Stanion C.E (Aided) Primary School

Online Safety Policy

The root of the ethos of Stanion Church of England Primary School is based on the two commandments in Saint Matthew's Gospel.

'Love the lord your God with all your heart, with all your soul, and with all your mind.'

'Love your neighbour as yourself.'

Policy Statement As with all schools, we have a duty to ensure that children and young people are protected from potential harm both within and beyond the school environment. Every reasonable effort will be made to safeguard against all risks; however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children, young people and staff continue to be protected.

Aims

- To emphasise the need to educate staff, parents, children and young people about the pros and cons of using new technologies both within, and outside of, the school environment.
- To provide safeguards and rules for acceptable use to guide all users in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Scope of policy

This policy applies to all staff, pupils, governors, visitors and contractors accessing the internet or using technological devices on school premises. This includes staff or pupil use of personal devices, such as mobile phones or iPad which are brought onto school grounds. This policy is also applicable where staff or individuals have been provided with school issued devices for use off-site, such as school laptop or work mobile phone.

Responsibilities

Teaching and Support Staff (including volunteers)

All staff have a shared responsibility to ensure that children and young people are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all who work in schools are bound. Staff must take all reasonable precautions to ensure pupils do not access inappropriate on-line resources – and they must take immediate action if inappropriate material is encountered.

Staff receive Online-Safety training and updates throughout the year from the Computing Coordinator, Safeguarding team or Senior Leadership team. The school runs a Parent Information Evening in addition to sharing important information on a regular basis. Each month, we send out easy to follow guides, which focus upon specific risks, as a way of helping to inform parents and carers of potential sites and activities their children could be using. We encourage these to be used not only as an educational guide for parents but also to help to facilitate conversations between adults and children around different, current issues.
Staff may use the school's ICT systems for private purposes, but not for personal financial gain, gambling, political purposes, advertising, or for accessing text or imagery which is unlawful or could cause offence to the general school community. Any personal device brought on to school premises must be free of any files which, if opened in error, might cause offence and should not be connected to the Wi-Fi during the school day.

Technical Staff
Technical staff (e.g. from Capita, Talk-Straight ISP or Viglen) are responsible for ensuring that -

- The school's ICT infrastructure is secure and not open to misuse or malicious attack.
- Anti-virus software is installed and maintained on all school machines and portable devices.
- The school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the Online Safety Lead and the Designated Person for Safeguarding.
- Any problems or faults relating to filtering are reported to Designated Person for Safeguarding and to the broadband provider immediately and recorded on the Online Safety Incident Log.
- Users may only access the school's network through a rigorously enforced password protection policy, in which passwords are regularly changed.
- He/she keeps up to date with Online Safety technical information in order to maintain the security of the school network and safeguard children and young people.
- The use of the school network is regularly monitored in order that any deliberate or accidental misuse can be reported to the Online Safety Lead.

Stanion students
Students at Stanion Primary School are responsible for:

- Signing the agreement to, and abiding by, the Acceptable Use Rules for pupils.
- Using the internet and technologies in a safe and responsible manner within school.
- Informing staff of any inappropriate materials, cyberbullying or contact from unknown sources.

Incident Reporting
In the event of pupils or staff unintentionally encountered inappropriate on-line material, or the intentional misuse by staff or pupils of the school network, a report must be made to the Head teacher/Designated Person for Safeguarding/ Online Safety Lead immediately and

the Online Safety Incident Flowchart (see Appendix 1) should be followed, as well as the Online Safety Log being filled in.
In the event of minor or accidental misuse, internal investigations should be initiated and disciplinary procedures followed where appropriate. Lessons should be learnt from accidental misuse, and remedial action (such as blocking specific websites) should be taken.
Additionally, all security breaches, lost/stolen equipment or data, unauthorised use or suspected misuse of ICT should be reported immediately to the Head teacher and Online Safety lead.
All incidents must be recorded on the Online Safety Incident Log to allow for monitoring, auditing and identification of specific concerns or trends.

