



Shardlow Primary School

Aspire Achieve Thrive



Online Safety Policy

Approved by:	Local Governing Body
Date:	October 2025
Minute no:	Out of Committee
Version:	V5
Review cycle:	Annual



Version Control

Version	Date	Author	Changes
V1	19.06.2019	JD	Replaced E-safety Policy
V2	6.3.2020	JD	Updated Online Safety Policy to reflect the changes from the safeguarding board to the new Derbyshire partnership and KCSIE19
V3	20.1.2022	JD	Edited terminology, ensured policy up to date with latest Derbyshire guidance and referenced child friendly online safety policy.
V4	13.1.2024	JD	
V5	2.10.2025	JD	Edited to ensure policy up to date with latest Derbyshire guidance and in line with KCSIE. Reformatted

Contents

1. Introduction.....	0
2. Intent.....	1
3. Implementation	1
4. Roles and Responsibilities	3
5. Education – Pupils.....	5
6. Procedures for Responding to Specific Online Incidents or Concerns	7
7. Impact	13
8. Reporting Procedure.....	13
9. Social Media.....	14
10. Monitoring & review.....	15

Appendix 1 - Online Safety - Prevention Activities

Appendix 2 - Adult Guidelines for school internet use

Appendix 3 - Template Permission Letter

Appendix 4 - Pupil guidelines for internet use in school

Appendix 5 - Legislation

Appendix 6 - Links to other organisations/documents

Appendix 7 - Rules

Appendix 8 - Pupils & parents online safety contract

1. Introduction

- 1.1 At Shardlow Primary School we are aware of the responsibility we have to educate our pupils on online safety issues; teaching our children appropriate conduct to enable them to extend their use of computers, technology and the internet in and beyond the context of the classroom. The safety and legal rights of our pupils are of paramount importance to our school. We endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used. Online safety posters are prominently displayed around school. Pupils are taught a wide range of online safety topics, including responsible use, cyberbullying awareness, digital footprints, and data privacy.
- 1.2 This online safety policy should be viewed in conjunction with the acceptable use of IT policy. It will be shared all staff who must sign once they have read it. New staff will receive online safety training during their induction, in addition to reading the acceptable use policy. Supply teachers must sign an acceptable use of ICT agreement before using technology equipment in school. Our effective online safety practice is shared with other schools in the One Academy Trust when Computing co-ordinators meet. We also work closely with parents and guardians to promote safe online practices at home and encourage them to be aware of the tools and resources available to support their children's online safety.

- 1.3 Online safety is recognised as an integral part of leadership at Shardlow Primary School. All staff have completed Hays online safeguarding training which highlights the issues raised by CEOP (Child Exploitation and Online Protection.)
- 1.4 In the event of any online safety-related safeguarding concerns, the school's established safeguarding procedures should be followed. Please refer to the Safeguarding Policy for further details on reporting and managing concerns. Kylie Magner (headteacher) has overall responsibility. Sally Marshall and Julia Gillard are also designated safeguarding leads, and those to report to in the event of any concerns. All teachers are responsible for promoting and actively advocating safe behaviours in their classrooms and follow school online safety procedures.

2. Intent

- 2.1 The intent of this policy is to:
- Ensure that all pupils and staff use the Internet responsibly for educational, professional, and approved personal purposes.
 - Ensure that Internet use is monitored using appropriate filtering and monitoring tools, ensuring compliance with the school's online safety policy and safeguarding guidelines.
 - Provide a system to protect staff and pupils from inappropriate sites, information, and individuals.
 - Establish rules that are consistent with procedures already in place for Internet use.
- 2.2 The Internet is an essential tool for communication and learning. The Government has emphasized the need for schools to make full use of the Internet to support educational activities. Our school connects to the Internet via broadband provided by AIT and supported by Smoothwall Monitor which provides filtering and monitoring services designed to block access to inappropriate content. Online incidents picked up by Smoothwall Monitor are reported to the Headteacher and AIT for review.
- 2.3 There is no regulatory body for the Internet, and since anyone can publish content online, it's not possible to guarantee that filtering systems will be 100% effective. For this reason, the school has put additional safety measures in place, including regular reviews of filtering and monitoring systems, to ensure the safest possible online environment for our pupils and staff.

