Calstock and Stoke Climsland Schools

Online Safety Policy 2023

For implementation December 2016

Review: September 2023 ready for implementation by November 2023

Calstock and Stoke Climsland Primary Schools believe that the safe use of information and communication technologies in school has the potential to bring great benefits. Recognising online safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

Involving the community

Calstock and Stoke Climsland Primary Schools view online safety as a whole school issue and aim to develop a holistic approach to writing and updating the online safety policy as well as embedding safe practice for all members of the school community.

We aim to work in partnership with our school communities (staff, pupil councils, parent groups) to ensure that the online safety policy is adapted specifically to reflect the needs and requirements of each school. We encourage all members (staff, parents/carers, pupils etc.) to be actively involved in developing the online safety policy so that through collaboration we create a policy that is appropriate for our establishments.

Due to the constantly evolving nature of technology (and relevant local and national guidance and legislation), we will review and update this policy annually, bringing forward this review when necessary in response to issues arising.

Contents

1. Calstock and Stoke Climsland Primary Schools' Online Safety Ethos

The internet and information technologies are an important part of everyday life, and children must be supported to learn to use them safely and effectively.. The purpose of this policy is to:

- Identify what is expected of all members of the school community.
- Outline key procedures we will adopt when responding to online safety concerns.
- Raise awareness with all members of the school communities regarding the potential risks as well as benefits of technology.
- Safeguard and protect all members of Calstock and Stoke Climsland communities online.

- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of Calstock and Stoke Climsland Primary Schools (collectively referred to as 'staff' in this policy) as well as children and parents/carers.
- This policy must be read in conjunction with other relevant school policies including (but not limited to): child protection and safeguarding; behaviour management (including pupil discipline and anti-bullying); guidance for safer working practice for those working with children and young people in education settings (October 2015) (issued to all staff along with code of conduct); Acceptable Use Agreements; relevant curriculum policies including Sex and Relationships Education (SRE).

1.1 Writing and reviewing the online safety policy

The Designated Safeguarding Lead (DSL) is:	Ben Towe
The Online safety lead for the Governing Body is:	Sophie Wheatley
The date for the next policy review is:	November 2024

1.2 The key responsibilities of the schools' leadership and management are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities, including liaison with the ICT subject leader and the online safety governor lead.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including Acceptable Use Agreements which cover appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of school systems and networks and to ensure that the school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

1.3 The key responsibilities of the Designated Safeguarding Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Ensuring that online safety is promoted to parents and carers and other stakeholders through a variety of channels and approaches.
- Working with the school business manager, LA advisors and technical support staff to ensure that practice is in line with current legislation on data protection and data security.
- Maintaining records of online safety concerns/incidents and actions taken through the schools' existing safeguarding procedures and records.
- Reporting to the Governing Body and other agencies as appropriate, on online safety concerns.
- Liaison with the local authority and other local and national bodies, as appropriate.

- Working with the school leadership to review and update the online safety policies, Acceptable Use Agreements and other related policies on a regular basis (at least annually).
- Ensuring that online safety is integrated with other appropriate school policies and procedures.

1.4 The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Adhering to the Acceptable Use Agreement.
- Taking responsibility for the security of school systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying concerns about individuals and taking appropriate action by following school safeguarding policies and procedures.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.

1.5 Key responsibilities for staff managing the technical environment are:

The schools' internet and technical services are provided by NCI. The school business manager works closely with NCI, in consultation with the DSL, to provide a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised, by ensuring that:

- All staff take responsibility for the implementation of the security of systems and data in partnership with the leadership and management team.
- The school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Reasonable steps are taken to prevent deliberate or accidental misuse and any breaches or concerns are reported to the DSL who records them and takes appropriate action
- NCI will contribute to providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- The school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Appropriate anti-virus software and system updates are installed and maintained on all school machines and portable devices.
- Reasonable steps are taken to protect sensitive data including staff password protection and encryption of portable devices that might hold such data.