Monitoring
School staff and ICT technical staff may monitor user activity, including any personal use of the school ICT system, or equipment such as school laptops (both within and outside of the school environment) and users are made aware of this in the Acceptable Use Policy.

The Curriculum
Online Safety is of the upmost importance within our school and is taught in both discrete lessons as well as embedded into our Computing and wider curriculum. Using the Rising Stars scheme of work for computing, children and teaching staff are made aware throughout of the possible Online Safety links which can be made during each unit. All classes are also expected to teach a discrete Online Safety lesson each term following the rolling programme as provided by our new scheme of work 'Rising Stars Online Safety'.
As part of the Online Safety curriculum, the children are taught through discussions and appropriate, related activities to become positive digital citizens by teaching safe and appropriate behaviour online. In the ever changing, fast paced world we believe that it is vital to teach and embed the five pillars to Online Safety and ensure links are made throughout to wellbeing. The five pillars are considered as:

- Online Behaviour
- Online Activity
- Online Resilience
- Online Wellbeing
- Online Role Models

We are careful to ensure that as part of our Online Safety lessons that we also teach protective behaviours and so guarantee that all children know and are aware of who they can talk to; should an issue arise. The children also have an Online Safety workshop each year delivered by the Online Safety Lead for Northamptonshire.

Pupils with additional learning needs
The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of Online Safety awareness sessions and internet access.

Email Use

Staff

The school provides all teaching staff and governors with a professional email account to use for all school related business, including communications with children, parents and carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.

- Under no circumstances will staff members engage in any personal email communications with current or former pupils outside of authorised school systems.
- All emails should be professional in tone and checked carefully before sending, just as an official school letter would be.
- Staff should inform their line manager or the Online Safety Lead if they receive an offensive or inappropriate email via the school system.
- Staff should monitor the use of the email accounts by the pupils throughout the school year, even when the pupils are focussing on a different unit of the National Curriculum. Any offensive or inappropriate emails should be reported to the Online Safety Lead.

Pupils

The school provides individual email accounts for pupils to use as part of their entitlement to understand different ways of communicating and using ICT to share and present information. This is provided through our learning platform on DB Primary.

Pupils will use their school issued email account for any school related communications, including homework or correspondence with teachers. Email content will be subject to monitoring and filtering for safeguarding purposes.

Pupils will be taught about email safety issues, such as the risk of exposing personal information, opening attachments from unknown sources and the management of inappropriate emails. Pupils will also be guided in the correct tone to use in email correspondence and regularly reminded of restrictions on abusive or inappropriate content. The forwarding of chain letters is strictly prohibited in school and should be reported to a member of staff immediately.

It is the responsibility of each account holder to keep their password secure and to report any suspected breaches of password security to the Online Safety Lead or Network Manager. Account holders must never share their password with another user, or allow access to their email account without the express permission of the Head teacher.

Managing remote access

- Only equipment with the appropriate level of security should be using for remote access (i.e. encryption on any devices where sensitive data is stored or accessed)
- Log-on IDs and PINs should be confidential and use information that cannot be easily guessed (e.g. date of birth, telephone number, number patterns)
- For security purposes, network access information should not be written down in an easily-accessible place (e.g. on a noticeboard next to the server) or stored with a device in case of theft or unauthorised access.

Internet Access and Age Appropriate Filtering

- Filtering levels are managed and monitored in school via an administration tool/control panel, provided by our broadband supplier, which allows an authorised staff member to instantly allow or block access to a site or specific pages and manage user internet access. Staff members are aware of our broadband supplier's contact details and the procedure they need to follow.
- Age appropriate content filtering is in place across the school, ensuring that staff and pupils receive different levels of filtered internet access in line with user requirements (e.g. YouTube at staff level but blocked to pupils)
- All users have unique usernames and passwords to access the school network which ensures that they receive the appropriate level of filtering.

