Southerly Point Co-operative Multi-Academy Trust

Southerly Point Co-operative Multi-Academy Trust

ONLINE SAFETY AND DATA SECURITY POLICY

Equality Impact Assessment

The EIA has not identified any potential for discrimination or adverse impact and all opportunities to promote equality have been taken.*	✓
The EIA has not identified any conflict with the Trust's co-operative values and the Church Schools' values.	✓
Adjust the policy to remove barriers identified by the EIA or better promote equality.	✓

*Inclusive of protected characteristics

Provenance	**Date**
Working Party	**May 2017**
HR checks	**N/A**
Union Consultation	**Oct 2017**
Trustees' Ratification	**Dec 2017**
Implementation	**Feb 2018**

Review Date
By April 2018 in light of GDPR
April 2020

To be read in conjunction with:	**Data Protection and Freedom of Information policy** **Safeguarding and Child Protection Policy** **Staff Code of Conduct**

SCHOOL NAME: Wwendron Church of England Primary School

CCTV ON SITE: YES

KEY STAFF:

Senior Leader with responsibility for Online Safety & Data Protection	Mr. Paul Hunkin
Network Manager/ Network Service Provider	
Online Safety Co-ordinator	Mr. Paul Hunkin
Designated Safeguarding Lead	Mr. Paul Hunkin
Access to CCTV	Mr. Paul Hunkin

Southerly Point Co-operative Multi-Academy Trust

ONLINE SAFETY AND DATA SECURITY POLICY

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Instagram, Snapchat, Whatsapp, Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

We understand the responsibility to educate our pupils on Online Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

We hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the Trust and its schools. This can make it more difficult for us to use technology to benefit learners.

Everybody in the Trust has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Protocol (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the Trust (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned by the School at any time without prior notice.

If you are in doubt as to whether the individual requesting such access is authorised to do so, please contact the network manager or responsible Senior Leader.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Any violations will be investigated and dealt with in accordance with our Acceptable Use Policy, Behaviour Policy, Online Safety, Anti-Bullying, Safeguarding and any other relevant School policies.

Where specialist-monitoring software is in place, as deemed appropriate by individual schools' risk assessment (KCSIE 2016), it produces alerts to any access to inappropriate websites. It also gives an early warning of potentially harmful situations, like predator grooming or radicalisation threats. The captured evidence helps staff choose the best course of action, from support for victims of bullying, or protecting a vulnerable child, to confronting a pupil who is acting inappropriately. The monitoring software also provides a powerful incentive for pupils to use all technology and devices safely and concentrate in lessons.

Learning good habits at School prepares children for a continued safe digital future.

Breaches

A breach or suspected breach of policy by a Trust employee, contractor or pupil may result in the temporary or permanent withdrawal of Trust ICT hardware, software or services from the offending individual.

For staff, any policy breach is grounds for disciplinary action in accordance with the Trust Disciplinary Procedure and Staff Code of Conduct.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;

- Conduct audits to assess whether organisations' processing of personal data follows good practice
- Report to Parliament on data protection issues of concern

Pupils who breach this policy will be sanctioned in accordance with the School's behaviour policy.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the School's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. (See front page)

Please refer to the relevant section on Incident Reporting, Online Safety Incident Log & Infringement.

Acceptable Use Protocol (AUP): Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in School. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to read and agree to this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the responsible Senior Leader.

Please see Appendix 1 for the Staff Acceptable Use Protocol for signing.

Acceptable Use Protocol (AUP): Pupils

The Acceptable Use Protocol is intended to ensure:

- that the students in our care will be responsible users and stay safe while using the school's ICT resources and the internet for all use.
- that school / college ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Please see Appendix 2 for the Primary Pupil Acceptable Use Protocol.

Please see Appendix 3 for the Secondary Pupil Acceptable Use Protocol.

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- Where ICT equipment is issued to staff (laptops etc) it is logged and records serial numbers as part of the School's inventory.
- Do not allow your visitors to plug their ICT hardware into the School network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.
- Ensure that all ICT equipment that you use is kept physically secure when not in use. Portable devices should be locked away out of sight overnight.
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.
- It is imperative that you save your data on a frequent basis to the School's network. You are responsible for the backup and restoration of any of your data that is not held on the School's network.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted.
- A time locking screensaver is applied to all machines. Any device accessing personal data must

have a locking screensaver as must any user profiles.