1.6 The key responsibilities of children and young people are:

- Contributing to the development of online safety policies.
- Adhering to the Acceptable Use Agreement.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Assessing the personal risks of using any particular technology and behaving safely and responsibly to limit those risks.

2. Online Communication and Safer Use of Technology

2.1 Managing the schools' websites

The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).

- The head teacher/school business manager will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate and that intellectual property rights, privacy policies and copyright are respected.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.
- Images and videos will only be shared online if parental permission has been given and pupils will not be identified by their full names.

2.2Managing email

All members of staff are provided with a specific school email address to use for any official communication. The use of personal email addresses by staff for any official school business is not permitted. Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.

- All emails sent should be written thoughtfully and carefully.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.3 Video conferencing and webcam use for educational purposes

The school acknowledges that video conferencing is a challenging activity with a wide range of learning benefits, particularly for providing a link between Calstock and Stoke Climsland Schools. All use of video conferencing will be risk-assessed, and appropriate procedures put in place to protect children from unauthorised access or contact. All video communications will be supervised by an adult.

2.4 Appropriate and safe classroom use of the internet and any associated devices

Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.

- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability.
    - At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which support the learning outcomes planned for the pupils' age and ability.
    - At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
    - All school owned devices will be used in accordance with the school Acceptable Use Agreements and with appropriate safety and security measures in place.
    - Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
    - Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
    - The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
    - Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
    - The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
    - The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

3. Social Media Policy

All members of the schools' communities are advised to exercise caution in using social media services, taking care to set their privacy settings appropriately, to respect the privacy of others in particular avoiding reference to sensitive school matters and ensure that they post nothing that may be considered threatening, hurtful or defamatory to others.

- The school will block pupil and staff access to social media and social networking sites whilst on site.
- Any concerns regarding the online conduct of any member of the school communities on social media sites should be reported to the leadership team and will be managed in accordance with policies such as behaviour management, allegations against staff and child protection and safeguarding. Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed.

3.1 Staff personal use of social media

- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school policies and the wider professional and legal framework.

3.2 Pupils' use of social media

- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any under age use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Expectations for safe use of personal devices and mobile phones

All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.

- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items.
- Mobile phones and personal devices must not be used in sensitive areas such as changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the behaviour policy.

4.2 Pupils' use of personal devices and mobile phones

Pupils are not permitted to carry mobile phones in school.

- If a pupil needs to contact his/her parents/carers they will be allowed to use the school phone.
- If a pupil brings a mobile phone into school, for example if they are being collected from school to spend the night on a visit, then the phone should be given to the class teacher at the start of the day. They will store it securely and return it to the pupil at home time.

4.3 Staff use of personal devices and mobile phones

Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.

- Images taken of children as part of assessment or other activities will be afforded particular care at all times.
- Staff are advised to use passwords/pin numbers (which are kept confidential) to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen.

4.4 Visitors use of personal devices and mobile phones

Parents/carers and visitors will be asked not to use mobile technologies while on the school premises.

5. Policy Decisions

5.1 Authorising internet access

The school will ensure that all staff and pupils who are granted access to the school's devices and systems have signed the acceptable use agreement. Wifi passwords will be changed periodically

6. Online safety education engagement approaches

6.1 Engagement and education of children and young people

An online safety curriculum will be established and embedded throughout the schools, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.

- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the school's internal online safety education approaches.

6.2 Engagement and education of children and young people considered to be vulnerable

The federation will ensure that differentiated and ability appropriate online safety education is given, with input from specialist staff as appropriate (e.g. SENDCO).

6.3 Engagement and education of staff

The online safety policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.

6.4 Engagement and education of parents and carers

The federation recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology. Parents' attention will be drawn to the federation's online safety policy and expectations in newsletters, letters, school prospectus and school websites.

- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent consultation evenings.
- Parents will be expected to read the Acceptable Use Agreement for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

7.2 Security and Management of Information Systems

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data taken off site will be stored on encrypted laptops or encrypted USB drives.

7.3 Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff must always keep their password private and must not share it with others or leave it where others can find it.

