



Online safety policy

Stanton Bridge Primary School

Adopted: November 2022

Review date: November 2024 / legislation changes

Online safety policy

Stanton Bridge Primary School recognises that ICT and the Internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

Online safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Online safety is a whole-school issue and responsibility.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in our **Behaviour Policy**.

I. Roles and Responsibilities

The school online safety coordinator is Mrs Emma Good.

The designated member of the governing body responsible for online safety is Dr. Rixon.

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy by reviewing e-safety incidents and monitoring reports. Online safety falls within the remit of the governor responsible for Safeguarding. The role of the online safety governor will include:

- Ensure an online safety policy is in place, reviewed every year and is available to all stakeholders
- Ensure that there is an online safety leader who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive.
- Ensure that procedures for the safe use of ICT and the Internet are in place and adhered to
- Hold the headteacher and staff accountable for online safety.

Headteacher and SLT

The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the online safety leader. Any complaint about staff misuse must be referred to the online safety leader at the school or, in the case of a serious complaint, to the headteacher.

- Ensure access to induction and training in online safety practices for all users.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures be supervised by a named member of SLT.
- Ensure that pupil or staff personal data as recorded within school management system sent over the Internet is secured.
- Work in partnership with the DFE and the Internet Service Provider and school Technician and Computer Manager to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- The Senior Leadership Team will receive monitoring reports from the online safety manager and IT Technician.

Online safety coordinator:

- Leads Online Safety meetings.
- Work in partnership with the DFE and the Internet Service Provider and school IT Technician to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Receives reports of e-safety incidents and creates a log of incidents to inform future online safety developments with the IT Technician.
- Reports to Senior Leadership Team.
- Liaise with the nominated member of the governing body & headteacher to provide an annual report on online safety.

Computing subject leader / Technical Staff:

The Computing Subject leader is responsible for ensuring:

- That the schools technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the headteacher; online safety coordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies.

2. Communicating School Policy

This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHCEE lessons where personal safety, responsibility, and/or development are being discussed.

3. Making use of ICT and the Internet in school

The Internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

School monitoring system used to supplement the filtering system.

Education Protect by Impero

Stanton Bridge uses Impero Education Pro filtering system, it is an online safety software is compliant with the UK Safer Internet Centre's 'appropriate monitoring' provider checklist. Also it protects students with state-of-the-art online safety technology, in line with Ofsted and ISI. Designed in response to UK Government requirements, such as the Prevent duty and the Department for Education's Keeping Children Safe in Education guidance (KCSIE), Impero Education Pro's state-of-the-art safeguarding software helps schools to fulfil their legal duty of care around internet safety and safeguarding. This best practice approach to safeguarding in schools, including active monitoring and logging incident captures to provide contextual insight, helps schools to identify potential risk, respond before an incident escalates, and educate students about responsible internet behaviour. The school has provided enhanced user-level filtering through the use of the Impero filtering programme. In reality, there is no filtering system can guarantee 100% protection against access to unsuitable sites. Therefore, Stanton Bridge Primary School use Impero software to monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement.

#Stanton Bridge Primary School's internet filtering controlled by Coventry City Council

- Teachers: controlled via Coventry LEA Proxy
- Students: controlled via Coventry LEA Proxy.
- SWURL control panel is a site used to allow and block list is available using the SWURL control panel.
- Both teachers and students group membership are controlled through Domain Controllers: SVR-SBP-DC01 (10.253.216.32) & SVR-SBP-DC02 (10.253.216.33) Active Directory.

McAfee

- McAfee software allows users to block or displays content you want to see, based on categories of your choice.

Web/Internet Filtering

- Stanton Bridge Primacy School maintains and supports the managed filtering service (SWURL Smoothwall Web Filter) provided by Coventry City Council, this filtering service has been set up based on BECTA recommendations.

Password

- A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly.
- A password policy is often part of the School's official regulations and may be taught as part of security awareness training.
- You Should Not Share Your Passwords. Please see Password Policy

Some of the benefits of using ICT and the Internet in schools are:

For pupils:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.
-

Keys stage 1 and 2 are required to complete a conduct of conduct.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

EYFS:

Reception and Nursery use software called 2 simple on school iPods that have passcodes for security to capture images of the children and make digital notations of the learning the practitioner has witnessed. All EYFS staff are aware that they can use the iPod at home to make notations but they are told they cannot plug the iPod into a personal computer and can only connect it to a secure computer at school. They keep them on themselves at all times during the school day.

All staff and governors are required to complete an acceptable use policy.

4. Well being

We recognise that people may suffer from mental health wellbeing issues online so we have implemented strategies to support people's mental health and wellbeing. We delivered workshops for pupils and parents for online digital devices and we are very thorough in ensuring the safety of pupils online. We monitor pupil's online activity and take the necessary steps if any concerns arise. We also signpost pupils to appropriate organisations to provide the necessary service.

Please see **Well being policies and documents** for more information.

5. Learning to Evaluate Internet Content

With so much information available online it is important that pupils learn how to evaluate Internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught to:

- Be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- Use age-appropriate tools to search for information online
- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiarism very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

Recent popularity of Fake news and Online Hoaxes

A hoax is a deliberate lie designed to seem truthful. The internet and social media provide a perfect platform for hoaxes, especially hoaxes about challenges or trends that are said to be harmful to children and young people to be spread quickly.

<https://www.gov.uk/government/publications/harmful-online-challenges-and-onlinehoaxes/harmful-online-challenges-and-online-hoaxes> Feb 2021

If a harmful online challenge or online hoax might be circulating between children, the DSL and the Safeguarding Team will investigate and take the necessary steps to safeguard children. They may share relevant information to parents, local authority and the police.