- Privately owned ICT equipment should not be used on the School network, but access the internet through the School Wi-Fi is allowed at the discretion of the responsible Senior Leader.
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled.
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All ICT equipment allocated to staff must be authorised by the Network Manager or Senior Leader responsible for:
    - maintaining control of the allocation and transfer to the member of staff
    - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).
- Where access is provided to WIFI, a procedure is in place to remove access to the school WIFI for school leavers, both staff and pupils. Where Temporary Guest access is available, it will be restricted and passwords re-set regularly.

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy.
- Staff must ensure that all School data is stored on the School network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.
- Synchronise all locally stored data, including diary entries, with the central School network server on a frequent basis.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support.
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if supplied.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as Smartphones, iPads, games players, portable hard drives, cameras and smart watches etc. are generally very familiar to children outside of School. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in School is allowed. Our Trust chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones), often referred to as BYOD (Bring Your Own Device)

- The School allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the School allow a member of staff to contact a pupil using their personal device.
- In secondary schools, pupils are allowed to bring personal mobile devices/phones to School but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent. Use at social times is at the discretion of the school.
- In primary school, the use of mobile devices is solely at the discretion of the school.
- Staff who wish to set up and use a School e-mail account on their personal mobile device will need to have some form of device locking e.g. password or pin. If the device is lost or stolen, the Network Manager or responsible Senior Leader needs to be informed as soon as possible. The member of staff is responsible for ensuring the device is remotely wiped of data and must report that this has been done. This can done by a variety of methods. For further guidance ask your network manager.
- This BYOD technology may be used for educational purposes but the class teacher should agree the activity with the Responsible Senior Leader or Online Safety Co-ordinator.
- Decisions regarding access to the School Wi-Fi system will be made by the Senior Leader and decisions will be final and binding.
- Pupils and staff using personal mobile devices on the School Wi-Fi system are subject to internet filtering and expected to abide by the AUPs they have signed or agreed to electronically.
- The School is not responsible for the loss, damage or theft of any personal digital device
- The sending of inappropriate text, emails or instant messages between any member of the School community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the School community
- Users bringing personal devices into School must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the School community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the School community.
- Where the School provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.
- Where the School provides a laptop for staff, this device should only be used for School business.
- Never use a hand-held mobile phone whilst driving a vehicle.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using School provided anti-virus software before being used.
- Delete without reading any emails from people you do not know.
- Do not follow any links to questionnaires, offers, requests, etc. from unknown sources. Delete the email.
- Do not forward any suspect emails to anybody: Delete it.
- Delete emails with attachments that you were not expecting even if you know the person sending, if the wording seems “off” in some way. These programs can often spoof the Sender field in emails to make it look like someone you know is emailing you.

- Never interfere with any anti-virus software installed on School ICT equipment.
- If your machine is not routinely connected to the School network, you must make provision for regular virus updates through the ICT technical team.
- If you suspect there may be a virus on any School ICT equipment, stop using the equipment and contact the ICT technical team immediately. The ICT technicians will advise you what actions to take and be responsible for advising others that need to know.

Data Security

The accessing and appropriate use of data is something that the Trust takes very seriously.

Security

- The School gives relevant staff access to its Management Information System, with a unique username and password.
- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibilities in relation to accessing School data through staff meetings and/or staff bulletins.
- Staff have been issued with the relevant data protection policy documents and the ICT Acceptable Use Protocol.
- The Headteacher has identified relevant responsible persons for managing data security.
- Staff must keep all School related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times whenever possible.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared multi-function print, fax, scan and copiers are used. These devices are password protected to minimize risk.

Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the School's response. The responsible Senior Leader has the following responsibilities:

- lead on information risk assessment
- advise School staff on the appropriate use of information systems
- make sure that information handling complies with legal requirements

The Office of Public Sector Information has produced Managing Information Risk, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support relevant responsible staff members in their role.

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. SLT should be able to identify across the School:

- what information is held, and for what purposes
- what information needs to be protected, how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of

However, it should be clear to all staff that the handling of secure data is everyone's responsibility – whether

they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media formatted and over written at least 5 times or in line with the most recent government legislation to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to:

  The Waste Electrical and Electronic Equipment Regulations 2006

  The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

  http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

  http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

  http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

  Data Protection Act 1998

  https://ico.org.uk/for-organisations/education/

  Electricity at Work Regulations 1989

  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The School will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
- The School's disposal record will include:
  - Date item disposed of
  - Authorisation for disposal, including:
    - verification of software licensing
    - any personal data likely to be held on the storage media? *
  - How it was disposed of eg waste, gift, sale
  - Name of person & / or organisation who received the disposed item

* if personal data is likely to be held, the storage media will be over written at least 5 times or in line with latest government legislation, to ensure the data is irretrievably destroyed. We may also choose to physically destroy the storage media to reduce risk further.