7.4 Filtering and Monitoring

- The schools will ensure that we have age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- Any material that the school believes is illegal will be reported to appropriate agencies.

8. Responding to Online Incidents and Safeguarding Concerns

All members of the school community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.

- The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving child protection concerns, which will then be recorded and acted on appropriately.
- The school will manage online safety incidents in accordance with the school behaviour policy where appropriate.

9. Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

Calstock and Stoke Climsland Primary Schools will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting"). "Sexting" is viewed as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

- If either school is made aware of an incident involving creating youth produced sexual imagery they will:
    - Act in accordance with the school's child protection and safeguarding policy
    - Immediately notify the designated safeguarding lead.
    - Store the device securely.
    - Carry out a risk assessment in relation to the children involved.
    - Consider the vulnerabilities of children involved (including carrying out relevant checks with other agencies)
    - Make a referral to children's social care and/or the police (as needed/appropriate).
    - Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Implement appropriate sanctions in accordance with the schools' behaviour policy but taking care not to further traumatise victims where possible.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
    - Inform parents/carers about the incident and how it is being managed.
    - The schools will have regard to the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.
    - The schools will not view an image 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 (in these cases the image will only be viewed by the Designated Safeguarding Lead).
    - The schools will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.
    - If an indecent image has been taken or shared on the school network or devices then the school will take action to block access to all users and isolate the image.

9.2. Responding to concerns regarding Online Child Sexual Abuse and Exploitation

Calstock and Stoke Climsland Primary Schools will ensure that all members of the school community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children, how to respond to concerns and sources of support regarding online child sexual abuse.

- If the school is made aware of an incident involving online child sexual abuse of a child then it will:
    - Act in accordance with the federation child protection and safeguarding policy

- Immediately notify the designated safeguarding lead.
- Store any devices involved securely.
- Immediately inform police
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse, e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
- Carry out a risk assessment which considers any vulnerabilities of pupils involved (including carrying out relevant checks with other agencies).
- Make a referral via the MARU (if needed/appropriate).
- Put the necessary safeguards in place for pupils e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.

9.3. Responding to concerns regarding Indecent Images of Children (IIOC)

Calstock and Stoke Climsland Primary Schools will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC).

- If the school is made aware of Indecent Images of Children (IIOC) then the school will:
  - Act in accordance with the federation child protection and safeguarding policy
  - Immediately notify the school Designated Safeguard Lead.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations e.g. the police (using 999 if a child is at immediate risk), the LADO (if there is an allegation against a member of staff), children's social services.
  - Ensure where relevant 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.
  - 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.
- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
  - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
  - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.

9.4. Responding to concerns regarding radicalisation and extremism online

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. Staff and governors undertook WRAP training at Calstock CP School on 15 September 2016 (workshop to raise awareness of Prevent) and new governors and staff are asked to complete online Prevent training.

- If concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL), who is also the Single Point of Contact for Prevent, will be informed immediately and action will be taken in line with the child protection and safeguarding policy, including a referral to the MARU or discussing concerns with the Prevent Lead for Cornwall if appropriate.
- Online hate content will be responded to in line with existing school policies, including behaviour management. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately.
- Online safety education will enable children to understand at an age appropriate level that people they may encounter online including through online gaming, forums and chatrooms, may not be who they appear to be and may have an ulterior motive for befriending them.
- The danger of radicalisation will be countered by promoting British values through our curriculum and throughout school life.

9.5 Responding to concerns regarding cyberbullying

Cyberbullying, along with all other forms of bullying, of any member of Calstock and Stoke Climsland Primary Schools will not be tolerated and will be dealt with in line with the federation behaviour management policy.

- All incidents of online bullying reported will be investigated and recorded.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Local Authority Safeguarding Team and/or Police.
- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools' e-Safety ethos.

9.6 Responding to concerns regarding online hate

Online hate at Calstock and Stoke Climsland Primary Schools will not be tolerated.

- All incidents of online hate reported to the school will be recorded.

The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Local Authority Safeguarding Team and/or Police.