attempting to access or accessing the school network, using the account of a member of staff		X					X	
Corrupting or destroying the data of other users		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
Using proxy sites or other means to subvert the school's filtering system		X				X		X
Accidentally 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			