# Online Safety Policy

| | |
|---|---|
| **Status:** | Non-Statutory |
| **Designated Committee:** | Finance and Resources |
| **Date Approved:** | Autumn 2022 |
| **Date of Next Review:** | Autumn 2023 |

**Contents**



**Appendices**

## 1. Introduction

1.1 All Saints CE Primary School recognises the Internet and other digital technologies provide a good opportunity for children and young people to learn. These new technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

1.2 As part of our commitment to learning and achievement we at All Saints CE Primary School want to ensure that new technologies are used to:

- Raise standards.
- Develop the curriculum and make learning exciting and purposeful.
- Enable children to learn in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding.

1.3 We are committed to an equitable learning experience for all children using ICT technology and we recognise that ICT can give children with disabilities and SEND increased access to the curriculum to enhance their learning.

1.4 We are committed to ensuring that all children will be able to use new technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are informed about the risks that exist so that they can take an active part in safeguarding children.

1.5 The nominated senior person for the implementation of the School's e- Safety policy is the headteacher.

## 2. Scope of Policy

2.1 The policy applies to:

- all children;
- all teaching and support staff (including peripatetic), school governors and volunteers;
- all aspects of the School's facilities where they are used by voluntary, statutory or community organisations.

2.2 All Saints CE Primary School will ensure that the following elements are in place as part of its safeguarding responsibilities to children:

- a list of authorised persons who have various responsibilities for online safety;
- a range of policies including acceptable use policies that are frequently reviewed and updated;
- information to parents that highlights safe practice for children and young people when using new technologies;
- audit and training for all staff and volunteers;
- close supervision of children when using new technologies;
- education that is aimed at ensuring safe and responsible use of new technologies;
- a monitoring and reporting procedure for abuse and misuse.

## 3. Infrastructure and Technology

3.1 Partnership working

3.1.1 All Saints CE Primary School recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is the Schools Broadband Team who provide a managed (not 'locked down') network system. We fully support and will continue to work with schools broadband to ensure that pupil and staff use of the Internet and digital technologies is safe and responsible.

3.1.2 As part of our wider safeguarding responsibilities, we seek to ensure that voluntary, statutory and community partners also regard the welfare of children as paramount. We therefore expect any organisation using the school's ICT or digital technologies to have appropriate safeguarding policies and procedures.

3.1.3 We work with our partners and other providers to ensure that any children who receive part of their education away from school are e-safe.

**Policies and procedures**

Our policies are aimed at providing a balance between exploring the educational potential of new technologies and safeguarding children. We systematically review and develop our online safety policies and procedures ensuring that they continue to have a positive impact on pupil's knowledge and understanding. We use the views of children and families to assist us in developing our online safety policies and procedures.

4.1 Use of new technologies

4.1.1 We seek to ensure that new technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

4.1.2 All Saints CE Primary School expects all staff and children to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below:1 These expectations are also applicable to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Users are not allowed to:

Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting illegal acts
- Any other information which may be offensive, embarrassing or upsetting to peers or colleagues (i.e cyberbullying) e.g. abusive text or images; promotion of violence; gambling; criminally racist or religious hatred material

1 For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, PDAs etc.

4.1.3 The School recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and permission given by senior leaders, so that the action can be justified, if queries are raised later.

4.1.4 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity

4.1.5 In addition, users are not allowed to:

- Use school broadband or an equivalent broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves schools broadband or members of Local Authorities in any way;
- Visit sites that might be defamatory or incur liability on the part of schools broadband or member Local Authorities or adversely impact on the image of schools broadband.

- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of schools broadband, or to schools broadband itself;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
- financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;

- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet; Use the Internet for soliciting, revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorised access to facilities or services accessible via schools broadband.
- Undertake activities with any of the following characteristics:
- wasting staff effort or networked resources, including time on end systems accessible via the schools broadband network and the effort of staff involved in support of those systems;
- corrupting or destroying other users' data;
- violating the privacy of other users;
- disrupting the work of other users;
- using the schools broadband network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
- continuing to use an item of networking software or hardware after schools broadband has requested that use cease because it is causing disruption to the correct functioning of schools broadband.
- other misuse of the schools broadband network, such as introduction of viruses.
- Use any new technologies in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

4.1.6 Where schools broadband become aware of an illegal act or an attempted illegal act, they will comply with the law as it applies and take action directed by the police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

4.2 Definition of Abuse

Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet- enabled devices (Department for Education, 2018; Department of Health, 2017; Scottish Government, 2014; Welsh Assembly Government, 2018).
It can happen anywhere online that allows digital communication, such as:

- social networks
- text messages and messaging apps
- email and private messaging
- online chats
- comments on live streaming sites
- voice chat in games.

