BETTER TOGETHER

Shawlands Primary School

e-Safety Policy

REVIEWED ANNUALLY

Reviewed by D Thompson SUMMER 2023

Approved by the Governing Body on:

Signed……………………………………

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

Our pupils increasingly use mobile phones, tablets and computers on a daily basis. They are a source of fun, entertainment, communication and education. However, we know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive communications, to enticing children to engage in sexually harmful conversations, webcam photography, encouraging radicalisation or arranging face-to-face meetings. The school's online safety policy explains how we aim to keep pupils safe in school which includes reasonable filters and monitoring which are outsourced to our ICT Technical Support, Trust IT.

Cyberbullying and sexting by pupils, via texts and emails, will be treated as seriously as any other type of bullying and in the absence of a child protection concern will be managed through our anti-bullying and behaviour management procedures.

Chatrooms and some social networking sites are the more obvious sources of inappropriate and harmful behaviour and pupils are not allowed to access these sites in school. Some pupils will undoubtedly be 'chatting' outside school and are educated about the risks of this through PSHE/SRE.

Parents are encouraged to consider measures to keep their children safe when using social media; this includes an annual e-safety workshop for parents. Our approach to online safeguarding covers the four broad areas of risk (the four c's):

- **Content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- **Contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you pupils, students or staff are felt to be at risk, this will always be reported to the AntiPhishing Working Group (https://apwg.org/). Our Acceptable IT Use Policy (AUP) for staff and pupils will be enforced and parents are also informed of expectations.

Commented [DT1]: Content broken down into the 4 Cs as recommended by recent Safeguarding review

Our e-Safety Policy has been written by the ICT Coordinator using Barnsley Learning Network and government guidance. It has been agreed by senior management and governors. It will be reviewed annually.

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 and 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 (DfE) statutory safeguarding guidance, Keeping Children Safe in Education (2023), and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- 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 and the relationships, sex and health education government guidance.

3. Why is Internet Use Important?

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

4. How Will Internet Use Enhance Learning?

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
Pupils will learn appropriate Internet use, what is and what is not appropriate use, and given clear objectives for Internet use.
Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
Pupils will be educated in the effective use of the Internet. They will be taught a range of skills including researching, for example knowledge location, retrieval and evaluation as well as skills such as uploading work and images to share with other learners.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LA and DFE.

5. Online Safety Education

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and lessons
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil AUP (Appropriate Use Policy). and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms and where devices are stored and charged
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Commented [DT2]: Do we have this info on log-in screens?

6. Roles and Responsibilities

All staff have a responsibility for Safeguarding no matter what their role. These are outlined clearly in Part One of Keeping Children Safe in Education 2023

6.1 The Governing Body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board 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). All governors will: Ensure that they have read and understand this policy, and agree and adhere to the terms on AUP

6.2 The Headteacher

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

6.3 The Designated Safeguarding Lead

Details of the school's DSL are set out in our child protection and safeguarding policy as well relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy (this will be on CPOMS in line with the Child-Protection and Behaviour Policies)
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy (this will be on CPOMS in line with the Child-Protection and Anti-Bullying Policies)
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

6.4 The ICT Manager

The ICT manager is responsible for:

- Working with ICT Support (Trust-IT) to lock access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this and other relevant policies
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Anti-Bullying Policy

This list is not intended to be exhaustive.

6.5 All Staff and Volunteers

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

- Maintaining an understanding of this policy and implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school b Anti-Bullying Policy

This list is not intended to be exhaustive.

6.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher 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
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
    - What are the issues? - UK Safer Internet Centre Hot topics –
    - Childnet International Parent factsheet - Childnet International

7 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.

8 Some current issues

8.1 Child on Child Abuse – sexting/cyberbullying/sexual assaults

All staff must be aware that children are capable of abusing their peers, and that safeguarding issues can manifest themselves as child on child abuse. At Shawlands we have a culture of 'it can happen here' and where it does it will not be ignored or tolerated. Such incidents regardless of the genders of those involved must always be taken seriously and acted upon under the appropriate policy e.g. the safeguarding or bullying policy, and not dismissed as 'banter' or 'part of growing up'. Victims as well as perpetrators will be supported through the school's pastoral system. All incidents will be dealt with on a case-by-case basis, supported by social care and the police if required. Any hate crime/incident will be reported through local reporting mechanisms.

At all times children will be reminded that the law is there to protect, not criminalise, children. Child on child abuse can include any form of bullying, abuse (including sexual), physical (including online threats of violence or harm) and causing someone to engage in sexual activity without consent, though we recognise that abuse does not always have to by physical or violent and may include online behaviours.

8.2 Sexting

Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages. They can be sent using mobiles, tablets, smartphones, laptops - any device that allows you to share media and messages.

School will follow the updated guidance;

http://swgfl.org.uk/magazine/Managing-Sexting-Incidents/Sexting-Advice.aspx
https://www.gov.uk/government/publications/searching-screening-and-confiscation

In practice, this means that any concerns will be sensitively investigated by the DSL or DDSL, with parents of both any perpetrators and victims being informed. Follow-up actions will be proportionate and restorative, with an emphasis on helping all children involved being supported in order to move on positively.

8.3 Bullying

Bullying is usually defined as behaviour that is:

- repeated
- intended to hurt someone either physically or emotionally
- often aimed at certain groups, for example because of race, religion, gender or sexual orientation

It is a very serious issue that can cause considerable anxiety and distress. At its most serious level, bullying can have a disastrous effect on a child's wellbeing and in very rare cases has been a feature in the suicide of some young people.

All incidences of bullying, including cyber-bullying and prejudice-based bullying will be recorded and reported and will be managed through our Behaviour and Anti-Bullying Policies.

The school's Behaviour and Anti-Bullying Policies are available on the school website, and paper copies are available on request by parents.

If the bullying is particularly serious, or the tackling bullying procedures are deemed to be ineffective, the Headteacher and the DSL will consider implementing child protection procedures including fixed-term suspension.

Any bullying incidents including discriminatory and prejudicial behaviour e.g. racist, disability and homophobic bullying and use of derogatory language will be dealt with, recorded and analysed in-line with the school's Behaviour and Anti-Bullying / Anti-Racism Policies. Parents will be notified and restorative work done with the child involved to prevent repeated incidents. If necessary, a Prevent referral may be made.

9 Use of Digital and Video Images - Photographic, Video

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and 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.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might cause embarrassment or 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 not include full names
• Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website

10 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.

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. Any USB devices containing data relating to the school must be encrypted.

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

11 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. 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.

12 How Will the Risks Be Assessed?

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Children will be taught how to best deal with this situation.

13 How Will Complaints Regarding Internet Use Be Handled?

Parents and teachers must know how and where to report incidents. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy.

Complaints of a child protection nature must be dealt with in accordance with the school and LA child protection procedures.

a) Children using messaging and email facilities inappropriately may have their user name and password withdrawn, for a period of time to be decided by the class teacher, depending on the severity of the misuse. Responsibility for handling incidents regarding child protection will be delegated to the Headteacher.
b) Any complaint about staff misuse must be referred to the Headteacher.
c) Parents and pupils will need to work in partnership with staff to resolve issues.
d) There may be occasions when the police must be contacted. Early contact should be made to establish the legal position and discuss strategies.