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

E-mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of a school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsibly Online.

Managing e-mail

- The School gives all staff & governors their own e-mail account to use for all School business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- Staff & governors should use their School email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and

security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The School email account should be the account that is used for all School business

- Under no circumstances should staff contact pupils, parents, others members of staff or conduct any School business, using personal e-mail addresses
- The School requires a standard disclaimer to be attached to all e-mail correspondence, stating that:

  The information contained in this e-mail is confidential and may be legally privileged. It is intended solely for the use of the original recipient and others authorised to receive it. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking action in reliance of the contents of this information is strictly prohibited and may be unlawful. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system.

  We have taken reasonable precautions to ensure that this e-mail has been swept for viruses, we cannot however accept any liability for any related loss or damage that you may suffer as a consequence of our transmission of this e-mail.

  Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the school or Southerly Point Co-operative Multi-Academy Trust.
- The responsibility for adding this disclaimer lies with the network manager and will automatically be added as a footer. This disclaimer must not be edited or deleted by the account holder
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on School headed paper. They should be factual and professional.
- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
  - Delete all e-mails of short-term value
  - Do not use the e-mail application as an archiving or file storage system
  - E-mails that need to be kept should be identified for content and filed appropriately
  - Organise e-mail into folders and carry out frequent house-keeping on all folders, including 'sent' folder, retaining emails for a maximum of 18 months
- Staff must inform the Online Safety co-ordinator / line manager if they receive an offensive e-mail
- However you access your School e-mail, (whether directly, through webmail when away from the office or on personal hardware) all the School e-mail policies apply.
- Pupils may only use School approved accounts on the School system and only under direct teacher supervision for educational purposes.
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible Online Safety behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail

Pupils are introduced to e-mail as part of the Computing Programme of Study.

Sending e-mails

- Use your own School e-mail account so that you are clearly identified as the originator of a message. Having a clearly defined subject line helps the recipient to sort the email on receipt. A clear subject line also assists in filing all emails relating to individual projects in one place.
- On the 'To' line, only include the name of the person(s) who needs to undertake the action and c.c. those who need the email for information only
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the

minimum necessary and appropriate. Avoid the use of global or group address lists unless it is absolutely necessary. Never send on chain emails.

- If you send a message externally to more than one person, you must hide the recipients' email addresses. You can do this by putting just your own name in the "To" field, and putting the other addresses in the "Bcc" field.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal matters, including personal business, disputes or legal affairs, nor state views that may be libelous or detrimental to the reputation of the School
- Whenever possible, omit personal identifiable data such as names, date of birth, address, etc. from any emails. When referring to pupils in emails use their initials in the 'subject' of the email and not their full name.
- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section:
- E-mailing Sensitive, Confidential or Classified Information

Receiving e-mails

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; consult your network manager or responsible Senior Leader first (see earlier)
- Do not use the e-mail systems to store attachments. Where the main purpose of the email is to transfer documents, then the documents should be saved into the appropriate places in an electronic filing system or printed out and added to a paper file. The email can then be deleted.
- When receiving an email containing personal identifiable information about a pupil, parent/carer or member of staff, the email is classified as a record which must be dealt with appropriately under data protection guidelines. In these cases, print off a hard copy and place in the appropriate pupil or staff file or copy and save the information to the SIMS record and retain in line with the records retention schedule.
- Do not set up rules to automatically forward your School e-mail to a personal e-mail account.

E-mailing Sensitive, Confidential or Classified Information

ICO Definitions of personal and sensitive data:

- Personal data means data which relate to a living individual who can be identified, this can be names, addresses, photos, or other unique information to that person or individual such as a UPN or payroll number.
- Sensitive personal data means personal data consisting of information as to:-
    - the racial or ethnic origin of the data subject,
    - political opinions,
    - religious beliefs or other beliefs of a similar nature,
    - whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
    - physical or mental health or condition,
    - sexual life,
    - the commission or alleged commission by them of any offence, or
    - any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

- Where your conclusion is that e-mail must be used to transmit such data:

  Obtain express consent from your line manager to provide the information by e-mail and exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

    - Encrypt and password protect. See the Network Manager or responsible Senior Leader on how to do this.
    - Verify the details, including accurate e-mail address, of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

  - Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

Equal Opportunities

Pupils with Additional Needs

The School endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the School's Online Safety rules.

However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children and young people.