3. Implementation

- 3.1 There are six key elements in place to ensure that the use of the internet is safe and effective:

1. Information for Parents: Regular updates and guidance are provided to parents, highlighting the use of the internet and the importance of online safety.
 2. Adequate Staff Training: Staff receive ongoing training to ensure they are equipped with the knowledge and skills to support safe and effective internet use.
 3. Supervision of Children: Children are closely supervised while using the internet to ensure their safety and well-being.
 4. A Contract Between Child, Parent, and School: A clear agreement is established between the child, parent, and school, outlining expectations for safe internet use.
 5. Filtering of Undesirable Sites: The school uses an educational internet service provider to filter out inappropriate or harmful websites, ensuring safe browsing.
 6. Clear Rules and Sanctions: A set of clear rules regarding internet use is in place, with sanctions for pupils who fail to adhere to these guidelines.
- 3.2 Ongoing Guidelines and Training for Pupils: At the beginning of each academic year, and throughout the year during safety weeks, pupils receive clear guidelines on internet safety. Children are regularly reminded of the risks associated with networking and social media sites.

Internet Access

- 3.3 In addition to standalone computing lessons, teachers integrate online safety and internet use into their broader classroom practice and across the whole school (see Appendix A). Pupils are encouraged to utilize the wealth of information available on the internet, and they will be taught the skills necessary to critically analyse and evaluate these resources.
- 3.4 The availability of online resources has greatly expanded the range of educational materials accessible to classrooms. Electronic research skills have become essential in preparing future employees for the information age. Staff will support pupils in developing these skills, ensuring they are applied appropriately within the wider curriculum.
- 3.5 The school's internet facilities are available to three categories of users:
- Staff
 - Pupils
 - Visitors
- 3.6 Pupils will require a signed Internet Permission Letter from a parent or carer to access the school's internet services. A list of internet usage guidelines will be published and all pupils are expected to adhere to these rules. These guidelines will be reviewed regularly.
- 3.7 All staff members are responsible for explaining the rules and their implications to pupils. Staff should be vigilant and aware of potential misuses of internet access, understanding their responsibility to ensure the safety and well-being of the pupils in their care.

4. Roles and Responsibilities

- 4.1 This section outlines the online safety roles and responsibilities of individuals and groups within the school/academy:

Governors

- 4.2 Governors are responsible for the approval of the Online Safety Policy and for reviewing its effectiveness. This is achieved through regular receipt of information about online safety incidents and monitoring reports. A member of the Governing Body is assigned the role of link governor for Online Safety, usually as part of a wider safeguarding role. Their responsibilities include:

- Meetings with the Online Safety Co-ordinator/Officer.
- Monitoring of online safety incident logs.
- Monitoring of filtering/change control logs.
- Reporting to relevant governing body meetings.

Headteacher/Principal and Senior Leaders

- 4.3 The Headteacher has a duty of care to ensure the safety (including online safety) of all members of the school community.
- 4.4 The Headteacher and Designated Safeguarding Leads (DSLs) should be aware of the procedures to follow in the event of a serious online safety allegation made against a member of staff.
- 4.5 The Headteacher is responsible for ensuring that DSLs and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other staff members where needed.
- 4.6 The Headteacher will ensure a system is in place for monitoring and supporting staff who are responsible for online safety monitoring roles, providing both a safety net and necessary support for these staff members.

Designated Safeguarding Leads (DSLs)

- 4.7 The DSL takes day-to-day responsibility for online safety issues and plays a leading role in establishing and reviewing the school's online safety policies and documents.
- 4.8 The DSL ensures that all staff are aware of the procedures to follow if an online safety incident occurs.
- 4.9 The DSL provides training and advice to staff members.
- 4.10 The DSL liaises with the Local Authority/MAT/relevant body and school technical staff.
- 4.11 The DSL receives reports of online safety incidents and maintains a log of incidents to inform future online safety developments.
- 4.12 The DSL meets regularly with the Online Safety Governor to discuss current issues, review incident logs, and filtering/change control logs.