Children and young people can be revictimized (experience further abuse) when abusive content is recorded, uploaded or shared by others online. This can happen if the original abuse happened online or offline.
Children and young people may experience several types of abuse online:

- bullying/cyberbullying

- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- sexting (pressure or coercion to create sexual images)
- sexual abuse
- sexual exploitation.

Children and young people can also be groomed online: perpetrators may use online platforms to build a trusting relationship with the child in order to abuse them.
This abuse may happen online or the perpetrator may arrange to meet the child in person with the intention of abusing them.

4.3 Reporting Abuse

4.3.1 There will be occasions when either a pupil or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the pupil or adult should be report the incident immediately.

4.3.2 The School also recognises that there will be occasions where children will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances LSCB2 Procedures should be followed. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Safeguarding Lead for Child Protection within the School will refer details of an incident to Children's Social Care or the Police.

2 Chapter 9 of the LSCB Procedures

The School, as part of its safeguarding duty and responsibilities will, in accordance with LSCB Procedures assist and provide information and advice in support of child protection enquiries and criminal investigations.

5. **Education and Training**

5.1 All Saints CE Primary School recognises that new technologies can transform learning; help to improve outcomes for children and young people and promote creativity.

5.2 As part of achieving this, we aim to create an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our children to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use new technologies safely.

5.3 To this end we will:-

- Provide an age-related, comprehensive curriculum for online safety which enables children to become safe and responsible users of new technologies. This will include teaching children to exercise the skills of critical awareness, digital literacy and good online citizenship.
- The work on online safety will include the breadth of issues categorised into four areas of risk as identified in Keeping Children Safe in Education September 2021:
  • 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 feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

- Audit the training needs of all school staff and provide training to improve their knowledge and expertise in the safe and appropriate use of new technologies.
- Work closely with families to help them ensure that their children use new technologies safely and responsibly both at home and school. We will also provide them with relevant information on our online safety policies and procedures.

## 6. Standards and Inspection

All Saints CE Primary School recognises the need to regularly review policies and procedures to ensure that its practices are effective and that the risks to children are minimised.

3 Chapters 5, 9, 12 and 13 of the LSCB Procedures

### 6.1 Monitoring

6.1.1 Monitoring the safe use of new technologies includes both the personal use of the Internet and electronic mail and the monitoring of patterns and trends of use.

6.1.2 With regard to monitoring trends, within the school and individual use by school staff and children, All Saints CE Primary School will audit the use of the Internet and electronic mail in order to ensure compliance with this policy. The monitoring practices of the school are influenced by a range of national and Local Authority guidance documents and will include the monitoring of content and resources.

6.1.3 We will also monitor the use of mobile technologies by children, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti- bullying policy for further information). We will also ensure that school staff understand the need to monitor our children, and where necessary, support individual children where they have been deliberately or inadvertently been subject to harm.

### 6.2 Sanctions

6.2.1 We will support children and staff as necessary in the event of a policy breach.

6.2.2 Where there is inappropriate or illegal use of new technologies, the following sanctions will be applied:

- Child / Young Person
- The child/young person will be disciplined according to the behaviour policy of the school.
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

- Adult (Staff and Volunteers)
- The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for example, illegal Internet use or child protection concerns.

6.2.3 If inappropriate material is accessed, users are required to immediately report this to the headteacher and schools broadband so this can be taken into account for monitoring purposes.

## 7. Working in Partnership with Parents and Carers

7.1 We are committed to working in partnership with parents and carers and understand the key role they play in maintaining the safety of their children, through promoting Internet safety at home and elsewhere.

7.2 We also appreciate that there may be some parents who are concerned about the use of the new technologies in school. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a strategy that will allow their child to fully access the curriculum, whilst remaining safe.

## 8. Appendices of the Online Safety Policy

8.1 This policy statement should be read alongside our organisational policies and procedures for both staff and children, including:

- Child protection
- Procedures for responding to concerns about a child or young person's wellbeing
- Dealing with allegations of abuse made against a child or young person
- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures
- Photography and image sharing guidance
- ICT equipment (onsite and offsite)
- GDPR, data security and retention.