Online Safety

Online Safety - Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership for which the Trustees have ultimate responsibility to ensure that the policy and practices are embedded and monitored. In practice this is fulfilled by headteachers supported by governors in individual schools. Each school has a named Online Safety co-ordinator. All members of the School community have been made aware of who holds this post. It is the role of the Online Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Cornwall LA, CEOP (Child Exploitation and Online Safety Protection) and Childnet. The responsible Senior Leader and Online Safety co-ordinator update Senior Management and governors and all governors have an understanding of the issues and strategies at our School in relation to local and national guidelines and advice.

This policy, supported by the Trust's acceptable use protocols for staff, governors, visitors and pupils, is to protect the interests and safety of the whole School community. It is linked to the following School policies: safeguarding, child protection, health and safety, home–school agreements, and behaviour (including the anti-bullying) policy and PSHCE.

Online Safety in the Curriculum

ICT and Online Safety resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum and we continually look for new opportunities to promote Online Safety.
The School has a framework for teaching internet skills in Computing lessons
The School provides additional opportunities which may include PSHCE days, projects and tutorials to teach about Online Safety

- Educating pupils about the Online Safety risks that they may encounter outside School is done

informally when opportunities arise and as part of the Online Safety curriculum

- Pupils are made aware (as age appropriate) of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas (as age appropriate) through discussion, modeling and appropriate activities
- Pupils are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of Online bullying. Pupils are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Cyber mentors, Childline or CEOP report abuse button (as age appropriate)
- Pupils are taught to critically evaluate materials and learn good searching skills through the Computing curriculum and through general research opportunities in other subjects (as age appropriate).

Online Safety Skills Development for Staff

- Our staff receive regular information and training on Online Safety and how they can promote the 'Stay Safe' Online messages for example through staff meetings, briefings, bulletins and tutorial resources
- New staff receive information on the School's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the School community (see Online Safety Co-ordinator)
- All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the School Online Safety Messages

- We endeavour to embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used
- The key messages in the Online Safety policy will be introduced to the pupils at the start of each academic year
- Online Safety posters will be prominently displayed
- The key Online Safety advice will be promoted widely through School displays, website, newsletters, class activities and so on
- We will participate in Safer Internet activities as part of the school curriculum.

Incident Reporting, Online Safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the School's relevant responsible person or Online Safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access passwords), virus notifications, dubious emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the responsible Senior Leader.

Online Safety Incident Log

Keeping an incident log is an effective way of monitoring what is happening and identify trends or specific concerns within school (e.g. loss of equipment; cyberbullying; other breaches of the Online Safety policy) This is kept by the responsible Senior Leader. For example:

School Name Online Safety Incident Log

Details of ALL Online Safety incidents to be recorded by the Online Safety Co-ordinator.This incident log will be monitored termly by the Headteacher, Senior Leader or Safeguarding Governor. Any incidents involving Cyberbullying may also need to be recorded elsewhere.

Date & Time	Name of Pupil/Staff member	Male or female	Room and computer device number	Details of incident (including evidence)	Actions and reasons

The grid should be used in conjunction with the monitoring software.

Misuse and Infringements

Complaints

Complaints and/ or issues relating to Online Safety should be made to the Online Safety co-ordinator or responsible Senior Manager. Incidents should be logged and the Flowcharts for Managing an Online Safety Incident should be followed.