Here at Stanton Bridge we aim to provide relevant information to our school community. We provide updates via the school twitter feed and printed leaflets and regular meetings throughout the school year.

The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported to the school's IT Technician and then the online safety manager. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

6. Managing Information Systems

The school is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The IT Technician will review the security of the school information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted • Making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- Files held on the school network will be regularly checked for viruses
- The use of user logins and passwords to access the school network will be enforced
- Portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.

For more information on data protection in school please refer to our GTPR policy.

6.1 Emails

The school uses email (Microsoft Office 365) internally for staff and is an essential part of school communication, it is also used to enhance the curriculum by:

- Initiating contact and projects with other schools nationally and internationally • Providing immediate feedback on work, and requests for support where it is needed.

Staff and pupils should be aware that school email accounts should only be used for school related matters, ie for staff to contact parents, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

Password Policy:

A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly.

You Should Not Share Your Passwords.

Password expire after 90 days

User receive notification 14 days prior password expire date of 90 days

6.2 School Email Accounts and Appropriate Use

We will teach the children how to use email and will use Purple Mash and 2simple email. We shall only use whole class emails or group/ project email address.

Pupils will be educated through the computing curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

Staff have been made aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate with parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staffs are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell the Computing lead or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school.

7. Published Content and the School Website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies.

Personal information on staff or pupils will only be published in line with the schools Data Protection Policy (GDPR) and details for contacting the school will be for the school office only.

7.1 Policy and Guidance of Safe Use of Children's Photographs and Work

Colour photographs and pupils work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the schools Data Protection Policy (GDPR2018) images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a media consent form, which the parents/carers has the right to change consent at any time. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. This consent form will outline the school's policy on the use of photographs of children, including:

- How and when the photographs will be used
- How long parents are consenting the use of the images for
- School policy on the storage and deletion of photographs.

Parents will be contacted annually for consent, but under GDPR 2018, they are able to change their consent at any time.

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
 - all school publications
 - on the school website
 - in newspapers as allowed by the school
 - in videos made by the school or in class for school projects.
- Electronic and paper images will be stored securely.

- Names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (ie a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only.
- Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils. For more information on safeguarding in school please refer to our **school child protection and safeguarding policy**.

7.2 Complaints of Misuse of Photographs or Video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our **complaints policy** for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the school's **child protection and safeguarding policy** and **behaviour policy**.

Our pupils increasingly use electronic equipment on a daily basis to access the internet.

Unfortunately, some adults and young people will use and share content and images via social networking sites such as Facebook, Twitter, Tumblr, Snapchat and Instagram etc. to harm children. The harm might range from sending hurtful or abusive texts and emails, to grooming and enticing children to engage in sexually harmful conversations, webcam photography or face-to-face meetings.

Pupils may also be distressed or harmed by accessing inappropriate websites that promote unhealthy lifestyles, extremist behaviour and criminal activity.

Cyberbullying and sexting by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures. Serious incidents may be managed in line with our sexual exploitation policy or child protection procedures.

Many pupils own or have access to hand held devices and parents are encouraged to consider measures to keep their children safe when using the internet and social media at home and in the community. We offer advice through yearly workshops and offer guidance on the school's website.

All staff receive online safety training and have to adhere to the Social Media guidance

7.3 Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online.

Pupils are not allowed to access social media sites in school, there are various restrictions through the web filtering on the use of these sites in school that apply to both students and staff.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the computing curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Teachers will use a safe search engine such as Primary School ICT (<http://primaryschoolict.com>)
- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

8. Mobile Phones and Personal Device

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- Can make pupils and staff more vulnerable to cyberbullying
- Can be used to access inappropriate internet material
- Can be a distraction in the classroom
- Are valuable items that could be stolen, damaged, or lost
- Can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school takes certain measures to ensure that mobile phones are used responsibly in school. Some of these are outlined below.

- The school will not tolerate cyber bullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions read the **school behaviour policy**.
- A member of staff can confiscate mobile phones, and a member of the senior leadership team can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- Mobile phones must be switched off during school lessons or any other formal school activities.
- Any pupil who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.
- Images or files should not be sent between mobile phones in school.
- If staff wish to use these devices in class as part of a learning project, they must get permission from a member of the senior leadership team.

8.1 Mobile Phone or Personal Device Misuse

Pupils

- Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy. Their mobile phone may be confiscated.

Staff

- Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of school time.
- Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.
- Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the **child protection and safeguarding policy**, or in the staff contract of employment.
- For more detail see the **School Mobile Phone Policy** and the **GDPR Policy**.

9. Cyberbullying

The school, as with any other form of bullying, takes Cyber bullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the **behaviour policy**. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the school will:

- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- Record and report the incident
- Provide support and reassurance to the victim
- Make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provide may be contacted to do this if they refuse or are unable to remove it. They may have their Internet access suspended in school.

Repeated bullying may result in fixed-term exclusion. For further information please see our anti-bullying policy.

10. Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

11. Protecting Personal Data

Stanton Bridge believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the General Data Protection Regulations 2018, and following principles of good practice when processing data, the school will:

- Ensure that data is fairly and lawfully processed
- Process data only for limited purposes
- Ensure that all data processed is adequate, relevant and not excessive
- Ensure that data processed is accurate
- Not keep data longer than is necessary
- Process the data in accordance with the data subject's rights
- Ensure that data is secure
- Ensure, as far as possible, that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection **read the school's GDPR Policy**.

This policy will be reviewed annually