

St Day and Carharrack Community School



Online Safety Policy

Chair of Governors:

H L Collinge

Signed:

Helen Collinge

Date:

Summer 2019

Date for review:

Summer 2021

Scope of the Policy

This policy applies to all members of St Day and Carharrack School (including staff, governors, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of St Day and Carharrack School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off St Day and Carharrack School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

St Day and Carharrack School will deal with such incidents within this policy and associated behaviour and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online safety Governor. The role of the Online safety Governor will include:

- Regular meetings with the Online safety Co-ordinator
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors / Board / committee / meeting

Headteacher:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community
- The Headteacher and KS2 teacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the Online safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Online safety Coordinator:

takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority / relevant body

- liaises with NCI technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Online safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors (if required)

NCI Technical staff:

The Headteacher is responsible for ensuring:

- That the school's 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, in which passwords are regularly changed
- The filtering policy is applied and updated on a regular basis and that 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 / remote access is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher.

Teaching and Support Staff (including Governors, Volunteers and Visitors)

Are responsible for ensuring that:

They have an up to date awareness of online safety matters and of the current online safety policy and practices

- They have read, understood and signed the **Staff Acceptable Use Policy Agreement (Appendix 1)**
- They report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the online safety and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in

place for dealing with any unsuitable material that is found in internet searches

Child Protection / Safeguarding Designated Person

Should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils:

- Are responsible for using the school's digital technology systems in accordance with the **Pupil Acceptable Use Agreement (see Appendix 2)**
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online - Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. St Day and Carharrack School will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature.*- Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to the website / twitter
- Children are not permitted to bring into school mobile phones unless requested for a specific lesson. If on the rare occasion a child brings a mobile telephone into the school then this has to be handed into reception.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of

pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of ICT lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of Termly assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials/ content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Pupils need to seek permission to search the internet; staff should be vigilant in monitoring pupils use of websites.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website,
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant Newsletter

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Staff, Governors, Volunteers and Visitors must sign and agree to the terms of the **Acceptable Use Policy Agreement**.

Training will be offered as follows:

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
- The Online safety Coordinator will receive regular updates through attendance at external training events (eg from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online safety Coordinator will provide advice /guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions / online safety/ health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff and parents.

NCI Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that they meet recommended technical requirements
- There will be regular reviews and audits of the safety and security of NCI technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to technical systems and devices.
- The school secretary is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. NCI technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. An appropriate system is in place for users to report any actual / potential technical incident / security breach to the Headteacher. Incidents are logged in the school office and reported to NCI.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Prevent Strategy

As part of our commitment to safeguarding and child protection we fully support the government's Prevent Strategy, and take guidance from Teaching Approaches to help build resilience to extremism.

The Prevent strategy is a government strategy designed to stop people becoming terrorists or supporting terrorism. It:

- responds to the ideological challenge we face from terrorism and aspects of extremism, and the threat we face from those who promote these views
- provides practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support
- works with a wide range of sectors (including education, criminal justice, faith, charities, online and health)

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate

users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images. Parental permission will always be sought before this is permitted.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes unless agreed by the Headteacher.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate

- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

- Transfer data using encryption and secure password protected devices.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. St Day and Carharrack considers the benefit of using these technologies at certain times as the education benefits outweighs their risks / disadvantages:

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the nominated person – in accordance with the policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and students / pupils or parents / carers (email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media (See Appendix 3 Social Media Policy)

Social Media- Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.

- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

1. No reference should be made in social media to pupils, parents / carers or school staff
2. They do not engage in online discussion on personal matters relating to members of the school community
3. Personal opinions should not be attributed to the school
4. Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. **Incidents might involve illegal or inappropriate activities (see Appendix 4)**

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the Headteacher and report immediately to the police.

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

1. Have more than one member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
2. Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
3. It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

4. Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
5. Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority or national / local organisation (as relevant).
 - Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- Incidents of 'grooming' behaviour
- The sending of obscene materials to a child
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour procedures.

Student Incidents: Report to Headteacher for appropriate sanctions to be applied: informing parents/warning/exclusion.

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).