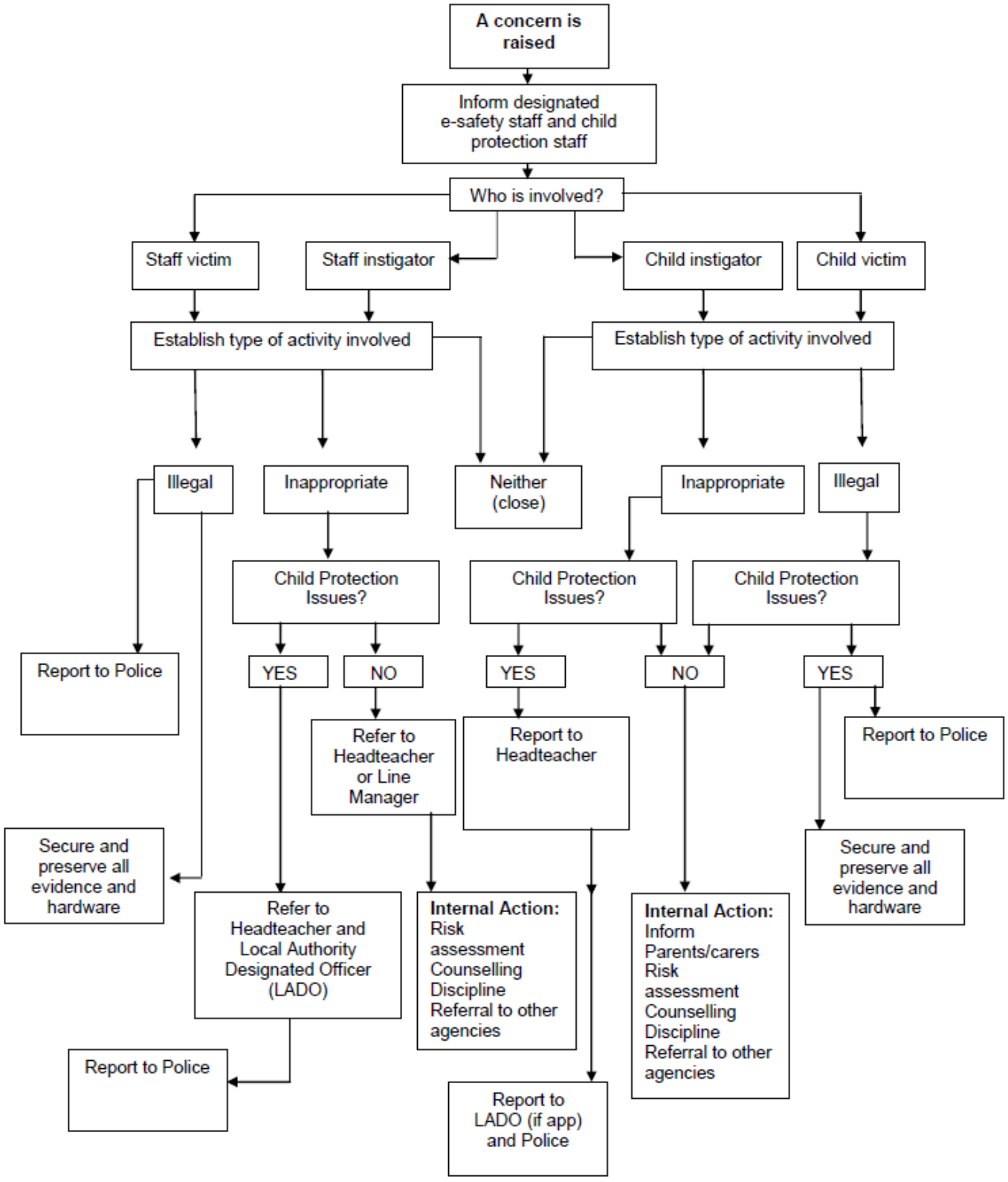
Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Online Safety co-ordinator or responsible Senior Leader

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation co-ordinated by the Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)

Users are made aware of sanctions relating to the misuse or misconduct for example through login information messages, staff guides, websites and AUPs.

Managing an Online Safety Incident



Other Incidents

It is hoped all members of the School community will be responsible users of digital technologies, who understand and follow School 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 of accessing inappropriate material, all steps in this investigative procedure should be followed in order to protect those undertaking the investigation:

- Have more than one senior member of staff / volunteer involved in this process. Investigating staff must not look at the material on their own. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the investigation 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.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the investigation, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- 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)
- 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 investigation 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. All documentation from the investigation 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 / disciplinary procedures.

Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use through the School network is logged and software continually monitors for any inappropriate use, taking screenshots of such activity. Whenever any inappropriate use is detected, it will be followed up and logged.

Managing the Internet

The School provides pupils with filtered and supervised access to Internet resources (where reasonable) through the School's fixed and mobile internet connectivity

Staff will preview any recommended sites, Online services, software and apps before use

Searching for images through open search engines is potentially risky; checks should be carried out beforehand by the teacher and guidance on appropriate search terms and techniques should be provided to pupils

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher

All users must observe software copyright at all times. It is illegal to copy or distribute School software or illegal software from other sources

All users must observe copyright of materials from electronic resources

Internet Use

You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience

Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other Online application

On-line gambling or non-educational gaming is not allowed in School

Social networking is not allowed in School other than the School's official Facebook page and Twitter feeds (exceptions may be agreed with the Online Safety co-ordinator for educational purposes related to Online Safety)

If staff or pupils discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the Online Safety coordinator, network manager or teacher as appropriate