**Appendix A:**

Internet Use

The school Admin and Curriculum network is protected by Schools Broadband firewalls which block inappropriate websites and emails. However, children should be supervised when using the internet to research information. Staff should follow the school's online safety guidance.

Staff must ensure that they adhere to the Internet Acceptable Use Policy and must not access social media sites for personal reasons during working time.

Social Media Sites

All employees are expected to adhere to the "use of social media sites" policy at all times. Employees must ensure that they conduct themselves in a manner that will not place children or vulnerable adults at risk, bring the school into disrepute or damage their own professional reputation.

Social media sites include: Facebook, My Space, Twitter and Instagram but are not limited to just these.

Mobile phones

Staff should follow the guidance included in the Safeguarding and use of social media polices. Staff should not be using mobile phones around the school or at any directed time. Any children bringing phones into school should leave them in the school office.

**Appendix B:**

All Saints CE Primary School Internet and ICT Acceptable Use Policy for Staff and Volunteers

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

| |
|---|
| **Name of staff member/governor/volunteer/visitor:** _____ |
| When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:<br>Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, or pornographic nature (or create, share, link to or send such material)<br>Use them in any way which could harm the school's reputation<br>Access social networking sites or chat rooms<br>Use any improper language when communicating online, including in emails or other messaging services<br>Install any unauthorised software, or connect unauthorised hardware or devices to the school's network<br>Share my password with others or log in to the school's network using someone else's details<br>Share confidential information about the school, its pupils or staff, or other members of the community<br>Access, modify or share data I am not authorised to access, modify or share<br>Promote private businesses, unless that business is directly related to the school |
| I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.<br><br>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.<br><br>I will let the designated safeguarding lead (DSL) and ICT manager know if a child 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.<br><br>I will always use the school's ICT systems and internet responsibly and ensure that children in my care do so too. |

| | |
|---|---|
| **Signed (staff member/governor/volunteer/visitor):**<br><br>_____ | **Date:**<br><br>_____ |

**Appendix C:**

**All Saints CE Primary School Acceptable Use Policy for Primary Children**

Please talk to your child about keeping safe on the internet, ensuring they are aware of the school's policy:

- to keep my username and password private and not to use anyone else's
- to keep all personal information private
- to block unknown links and attachments by not opening anything that I do not trust
- to report any messages or internet pages that are unsuitable or upsetting
- to tell someone I trust if someone asks to meet me offline

When using computer equipment in school…

- I understand that my behaviour will be checked
- I will not play games unless I have permission
- I will not open, copy, delete or change anyone else's files, without their permission
- I will be polite and think carefully about how I talk to others online and what I say about them
- I will not take, copy or send pictures of anyone without their permission
- I will not try to upload, download or open any files, programmes or websites which are unsuitable or illegal
- I will not try to get around the filtering or security systems
- I will not install any programmes nor change the settings
- I will not use chat and social networking sites unless I have permission from an adult
- I will not copy other people's work and pretend it is my own
- I will not try to download pirate copies of music, videos, games or other software
- I will check that information I use from the internet is from a trusted website

If I break these rules

- I understand that the school's behaviour guidelines will be followed

Further internet safety guidance can be found on the school website.

My parents/carers have spoken to me about the school's internet and email policy and I agree to follow it.

Name of child

Signed Date

I have read and discussed this policy with my child and give permission for him/her to use the school's ICT systems, including the internet.

Parent/Carer signature Date

**Appendix D:**

Email
All staff are supplied with a school outlook email account.

**Appendix F:**

Access and Privacy
The school's computers should not be used at any time for downloading, copying or storing illicit or offensive material, nor should video, music or other files which take up a large amount of space be stored on our servers. Users wishing to download and copy large files to a
should discuss it with the ICT Coordinator.

No user should attempt at any time to install any software of any kind onto the school network or onto any workstation connected to it, including screensavers. If a member of staff wishes to have software installed the agreement of the ICT Coordinator or headteacher should first be sought, the licence checked and the relevant media handed to the ICT Coordinator to arrange for installation.

All users of the network must be aware that their user areas and individual files may on occasion be accessed by the network administrators and files which contravene any part of this policy may be removed.

All use of the school's ICT resources should be in line with this policy and the rules laid out in the school's