Unauthorised use of non-educational sites during lessons

Unauthorised use of mobile phone /digital camera / other mobile device

Unauthorised use of social media /messaging apps / personal email

Unauthorised downloading or uploading of files

Allowing others to access school network by sharing username and passwords

Attempting to access or accessing the school network, using another student's / pupil's account

Attempting to access or accessing the school network, using the account of a member of staff

Corrupting or destroying the data of other users

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature

Continued infringements of the above, following previous warnings or sanctions

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school

Using proxy sites or other means to subvert the school's / academy's filtering system

Accidentally accessing offensive or pornographic material and failing to report the incident

Deliberately accessing or trying to access offensive or pornographic material

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

Staff Incidents: refer to Headteacher who will inform technical support, LA or police. Sanctions include: Warning, Suspension or Disciplinary action.

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).

Inappropriate personal use of the internet / social media / personal email

Unauthorised downloading or uploading of files

Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account

Careless use of personal data eg holding or transferring data in an insecure manner

Deliberate actions to breach data protection or network security rules

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature

Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils

Actions which could compromise the staff member's professional standing

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school

Using proxy sites or other means to subvert the school's filtering system

Accidentally accessing offensive or pornographic material and failing to report the incident

Deliberately accessing or trying to access offensive or pornographic material

Breaching copyright or licensing regulations

Continued infringements of the above, following previous warnings or sanctions

Deliberate actions to breach data protection or network security rules

Monitoring and review



The Headteacher is responsible for monitoring the implementation of this policy and for seeking the views of



staff, children and parents. The Headteacher will report to the governing body on the effectiveness of this policy.

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

1. UK Safer Internet Centre

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

South West Grid for Learning - <http://swgfl.org.uk/>

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

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

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

2. CEOP

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

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

3. Others

INSAFE - <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

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

Netsmartz - <http://www.netsmartz.org/>

4. Tools for Schools

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

5. Bullying / Cyberbullying

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour -

<http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) -

<http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work>

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

6. Social Networking

Digizen – [Social Networking](#)

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

SWGfL - Facebook - [Managing risk for staff and volunteers working with children and young people](#)

[Connectsafely Parents Guide to Facebook](#)

[Facebook Guide for Educators](#)

7. Curriculum

SWGfL Digital Literacy & Citizenship curriculum

Glow - <http://www.educationscotland.gov.uk/usingglowandict/>

Teach Today – www.teachtoday.eu/

Insafe - [Education Resources](#)

8. Mobile Devices / BYOD

Cloudlearn Report [Effective practice for schools moving to end locking and blocking](#)

NEN - [Guidance Note - BYOD](#)

9. Data Protection

Information Commissioners Office:

[Your rights to your information – Resources for Schools - ICO](#)

[Guide to Data Protection Act - Information Commissioners Office](#)

[Guide to the Freedom of Information Act - Information Commissioners Office](#)

[ICO guidance on the Freedom of Information Model Publication Scheme](#)

[ICO Freedom of Information Model Publication Scheme Template for schools \(England\)](#)

[ICO - Guidance we gave to schools - September 2012](#) (England)

[ICO Guidance on Bring Your Own Device](#)

[ICO Guidance on Cloud Hosted Services](#)

[Information Commissioners Office good practice note on taking photos in schools](#)

[ICO Guidance Data Protection Practical Guide to IT Security](#)

[ICO – Think Privacy Toolkit](#)

[ICO – Personal Information Online – Code of Practice](#)

[ICO Subject Access Code of Practice](#)

[ICO – Guidance on Data Security Breach Management](#)

SWGfL - [Guidance for Schools on Cloud Hosted Services](#)

LGfL - [Data Handling Compliance Check List](#)

Somerset - [Flowchart on Storage of Personal Data](#)

NEN - [Guidance Note - Protecting School Data](#)

10. Professional Standards / Staff Training

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

[Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs](#)

[Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs](#)

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

11. Infrastructure / Technical Support

Somerset - [Questions for Technical Support](#)

NEN - [Guidance Note - esecurity](#)

12. Working with parents and carers

SWGfL Digital Literacy & Citizenship curriculum

[Online Safety BOOST Presentations - parent's presentation](#)

[Connectsafely Parents Guide to Facebook](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops / education](#)

