"Love your neighbor as yourself. There is no commandment greater than this."
Mark Chapter 12: Verse 31

Data Security & Acceptable use of ICT Policy

Author:	Deputy Principal - Behaviour and Attitudes
Date adopted by Governors/Academy:	September 2017
Date of last review/amendment:	May 2023
Date of next review:	May 2025

"Love your neighbor as yourself. There is no commandment greater than this."
Mark Chapter 12: Verse 31

Introduction

At All Saints Academy our vision is "Living Well Together with **Dignity**, **Faith** and **Hope**". We aspire to take dignified decisions and afford dignity to all members of our community, regardless of background or circumstance. Our position as a Voluntary Aided Church Academy means that the Christian faith has a central role in all of our actions and decisions. We strive for excellence in all that we do, enabling our students to transform their lives and to hope for happy and successful futures.

Our vision translates into our everyday practice. The values of **Dignity, Faith** and **Hope** are particularly relevant in ensuring 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
- Email, Instant Messaging and chat rooms
- Social Media, including 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).

At All Saints Academy, we understand the responsibility to educate our pupils on eSafety 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.

Schools 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 school. This can make it more difficult for your school to use technology to benefit learners.

"Love your neighbor as yourself. There is no commandment greater than this."
Mark Chapter 12: Verse 31

Everybody in the Academy community 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 Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as iPads, 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).

The value of dignity is particularly relevant when we consider the needs of students with Special Educational Needs or Disabilities as we want to promote a community which is inclusive and accessible by all.

Purpose

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 sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Senior Leader responsible for GDPR.

This policy sets out the framework for a clear and consistent assessment of the overall performance of teachers, including the Executive Principal, and for supporting their development within the context of the academy's plan for improving educational provision and performance, and the standards expected of teachers. It also sets out the arrangements that will apply when teachers fall below the levels of competence that are expected of them.

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the Academy 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 ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, 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 academy business related information; to confirm or investigate compliance with Academy policies, standards and procedures; to ensure the effective operation of Academy ICT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Regulation 2018, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the email or voicemail 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 General Data Protection Regulation 2018, 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.

Breaches

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

“Love your neighbor as yourself. There is no commandment greater than this.”
Mark Chapter 12: Verse 31

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

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

- higher maximum penalty - £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher

- or, standard maximum penalty £8.7 million or 2% of the total annual worldwide turnover in the preceding financial year, whichever is higher

for serious breaches of the General Data Protection Regulation.

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

- Conduct an audit to check compliance with obligations as a trust service provider, and make recommendations
- Serve and Enforcement Notice order is there has been a breach, requiring an organisation to take specified steps to comply with the law
- Issue a Monetary Penalty Notice requiring you to pay £1,000
- Prosecute those who commit criminal offences under the Act;
- Report to Parliament on data protection issues of concern

> "Love your neighbor as yourself. There is no commandment greater than this."
> Mark Chapter 12: Verse 31

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 Academy's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individual in the school is the member of SLT responsible for GDPR.

Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements.

Computer viruses

- All files downloaded from the Internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- 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 your IT team.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Data security

- The Academy 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 responsibility when accessing school data

- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use

- Staff 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

- It is the responsibility of individual staff to ensure the security of any personal or sensitive information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used

Relevant Responsible Persons

Members of the Senior Leadership Team will have the following responsibilities:

- lead on the information risk policy and risk assessment
- advise Academy staff on appropriate use of school technology
- act as an advocate for information risk management

The Office of Public Sector Information has produced Information security - The National Archives to support relevant responsible staff members in their role.

“Love your neighbor as yourself. There is no commandment greater than this.”
Mark Chapter 12: Verse 31

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 over written multiple times 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

_General Data Protection Regulation 2018

- Electricity at Work Regulations 1989
  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

The Academy will maintain a comprehensive inventory of all its ICT equipment including a record of disposal. The Academy’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 e.g. waste, gift, sale
- Name of person and / or organisation who received the disposed item

*if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

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

Further information available at:
Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website
https://ico.org.uk/

Email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email 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 email in relation to their age and how to behave responsibly online.

Staff and governors should use a school email account for all official communication to ensure that children are protected through the traceability of all emails through the school email system. In addition, it is important that governors are protected against possible allegations of inappropriate contact with children. This is to help mitigate the chance of issues occurring and is an essential element of the safeguarding agenda.