It is at the responsible Senior Leader's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- Our School uses web-filtering which is the responsibility of the Network Manager
- The Trust schools are aware of their responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and pupils are aware that School based email and internet activity is filtered, monitored and explored further if required
- The School may use management control tools for controlling and monitoring workstations but at the very least staff will be vigilant for misuse of computers by their classes
- It is the responsibility of the School, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all School machines
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the School's responsibility nor the network manager's responsibility to install or maintain virus protection on personal systems. If pupils or staff are concerned about possible infection of their removable media it must be given to the IT technician or Online Safety co-ordinator for a safety check first
- Pupils and staff are not permitted to download programs or large files on School based technologies without seeking prior permission from network manager
- If there are any issues related to viruses or anti-virus software, the network manager should be informed as soon as possible

Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- The School endeavors to deny access to social networking and Online games websites to pupils within School
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our pupils are asked to report any incidents of Cyberbullying to the School
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using systems approved by the responsible Senior Leader.
- Social Media such as Facebook and Instagram have age related Terms and Conditions which should be observed. http://www.coppa.org/comply.htm

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting Online Safety both in and outside of School and to be aware of their responsibilities. We regularly consult and discuss Online Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are actively encouraged to contribute to adjustments or reviews of the School Online Safety policy through parent voice activities
- Parents/carers are asked to read through and sign acceptable use protocol on behalf of their child on admission to the School
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (eg, on the School website)
- The School disseminates information to parents relating to Online Safety where appropriate in the form of;
    - Information evenings
    - Practical training sessions eg current Online Safety issues
    - Leaflets
    - School website information
    - Newsletter items

Passwords and Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Visitors such as supply staff and pupil teachers may be given a particular 'Cover' or 'Trainee' or 'Visitor' username and password, with suitable access rights. These areas are checked, files deleted and passwords changed as appropriate.

Staff and pupils are regularly reminded of the need for password security.

- **Always use your own** personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Passwords must contain a minimum of six characters and be difficult to guess
- Password changes will be enforced every term for staff
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on loose paper or in an unprotected file
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- **Never tell a child or colleague your password**
- **If you aware of a breach of security with your password or account inform the network manager immediately**
- Passwords for staff and pupils who have left the School are changed immediately and their accounts are subsequently removed from the system. Leaving procedures are in place to enable this to happen.

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- All staff usernames are fitted with an automatic lockout screen
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-School environment
- Only download personal data from systems if expressly authorised to do so by the responsible Senior Leader
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the appropriate schedule

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media is purchased with encryption or consult with the Network Manager or Trust IT Technicians who will be able to install encryption software
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or formatted and overwritten at least 5 times or in accordance with the latest government legislation.

Remote Access via any Device

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to School systems, keep all dial-up access information such as logon IDs, passwords and additional passphrase confidential and do not disclose them to anyone
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the School community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the School permits the appropriate taking of images by staff and pupils with School equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Responsible Senior Leader, images can be taken provided they are transferred immediately and solely to the School's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the responsible Senior Leader. Such images of pupils and/ or staff must be stored and used for School purposes in line with School policy and must never be distributed outside the School network without the permission of all parties involved. This includes educational visits, all occasions when the pupil is in School uniform or when otherwise representing the School
- Staff must check image permissions recorded in SIMS before any image can be uploaded for publication
- On occasions, it may be suitable to seek separate permissions for certain events such as trips and visits and where media organisations may be present for example.

Consent of Adults Who Work at the School

Permission to use images of all staff who work at the School is sought on induction and a copy is located in the personnel file

Publishing Pupil's Images and Work

On a child's entry to the School, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the School web site and social media page
- in the School prospectus and other printed publications that the School may produce for promotional purposes

- in promotional videos and CDs
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this School unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the School.

Pupils' names will not be published alongside their image unless permission has been given. Pupils' full names will not be published unless permission has been given. E-mail and postal addresses of pupils will not be published.

Only a small number of staff have access to School approved internet systems and the appropriate authority to upload to the internet. Uploading names and/or images to unofficial systems is not permitted and could result in disciplinary action.

Storage of Images

- Images/ films of children are downloaded and stored on the School's network and within online storage such as the School's Google Apps for Education environment
- Pupils and staff are not permitted to use personal portable media for storage of images (eg, USB sticks) without the express permission of the Responsible Senior Leader
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the School network or Google Apps
- The relevant staff who uploaded the images have the responsibility of deleting the images when they are no longer required.