[The Digital Universe of Your Children - animated videos for parents \(Insafe\)](#)

[Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide](#)

[Insafe - A guide for parents - education and the new media](#)

[The Cybersmile Foundation \(cyberbullying\) - advice for parents](#)

13. Research

[EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)

[Futurelab - "Digital participation - its not chalk and talk any more!"](#)

[Ofcom – Children & Parents – media use and attitudes report - 2015](#)

Acceptable Use Agreement for Staff, Governors, Volunteers and Visitors

St Day & Carharrack Community School Policy

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies out of school.
- I understand that the school digital technology systems are only intended for educational use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Headteacher.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted .
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this **Acceptable Use Policy** applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school digital technology systems and my own devices within these guidelines.

Staff /Governor/ Volunteer/ Visitor Name:

Signed:

Date:.....

Acceptable Computer Use Agreement for Children (updated 2018)

All children use computer facilities including Internet access as an essential part of learning. We expect all children to be safe and responsible when using any IT. Please read and discuss these eSafety rules with your child and return the slip to give your consent.

Computers are a fantastic resource and offer great potential to support the curriculum. Internet access at school is available to the children through NCI which is a safe environment, protected by both a firewall and filtered content.

We teach the children how to be responsible and safe with the resources and on the internet. We follow the rules of 'Be SMART on the internet' and age appropriate resources for KS 1 which can be found below and at www.childnet.com. This site contains lots of useful information for parents including how to support younger children.



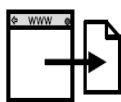
SAFE

Keep safe by being careful not to give out personal information - such as your name, email, phone number, home address, or school name - to people who you don't trust online.



MEETING

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.



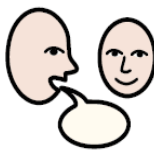
ACCEPTING

Accepting emails, IM messages, or opening files, pITures or texts from people you don't know or trust can lead to problems - they may contain viruses or nasty messages!



RELIABLE

Someone online may be lying about who they are, and information you find on the internet may not be reliable.



TELL

Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried. You can report online abuse to the police at: www.thinkuknow.co.uk.

St Day & Carharrack Community School

Acceptable Computer Use Agreement (updated 2018)

eSafety Rules

- I will follow the SMART rules and only use IT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will not tell other people my IT passwords.
- I will only open/delete my own files.
- I will make sure that all IT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of IT can be checked and that my parent will be contacted if a member of school staff is concerned about my eSafety.



Parent's Consent for Internet Access **September 2018**

Child's Name:

We have discussed the school e-safety rules and I give permission for my child to access the Internet. I understand that the school will take all reasonable precautions to ensure that children cannot access inappropriate materials but I appreciate that this is a difficult task. My child agrees to follow the e-Safety rules and to support the safe use of IT at St Day & Carharrack Community School.

Parent Signature

Class **Date**

Appendix 3

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the school*, its staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- **Applies to all staff and to all online communications which directly or indirectly, represent the school.**
- **Applies to such online communications posted at any time and from anywhere.**
- Encourages the safe and responsible use of social media through training and education
- *Defines the monitoring of public social media activity pertaining to the school*

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy. Digital communications with pupils/students are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control

Roles & Responsibilities

- **Headteacher**
 - Facilitating training and guidance on Social Media use.
 - Developing and implementing the Social Media policy
 - Taking a lead role in investigating any reported incidents.
 - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
 - Approve account creation
- **Administrator / NCI technician**
 - Create the account following Headteacher approval
 - Store account details, including passwords securely
 - Be involved in monitoring and contributing to the account
 - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
 - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
 - Attending appropriate training
 - Regularly monitoring, updating and managing content he/she has posted via school accounts

- Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a Twitter account, or a “Friends of the school” Facebook page. Anyone wishing to create such an account must present a plan to the Headteacher which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the Headteacher and Governors an application will be approved or rejected. In all cases, the Headteacher must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy.** Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy.** If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
 - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
 - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
 - Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
 - *The school permits reasonable and appropriate access to private social media sites.*
- **Pupil/Students**
 - **Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account unless they have reached age 18 and above.**
 - The school's education programme should enable the pupils to be safe and responsible users of social media.
 - Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- **Parents/Carers**
 - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**

- The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Social Media – Information for Staff