In addition to the above, the following safeguards are also in place:

- Anti-virus and anti-spyware software is used on all networked devices and is updated on a regular basis.
- Restricted password-protected access ensures that information about children and young people cannot be accessed by unauthorised users.
- Encryption codes on wireless systems prevent hacking.
- Staff are required to preview any websites before use, including those which are recommended to pupils and parents for homework support.

Use of School and Personal ICT Equipment
School ICT Equipment

- Personal or sensitive data should only be stored on the school network or on an encrypted or password-protected device. It should not be stored on a memory stick, portable drive, etc.
- Personal ICT equipment, such as laptops or memory sticks, must not be connected to the school network without consent from the Head teacher or ICT Co-ordinator and a thorough virus check.

Personal devices including wearable technology and bring your own device (BYOD) Mobile/Smart Phones

Pupil use:
Phones are not allowed in school but in emergency situations they will be turned off and stored in the school office at the start of the school day and returned to the pupil before their homeward journey. The school secretary will log the deposit and return the phones. The headteacher will give authorisation in emergency situations.

Staff use: Personal mobile phones are permitted on school grounds, but should be used outside of lesson time only and should not be connected to the school Wi-Fi during the school day. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

- It is the responsibility of the staff member to ensure that there is no illegal or inappropriate content stored on their device when brought onto school grounds.

- Personal mobile phones should never be used to contact children, young people or their families.

Volunteers, contractors, governors:

Phones should be left in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.

Laptops/ iPads

- Staff must ensure that all sensitive school data is stored on the network and not on a personal device, unless the device is encrypted. In the event of loss or theft, failure to safeguard sensitive data could result in disciplinary action. Password protection alone is not sufficient.
- Personal use of school laptops or computing facilities whilst on site is permitted outside of lesson times, as long as it does not interfere with an employee's work, and as long as there is no access of inappropriate materials.
- Staff are aware that all activities carried out on school devices and systems, both within and outside of the school environment, may be monitored in accordance with this policy.
- Staff laptops should only be used by the person who it has been designated to.
- Staff will ensure that school laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.
- If staff bring their personal devices into school, they must not contain any material which might be deemed inappropriate in case this is revealed to pupils by accident.

Removable Media (Memory Sticks/USB)

- Where staff may require removable media to store or access sensitive data (e.g. IEPs, pupil attainment and assessment data) off site, only encrypted memory sticks will be used.
- Any passwords used for encrypted memory sticks/or other devices will be remain confidential to the user and shared only with authorised IT personnel for security and monitoring purposes.

Photographs and Video

- Parents and carers are informed that photographs or videos of young people may be used within the school environment, the school website and the prospectus. They may request that their child does not appear on the website or in the prospectus.
- Staff should ensure that personal mobile phones, tablets, cameras or other ICT are not used to take videos or photographs of pupils.
- Where photographs of pupils are published or displayed (e.g. on the school website) first names only will be displayed. Best practice would be to use non-identifying captions (e.g. Year 6 pupil playing football)

- Wherever possible, shots of pupils engaged in tasks will be taken, as opposed to 'portraits'. Images should never show young people in compromising situations or inappropriate clothing (e.g. swimming costumes).

Video conferencing

- All pupils are supervised by a member of staff when video conferencing, particularly when communicating with individuals or groups outside of the school environment (e.g. international schools)
- All video conferencing activities are time logged and dated with a list of participants.

Parent/Carer Involvement

- A copy will of the Acceptable Use rules will be available on the school website.
- When pupils first begin to use on-line resources freely, the pupils and their parents/carers are will be asked to read and sign acceptance of the rules, a copy of which will be stored at school.
- Parents are strongly encouraged to prevent their children using social media accounts if they are underage. The school unfortunately cannot enforce this advice outside of school but stress that parents are responsible for checking their child's internet usage.
- Wherever possible, and subject to prior arrangement, the school will endeavour to provide parents/carers without internet access to research online safety materials and resources.

Policy Ratified – 30th March 2023

Next Review – March 2024

Signed _____

Head Teacher

Signed _____

Chair of Governors

Appendices

Appendix 1