4.13 The DSL reports regularly to the Senior Leadership Team.

Teaching and Support Staff

4.14 Teaching and support staff are responsible for ensuring that:

- They maintain an up-to-date awareness of online safety matters and the current school Online Safety Policy and practices.
- They have read, understood, and signed the Staff Acceptable Use Policy (AUP).
- They report any suspected misuse or online safety concerns to the Headteacher/DSL for investigation.
- All digital communications with pupils, parents, or carers should be professional and conducted using official school systems.
- Online safety issues are integrated into all aspects of the curriculum and other school activities.
- Pupils understand and adhere to the Online Safety Policy and acceptable use policies.
- 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, mobile devices, cameras, etc., in lessons and other school activities (where allowed), and implement current policies regarding these devices.

4.15 In lessons where internet use is pre-planned, pupils should be guided to websites that have been checked for suitability, and processes should be in place to address any unsuitable material encountered during internet searches.

Designated Safeguarding Lead (DSL)/Designated Person/Officer

4.16 The DSL (or designated person/officer) should be trained in online safety issues and be aware of the potential child protection/safeguarding issues that can arise from:

- The sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate online contact with adults/strangers.
- Potential or actual incidents of grooming.
- Online bullying.

Pupils

4.17 Pupils are responsible for:

- Using the school's digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- Having a good understanding of research skills and the need to avoid plagiarism while respecting copyright regulations.
- Understanding the importance of reporting abuse, misuse, or access to inappropriate material and knowing how to do so.

- Adhering to policies regarding the use of mobile devices and digital cameras, including the taking and use of images and policies on online bullying.
- Recognizing the importance of adopting good online safety practices when using digital technologies outside of school and understanding that the school's Online Safety Policy covers actions outside of school when they relate to school membership.

Parents/Carers

- 4.18 Parents and carers play a crucial role in helping their children understand the need to use the internet and mobile devices appropriately. The school will provide information to help parents understand online safety issues through various channels, such as:
- Parents' evenings
 - Newsletters
 - Letters
 - Website updates
 - Information about national and local online safety campaigns
- 4.19 Parents and carers will be encouraged to support the school in promoting good online safety practices and to follow guidelines on the appropriate use of:
- Digital and video images taken at school events.
 - Access to parents' sections of the school website/learning platform and online pupil records.

5. Education – Pupils

- 5.1 While regulation and technical solutions are vital, they must be complemented by educating pupils to take a responsible approach to online safety. The education of pupils in online safety and digital literacy is an essential component of the school's overall online safety provision. Children and young people need the help and support of the school to recognize and avoid online safety risks and build resilience.
- 5.2 Online safety should be a focus across the curriculum, and staff should reinforce online safety messages in all areas of learning. The online safety curriculum should be broad, relevant, and provide progression, with opportunities for creative activities. This will be provided in the following ways:
- A planned online safety curriculum should be integrated into the Computing curriculum and regularly revisited.
 - Key online safety messages should be reinforced through a program of assemblies and tutorial/pastoral activities.
 - Pupils should be taught in all lessons to critically evaluate the materials and content they access online and be guided in validating the accuracy of information.
 - Pupils should be taught to acknowledge the sources of information they use and to respect copyright when utilizing material accessed on the internet.

- Pupils should be supported in building resilience to radicalization by providing a safe space for debating controversial issues and helping them understand how they can influence and participate in decision-making.
- Pupils should understand the need for the Pupil Acceptable Use Agreement and be encouraged to adopt safe and responsible use both within and outside the school.
- Staff should act as role models in their use of digital technologies, the internet, and mobile devices.
- In lessons where internet use is pre-planned, it is best practice to guide pupils to websites that have been checked for suitability and have processes in place for addressing any unsuitable material found during internet searches.
- When pupils are allowed to freely search the internet, staff should be vigilant in monitoring the websites they visit.
- It is accepted that, for educational reasons, pupils may sometimes need to research topics (e.g. racism, drugs, discrimination) that would typically be blocked. In these cases, staff can request that the Technical Staff (or other relevant personnel) temporarily remove certain sites from the filtered list for the duration of the study. Requests should be auditable and include clear reasons for the need.