Managing your personal use of Social Media:

- “Nothing” on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts

The Do's

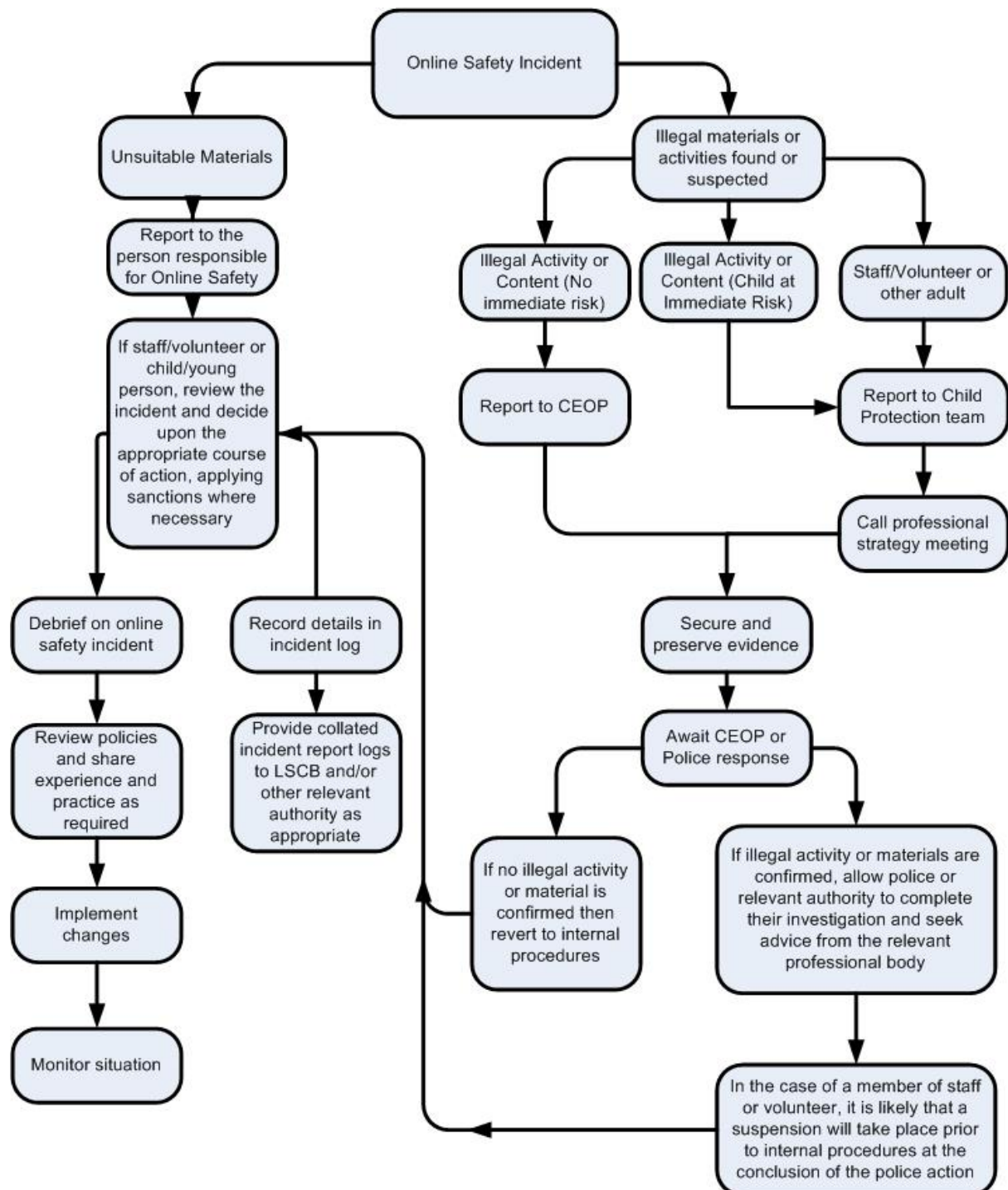
- Check with the Headteacher before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