Webcams and CCTV where used:

- Where the School uses CCTV, it is for security and safety. Designated staff have access to CCTV (see front sheet) Notification of CCTV use is displayed at the front of the School. Please refer to the hyperlink below for further guidance https://ico.org.uk/about-the-ico/consultations/cctv-code-of-practice-revised/
- Misuse of any webcam by any member of the School community will result in sanctions (as listed under the 'inappropriate materials' section of this document)
    - Cameras can be found around the School site. Notification is given in the areas filmed by cameras by signage
    - Parents/carers and staff are notified of the use of CCTV in the relevant Privacy Notice
- Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices
- We do not use publicly accessible webcams in School
- Webcams will not be used for broadcast on the internet without prior parental consent

Video Conferencing

This type of activity takes place very rarely. If pupils are involved:

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the School
- All pupils are supervised by a member of staff when video conferencing
- The School keeps a record of video conferences, including date, time and participants
- Approval from the Responsible Senior Leader is sought prior to all video conferences within School to end-points beyond the School
- No part of any video conference is recorded in any medium without the written consent of those

taking part

Servers

- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Data must be backed up regularly on a separate server located in a different building

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our School uses social media to communicate with parents and carers. A small School communications team is responsible for all postings on these technologies and monitors responses from others
- Staff ***are not*** permitted to access their personal social media accounts using School equipment at any time
- Selected ICT staff are able to setup Social Learning Platform accounts, using their School email address, in order to be able to teach pupils the safe and responsible use of social media
- Pupils are not permitted to access their social media accounts on School equipment or through School Wi-Fi.
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, pupils, parents and carers are made aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, pupils, parents and carers are made aware that their online behaviour should at all times be compatible with UK law
- Staff must not post inappropriate comments on social media about pupils, parents, colleagues or the School in general. Staff are required to uphold the reputation of the School, to maintain reasonable standards in their own behaviour, and to uphold public trust in the profession. Bringing the School or your profession into disrepute will result in disciplinary action, possibly leading to dismissal.
- If staff experience online abuse from pupils or parents, it is important not to retaliate i.e. personally engage with cyberbullying incidents. Keep any records of abuse – texts, emails, voice mails, or instant messages. Take screen prints of messages or web pages. Record the time, date and address of the site. Inform the Headteacher at the earliest opportunity so that the matter can be dealt with appropriately.

Systems and Access

- You are responsible for all activity on School systems carried out under any access/account rights assigned to you, whether accessed via School ICT equipment or your own devices
- Do not allow any unauthorised person to use School ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from School ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the School or may bring the School into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the School's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Hard drives must be formatted and overwritten at least 5 times or in line with the current government legislation. If someone outside of the Trust is appointed to dispose of the equipment, they must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data in the proscribed manner.

Writing and Reviewing this Policy

Staff and Pupil Involvement in Policy Creation

Staff, governors and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use through staff meetings, governor meetings and pupil council/digital leader meetings

Review Procedure

There will be on-going opportunities for staff to discuss with the Online Safety coordinator any Online Safety issue that concerns them.

There will be on-going opportunities for staff to discuss with the Responsible Senior Leader any issue of data security that concerns them.

There will several opportunities for pupils to feed back and contribute to the review of this policy e.g. via school council or pupil digital leaders meetings.

This policy will be reviewed every 2 years by the Trust and consideration will be given to the implications for future whole School development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Current Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to Online Safety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Appendix 1

Staff Acceptable Use Protocol

Southerly Point Co-operative Multi-Academy Trust

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in School. This protocol is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to read and agree to this protocol and adhere at all times to its contents. Any concerns or clarification should be discussed with the responsible Senior Leader.

- I will only use the School's email / Internet / Intranet / Google Apps and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the School or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, or any other personal social media link, to pupils.
- I will only use the approved, secure e-mail system for any School business.
- I will ensure that personal data (such as data held on SIMS software) is kept secure and is used appropriately, whether in School, taken off the School premises or accessed remotely. Personal data can only be taken out of School or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted and stored on a password secured laptop or memory stick.
- I will ensure that if I use my mobile device (phone or tablet) for school purposes, it will be thumbprint or pin protected. I understand that the school has the right to review my personal phone if I use it for school purposes.
- I accept that if I mislay my personal phone, where used for school purposes, that it is my responsibility to report this to the network manager/senior manager responsible for Online Safety and I must ensure that the phone is wiped clear of data.
- I will not install any hardware or software on school machines/network without permission of the network manager/senior person responsible for Online Safety and data security.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will not take images of children on my personal mobile devices.
- I will only take, store and use images of pupils and/or staff for professional purposes in line with Online Safety and data security and data protection policy and with the consent of the parent/carer or staff member. Once the images have served their function, I will delete them in accordance with the school's data protection guidelines.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- 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 understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my Online Safety activity, both in School and outside School, will not bring the School, my professional role or that of others into disrepute.
- I will support and promote the School's Online Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

Please complete the section below to show that you have read, understood and agree to the rules included in the Acceptable Use Protocol. If you do not sign and return this protocol, access will not be granted access to school / college ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school / college)
- I use my own equipment out of school / college in a way that is related to me being a member of this school / college. Eg. Communicating with other members of the school / college, accessing school / college email, website etc.