5.3 **Breaches of the Acceptable Use Policy** may result in one or more of the following actions:

- A warning
- Removal of email and/or internet access
- A letter home to parents
- A report to the Governors
- A report to appropriate external agencies

Vulnerable Learners

5.4 Shardlow Primary School recognizes that some learners are more vulnerable online due to various factors, such as:

- Children in care
- Children with Special Educational Needs and Disabilities (SEND) or mental health needs
- Children with English as an Additional Language (EAL)
- Children experiencing trauma or loss

5.5 We will ensure that differentiated and age-appropriate online safety education, access, and support are provided to vulnerable learners. When implementing an online safety policy and curriculum, we will seek input from specialist staff as needed, including the SENCO and Child in Care Designated Teacher.

Security When Using the Internet

5.6 Internet access is filtered by Smoothwall Monitor.

- 5.7 Pupils are not allowed to bring in disks or upload files from home unless they have been checked and virus-scanned by a teacher.
- 5.8 Pupils are not permitted to access 'open' newsgroups or chat rooms.
- 5.9 Any inappropriate material found on the internet will be reported to the internet service provider. The Computing Lead will serve as the point of contact for reporting these incidents.

Reducing Online Risk

- 5.10 We recognize that the internet is a constantly evolving environment, with new apps, devices, websites, and content emerging rapidly. To mitigate online risks, we will:
- Regularly review the methods used to identify, assess, and minimize online risks.
 - Examine emerging technologies for educational benefit and conduct appropriate risk assessments before allowing their use in the school setting.
 - Ensure appropriate filtering and monitoring measures are in place and take all reasonable precautions to ensure users can only access suitable material.
 - Due to the global and interconnected nature of the internet, it is impossible to guarantee that unsuitable material will not be accessed via our computers or devices.
- 5.11 All members of the school community are made aware of our expectations regarding safe and appropriate online behaviour. This includes the importance of not posting content, comments, images, or videos that could harm, distress, or offend members of the community. These expectations are clearly outlined in our Acceptable Use Policies and reinforced through various educational and training methods.

6. Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children

- 6.1 Our school/ setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" guidance and part 5 of 'Keeping children safe in education'.
- Shardlow Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
- Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- We also recognise that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

- We recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Shardlow Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
- Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.

6.2 If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.

- Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Reform children's behaviour using our behaviour policy
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL (or deputy) will discuss this with Derbyshire Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Youth Produced Sexual Imagery ("Sexting")

- 6.3 Shardlow Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- 6.4 We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- 6.5 Shardlow Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by

implementing preventative approaches, via a range of age and ability appropriate educational methods.

- 6.6 We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- 6.7 We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- 6.8 We will not:
- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
 - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
 - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- 6.9 If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
- Act in accordance with our child protection policies and the relevant Derbyshire Safeguarding Child Board's procedures.
 - Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
 - Store the device securely.
 - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
 - Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
 - Inform parents and carers, if appropriate, about the incident and how it is being managed.
 - Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
 - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
 - Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
 - Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
 - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- 6.10 Shardlow Primary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- 6.11 We also recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- 6.12 We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- 6.13 We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- 6.14 We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community.
- 6.15 If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
- Act in accordance with our child protection policies and the relevant Derbyshire Safeguarding Child Board's procedures.
 - If appropriate, store any devices involved securely.
 - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Derbyshire police via 101, or 999 if a child is at immediate risk.
 - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
 - Inform parents/carers about the incident and how it is being managed.
 - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
 - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- 6.16 We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.

- 6.17 Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report:
www.ceop.police.uk/safety-centre/
- 6.18 If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire police by using 101.
- 6.19 If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Derbyshire police using 101 unless immediate concerns and 999 will be used by the DSL (or deputy).
- 6.20 If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Derbyshire Police first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- 6.21 We will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- 6.22 We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- 6.23 We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- 6.24 If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire Police using 101.
- 6.25 If made aware of IIOC, we will:
- Act in accordance with our child protection policy and the relevant Derby City & Derbyshire Safeguarding Children Partnership Safeguarding procedures.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Derbyshire police or the LADO.
- 6.26 If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
- Ensure that the DSL (or deputy) is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Report concerns, as appropriate to parents and carers.
- 6.27 If made aware that indecent images of children have been found on the setting provided devices, we will:
- Ensure that the DSL (or deputy) is informed.

- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the Derbyshire police via 101 (999 if there is an immediate risk of harm) and Children's Services using Call Derbyshire (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

6.28 If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the headteacher is informed in line with our managing allegations against staff policy immediately and without any delay.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

Online Radicalisation and Extremism

- 6.29 We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- 6.30 If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy and Derbyshire prevent pathway which may include a referral into Channel.
- 6.31 If we are concerned that member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Cyberbullying

- 6.32 Cyberbullying (online bullying) as defined by Childnet is the, '*use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else.*' All staff at Shardlow Primary School are involved in the active prevention of cyber-bullying. Reporting cyberbullying is clear and visible. The school also appoints a number of Anti-Bullying Ambassadors, who report any such incidents and act as a peer for children to talk to if they wish to do so. Children must also refer to the Anti-Bullying policy displayed clearly in every classroom.
- 6.33 Cyberbullying can be any of the following (Cyberbullying: Understand; Prevent and Respond Guidance for Schools (Childnet)):
- intimidation and threats

- harassment and stalking
- vilification/defamation
- exclusion or peer rejection
- impersonation
- unauthorised publication of personal information or images
- manipulation

7. Impact

- 7.1 At Shardlow Primary School, we are committed to promoting the positive use of technology while ensuring the safety and well-being of all pupils. We continually evaluate the impact of our prevention activities, which are detailed in Appendix 1. These activities include a range of initiatives to raise awareness and provide pupils with the knowledge and support they need to stay safe online.
- 7.2 To make reporting incidents as easy as possible, we provide children with multiple opportunities to speak up throughout the school year. Posters are displayed prominently, and the school invites the NSPCC to conduct assemblies for both Key Stage 1 and Key Stage 2 pupils, educating them on how to respond if they experience or witness online abuse. Our “Speak Up, Speak Out” initiative encourages children to report any incidents of online bullying to an adult, with an emphasis on how they can do so safely and anonymously.
- 7.3 In addition to traditional reporting routes, we have established anonymous channels for pupils who may feel uncomfortable reporting in person. We actively encourage pupils to report any incidents they witness, empowering them to take an active role in preventing cyberbullying and fostering a supportive school environment.
- 7.4 Staff training is an ongoing priority, taking place regularly throughout the academic year to ensure all staff are aware of online safety practices and the latest developments in safeguarding. A weekly briefing further supports this by discussing any new issues or concerns related to safeguarding or online safety that may have arisen.
- 7.5 To keep parents and guardians informed, we include updates on safeguarding and online safety matters in our monthly newsletter, ensuring the wider school community is aware of key policies and activities aimed at supporting children’s online safety.

8. Reporting Procedure

- 8.1 The following steps should be taken immediately once an incident has been reported or identified, including providing adequate support for the person who has been cyberbullied:
 - Remove any material in question from circulation.

- Talk to the person who has carried out the bullying to ensure they understand why the behaviour is unacceptable. Steps will be taken to alter the bully's attitude and behaviour, and they will be given access to any help they may need.
- Talk to the parents of both parties involved to ensure they are aware of the situation and can offer support.
- Ensure any evidence of the incident is retained for further investigation. This may include screenshots, emails, messages, etc.
- Report the incident to the relevant service provider if it occurred on a platform or service, so they can take appropriate action.
- Provide guidance to staff and pupils on steps they can take to protect themselves online. For example, advise those targeted not to retaliate or reply, recommend blocking or removing individuals from contact lists, and remind them to carefully consider what personal information they share publicly.

8.2 Certain types of cyberbullying are illegal, and these should be taken very seriously:

- The sharing, saving, or downloading of indecent images of children (under the age of 18, including self-created images).
- Obscene content, such as depictions of rape or torture.
- Hate crimes and incidents, including racist and homophobic material; revenge pornography (sexual images of individuals over 18 published or forwarded without permission).
- Threats of violence, including threats of rape or death, and stalking or harassment.

8.3 In these cases, staff must report the incident to the Designated Safeguarding Lead (DSL), and the police may be consulted. Further advice can be sought from the Professionals Online Safety Helpline (telephone: 0844 318 4772, website: www.saferinternet.org.uk/about/helpline).