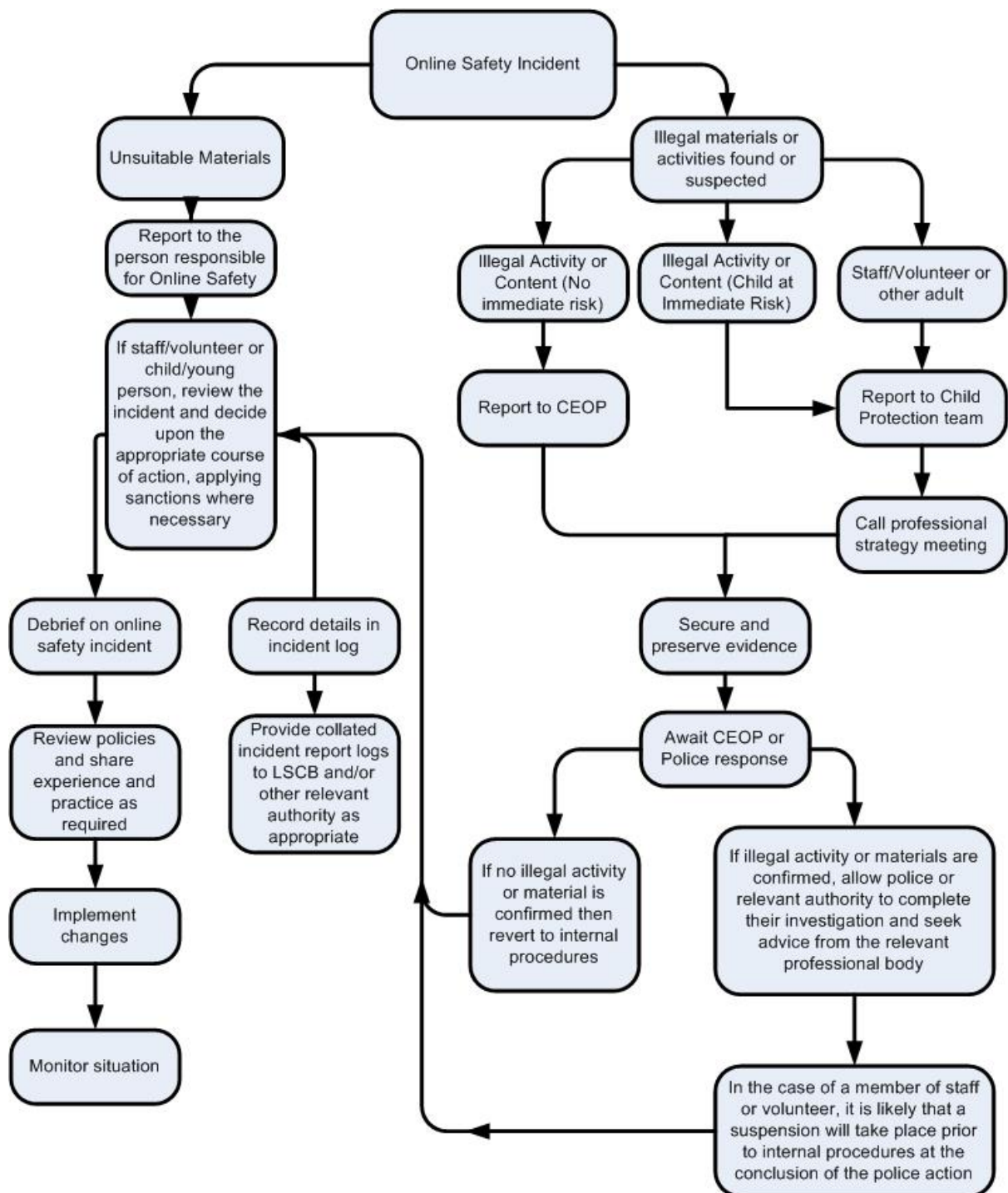
- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.



Responding to incidents of misuse – flow chart



Record of reviewing devices / internet sites (responding to incidents of misuse)

Year Group:

Date:

Reason for investigation:

.....

.....

.....

1. Details of first reviewing person

Name:

Position:

Signature:

2. Details of second reviewing person

Name:

Position:

Signature:

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address / device

Reason for concern

Conclusion and Action proposed or taken

Reporting Log

[illegible]

Training Needs Audit Log

[illegible]