Name
Signed
Date

Appendix 2

Primary Pupil Acceptable Use Protocol

This Acceptable Use Protocol is intended to ensure:

- that the children in our care will be responsible users and stay safe while using the school's ICT resources and the internet for all use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Protocol

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I will not use the school's ICT systems without permission.
- I will always make sure an adult is present when I am using the internet.
- I understand that the school will monitor the way I use the school's ICT systems and email.
- I will not tell anyone my password.
- I will never try to use someone else's password or user name.
- I will be aware of "stranger danger", when I am on-line.
- I will not share personal information about myself or others when on-line.
- I will never arrange to meet people off-line that I have communicated with on-line.
- I will tell an adult if I see any unpleasant or inappropriate material or messages, or anything that makes me feel uncomfortable while on-line.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or change anyone else's files, without their knowledge and permission.
- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language.
- I will not take or share images of anyone without their permission.

I understand that the school has a responsibility to make sure the school's ICT systems are secure and that they run smoothly:

- I will not bring my mobile phone or handheld device into school unless my parent or guardian has requested this for a particular reason and I have permission from the Headteacher to do so.
- I will not try to upload, download or access any materials which are illegal, inappropriate or may cause harm or distress to others.
- I will not try to bypass the school's filtering / security systems.
- I will tell a teacher of any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email.
- I will not install or attempt to install programmes of any type on a school computer.
- I will not try to alter computer settings.
- I will never use chat and social networking sites at school. I will remember how to stay safe when using them at home.

When using the internet I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- I will not try to download music and video which is protected by copyright.
- I should take care to check that any information that I use is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour when I am out of school where they involve my membership of the school community.
- I understand that if I break the rules set out in this Acceptable Use Protocol may lose access to the school's network and internet. My parents will be informed and, in the event of illegal activities, the police will be contacted.

Please complete the section below to show that you have read, understood and agree to the rules included in the Acceptable Use Protocol. ***If you do not sign and return this protocol, access will not be granted to school ICT systems.***

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school);
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, website etc.

Name of Pupil	Class
Signed (child)	
Date	

Appendix 3

Secondary Pupil Acceptable Use Protocol

Southerly Point Co-operative Multi-Academy Trust

This Acceptable Use Protocol is intended to ensure:

- that the students in our care will be responsible users and stay safe while using the school's ICT resources and the internet for all use.
- that school / college ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Protocol

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school / college purposes.
- I will not download or install software on school technologies.
- I will only log on to the school / college network, other systems and resources with the user name and password and have been given by the school.
- I will follow the school's / college's ICT security system and where I have a password will not reveal it to anyone and change them regularly.
- I will only use my school / college e-mail address.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.
- I will be aware of "stranger danger" when I am communicating on-line and I will not disclose or share personal information about others, or myself such as name, phone number or address.
- I am aware that when I take images of pupils and / or staff, I must only store and use these for school / college purposes in line with school / college policy and must never distribute these outside the school / college network without the permission of all parties involved. This includes educational visits and all occasions when I am in school uniform or when otherwise representing the school / college.
- I will ensure that my Online Safety activity, both in and outside school /college, will not cause my school / college, the staff, pupils or others distress or bring the school / college community into disrepute, including through uploads of images, video, sounds or texts.
- I will support the school / college approach to Online Safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school / college community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school / college if I have permission. I understand that, if I do use my own devices in school / college, I will follow the rules set out in this protocol, in the same way as if I was using school / college equipment.
- I understand that the school / college will not accept responsibility for the loss or damage of my personal electronic devices that I am given permission to or choose to bring on site.
- I understand that all my use of the Internet and other related technologies will be monitored and logged and can be made available to my teachers.

- I understand that these rules are designed to keep me safe; that if they are not followed, school / college sanctions will be applied and my parent / carer may be contacted. I also understand that, in the case of illegal activities, the police will be involved.

BESPOKE:

Please complete the section below to show that you have read, understood and agree to the rules included in the Acceptable Use Protocol. If you do not sign and return this protocol, access will not be granted access to school / college ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school / college)
- I use my own equipment out of school / college in a way that is related to me being a member of this school / college. Eg. Communicating with other members of the school / college, accessing school / college email, website etc.

Name of Student	Tutor Group
Signed	
Date	