9. Social Media

- 9.1 At Shardlow Primary School, we are proud of our pupils' respect, responsibility, motivation, confidence, open-mindedness, and independence. These values underpin our school's vision and aims. We also enjoy sharing pupils' achievements with our local community, parents, governors, and wider community members via Twitter.
- 9.2 When children start at Shardlow Primary School, their parents are asked to complete a Parental Permissions form to indicate whether they are comfortable with their child's photograph being shared on social media, in the press, or on the school website. Once these forms are obtained, they are distributed to all staff members to ensure that photographs are shared only with parental consent. When photographs are posted online, the child's full name will never be shared alongside the image.

Managing Email

- 9.3 The use of email as a form of communication is managed by staff to ensure it is used appropriately for educational purposes.

- 9.4 All staff must use their internal email accounts for school-related business.
- 9.5 Children must not provide personal details to any person or organization within an email, ensuring their privacy and security.

Data Protection

- 9.6 Personal data will be recorded, processed, transferred, and made available in compliance with current data protection legislation.
- 9.7 One Academy Trust has in place the following provisions:
- A trust-wide Data Protection Policy and Privacy Notices (see trust website).
 - The appropriate fee is paid to the Information Commissioner's Office (ICO) (trust-wide membership).
 - A Data Protection Officer (DPO) is appointed trust-wide. This role is currently fulfilled by SchoolPro.
 - Personal data is only held for the minimum time necessary to perform the school's functions.
 - Data is kept accurate and up-to-date, with inaccuracies corrected without unnecessary delay.
 - The lawful basis for processing personal data is documented, and details are included in the Privacy Notice (see Privacy Notices on the ONE Academy Trust website)
 - Data Protection Impact Assessments (DPIAs) are carried out as necessary.
 - Clear procedures are in place for data access, security, storage, and transfer, including safeguards when personal data is shared with third parties (e.g., cloud service providers).
 - Staff are trained in data protection awareness and are made aware of their responsibilities.
 - Data is securely stored on password-protected computers and devices and is only transferred using encryption and secure, password-protected devices.

For Portable Systems & Removable Media:

- 9.8 Any personal data stored on portable systems (e.g., laptops, memory sticks) must be encrypted and password-protected.
- 9.9 Devices must have approved virus and malware protection software.
- 9.10 Once the data is no longer required, it must be securely deleted in accordance with the school's data retention policy.

10. Monitoring & review

- 10.1 This policy will be reviewed annually as a minimum and approved by the Governing Body.

Online Safety Prevention Activities

- Online safety is embedded within the computing and PSHE curriculums.
- Child friendly online safety policy.
- Anti-Bullying Week
- Safer Internet Day
- NSPCC workshops
- School newsletter
- Weekly (minuted) briefing
- DSL weekly meeting

Adult guidelines for school internet use:

- The use of the Internet in school must be for professional and curriculum purposes.
- Staff are responsible for ensuring that the children know and understand the pupil rules for using the Internet.
- Material that is unsuitable for children should not be viewed, uploaded or downloaded.
- All web materials should be reviewed and evaluated prior to use with the children to ensure that the content is appropriate.
- Copyright and intellectual property rights must be respected.
- If you find something inappropriate as a result of a search, the site address should be reported to the designated safeguarding lead.
- When writing emails, swearing, racist, sexist or aggressive comments are not allowed. Do not state anything that could be interpreted as libellous.
- Staff are responsible for all emails sent and contacts made via email.
- Staff should treat outgoing and incoming email used in school as public.
- Do not respond to inappropriate emails. Inform the computing coordinator.
- Respect the privacy of other people's work files. Only enter them if permission from the member of staff has been given.
- The use of the Internet in school for financial gain, gambling, political purposes or advertising is forbidden.
- Any incident that breaks these guidelines must be reported.
- Staff using laptops for their professional use are responsible for ensuring that virus protection is updated as necessary.

If you choose to break these rules, the following could happen:

- A warning will be issued.
- Email and/or Internet access will be removed.
- The breach of the guidelines may be reported to the Governors.
- Appropriate external agencies may have to be involved.
- Appropriate disciplinary action may be taken.
- Other appropriate steps may also be taken.

Dear Parent/Carer

INTERNET PERMISSION

As part of the Computing curriculum, your child will be taught how to use the Internet to search for information and also how to send and receive email. You will be aware of the great increase in Internet use over the past few years and this school believes that it is essential to teach the skills needed to access the Internet in order to equip them for life outside school.

We have taken a number of steps to ensure that access to the Internet is safe for your child. The children will access the Internet through an Internet Service Provider. The provider that the school has chosen is especially designed for schools and filters out any undesirable material. There are rules that the children must follow. Please note that the School cannot be liable for any damages arising from your child's use of the Internet.

If the school becomes aware of any serious breaches of the filtering policy, we will inform parents of the child concerned.

The Internet is a very powerful tool, which can be used to support your child's education in many wonderful and creative ways. We ask that you fill in the form attached and return it to school.

If you have any questions or concerns, please do not hesitate to contact me.

Yours sincerely

J Dale

These guidelines will be shared with the children each academic year.

PUPIL GUIDELINES FOR INTERNET USE IN SCHOOL

Pupils are responsible for good behaviour on the Internet, just as they are in a classroom or a school corridor. General school rules apply.

The Internet is provided for pupils to conduct research and communicate with others. Parents' permission is required. The access is a privilege, not a right and access requires responsibility.

Individual users of the Internet are responsible for their behaviour and communications over the network.

During school time, teachers will guide pupils towards appropriate materials. Outside school, parents and carers must bear this responsibility, in the same way as they have responsibility for children accessing other information sources such as televisions, telephones, videos, radio and other media.

You need to make sure that you:

- Are only using the Internet for schoolwork.
- Are following the teacher's instructions when using the Internet.
- Ask "Is it true?" Not all the information on the Internet or in emails is true.
- Keep your password private.
- Are careful about what you send. Do not write or send anything that could upset and offend others.
- Do not put yourself in danger. Do not give personal information about yourself in an email or on a website.
- Do not put others in danger. Do not give personal information about other people in an email or on a website.
- Let your teacher know if you receive anything you do not feel comfortable with. Do not respond to it yourself.
- Do not arrange to meet anyone as a result of an email correspondence
- Do not download anything you think others may be upset by.
- Always respect other people's privacy. Do not go into other people's files without asking them first.
- Report anyone that chooses to break these rules to the teacher.

If you choose to break these rules, the following could happen:

- You could put yourself and others in danger.
- You could give yourself and the school a bad name.
- You may be banned from using the Internet for a time.
- You may not be allowed to use email.
- A letter could be sent home telling your parents what has happened.
- Other sanctions may be used depending on the incident.

Legislation

We have compiled this online safety policy in accordance with the following legislation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

Establish the facts;

- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.

The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

<http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Links to other organisations or documents

The following links have also been used in compiling this policy:

Safer Internet Centre – <https://www.saferinternet.org.uk/>

South West Grid for Learning - <https://swgfl.org.uk/products-services/online-safety/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Internet Watch Foundation - <https://www.iwf.org.uk/>

CEOP - <http://ceop.police.uk/>

ThinkUKnow - <https://www.thinkuknow.co.uk/>

[LGfL – Online Safety Resources](#)

INSAFE / Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis

Bullying / Online-bullying / Sexting / Sexual Harrassment

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyber_bullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

Social Networking

Digizen – [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

Curriculum

[SWGfL Digital Literacy & Citizenship curriculum](#)

Data Protection

[ICO Guide for Organisations \(general information about Data Protection\)](#)

[ICO Guides for Education \(wide range of sector specific guides\)](#)

Professional Standards / Staff Training

[DfE – Keeping Children Safe in Education](#)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

[Childnet – School Pack for Online Safety Awareness](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

[SWGfL Digital Literacy & Citizenship curriculum](#)

EYFS and Key Stage 1

Think then Click

These rules help us to stay safe on the Internet



We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.



We can search the Internet with an adult.

We always ask if we get lost on the Internet.



Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Pupils and Parents Online Safety Contract

Please complete, sign and return to the school office.

Pupil: _____

Class: _____

Pupil's Agreement

I have read and I understand the pupils online safety information, and will abide by the rules which are designed to keep both myself and the school safe.

Signed: _____

Date: _____

Parent's Consent

I have read and understood the online safety information and give permission for my child to access the Internet at school, and will encourage them to abide by these rules. Children will receive advice on online safety at school and advice for parents is available at www.thinkuknow.org.uk/parents or by contacting the school. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: _____

Please print name: _____

Date: _____