Managing Email

- The Academy gives all staff and governors their own email 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 emails and avoids the risk of personal profile information being revealed

- Staff and 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 email 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/carers or conduct any school business using personal email addresses

- The school requires a standard disclaimer to be attached to all email correspondence, stating that, ***‘the views expressed are not necessarily those of the school or the LA’***. The responsibility for adding this disclaimer lies with the account holder

- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

- Staff sending emails to external organisations, parents/carers or pupils are advised to cc. the Executive Principal, line manager or designated line manager

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes

- Emails 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 email account as follows:
    - ➢ Delete all emails of short-term value
    - ➢ Organise email into folders and carry out frequent house-keeping on all folders and archives

- The forwarding of chain emails is not permitted in school. All pupil email users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email 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 email

- Staff must inform the member of SLT responsible for GDPR or their line manager if they receive an offensive email

- Pupils are introduced to email when they are issued with their iPads.

- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all Academy email policies still apply

Sending emails

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section Emailing Personal or Confidential Information
- Use your own school email account so that you are clearly identified as the originator of a message
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School email is not to be used for personal advertising

Receiving emails

- Check your email regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; consult your network manager first
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of emails is not allowed

Emailing Personal or Confidential Information

Where your conclusion is that email must be used to transmit such data, obtain express consent from your manager to provide the information by email and **exercise caution when sending the email and always follow these checks before releasing the email:**

- Encrypt and password protect.
- Verify the details, including accurate email address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to email requests for information
- Do not copy or forward the email 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 email
- 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 email
- Request confirmation of safe receipt

Equal opportunities

Pupils with Additional Needs

The Academy endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' eSafety 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 eSafety issues.

“Love your neighbor as yourself. There is no commandment greater than this.”
Mark Chapter 12: Verse 31

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

eSAFETY

eSafety – Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Executive Principal and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Simon Miller who has been designated this role as a member of the Senior Leadership Team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Leaders and governors are updated by the Executive Principal/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at the Academy in relation to local and national guidelines and advice.

This policy, supported by the Academy’s acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policies and Personal Development Policy.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school provides opportunities within a range of curriculum areas to teach about eSafety as part of the creative curriculum

- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum

- Pupils are aware 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 through discussion, modeling and appropriate activities

- Pupils are 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 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 Childline or the ‘CEOP report abuse’ button

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the PSHCE programme and the ICT curriculum.

eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety and how they can promote the ‘Stay Safe’ online messages in the form of INSET, staff briefings and the staff bulletin.

"Love your neighbor as yourself. There is no commandment greater than this."
Mark Chapter 12: Verse 31

- Details of the ongoing staff training programme can be found *on the school training program*

- 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 eSafety and know what to do in the event of misuse of technology by any member of the school community (see eSafety Coordinator)

- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used and are part of the creative curriculum

- The eSafety policy will be introduced to the pupils at the start of each school year

- eSafety posters will be prominently displayed

- The key eSafety advice will be promoted widely through school displays, newsletters, class activities and so on

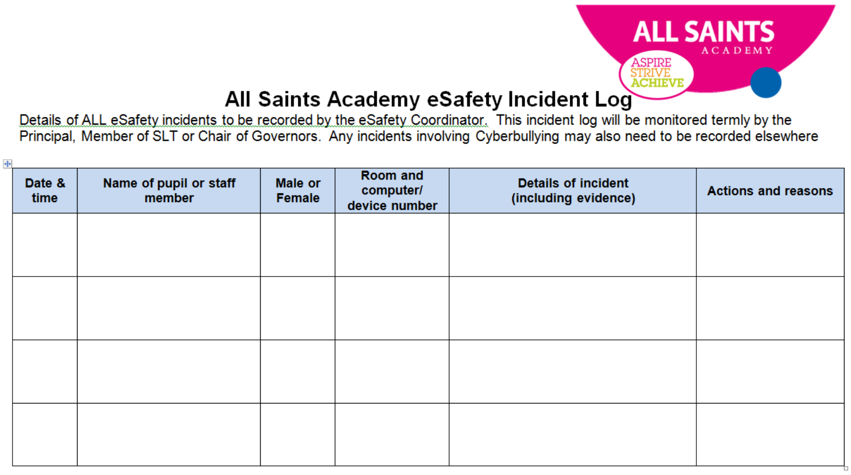
Incident reporting, ESafety incident log & infringements

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 eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Information Asset Owner.

eSafety Incident Log

An incident log allows us to monitor what is happening and identify trends or specific concerns.



ALL SAINTS ACADEMY
ASPIRE STRIVE ACHIEVE

All Saints Academy eSafety Incident Log

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Principal, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying may also need to be recorded elsewhere

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Executive Principal.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator

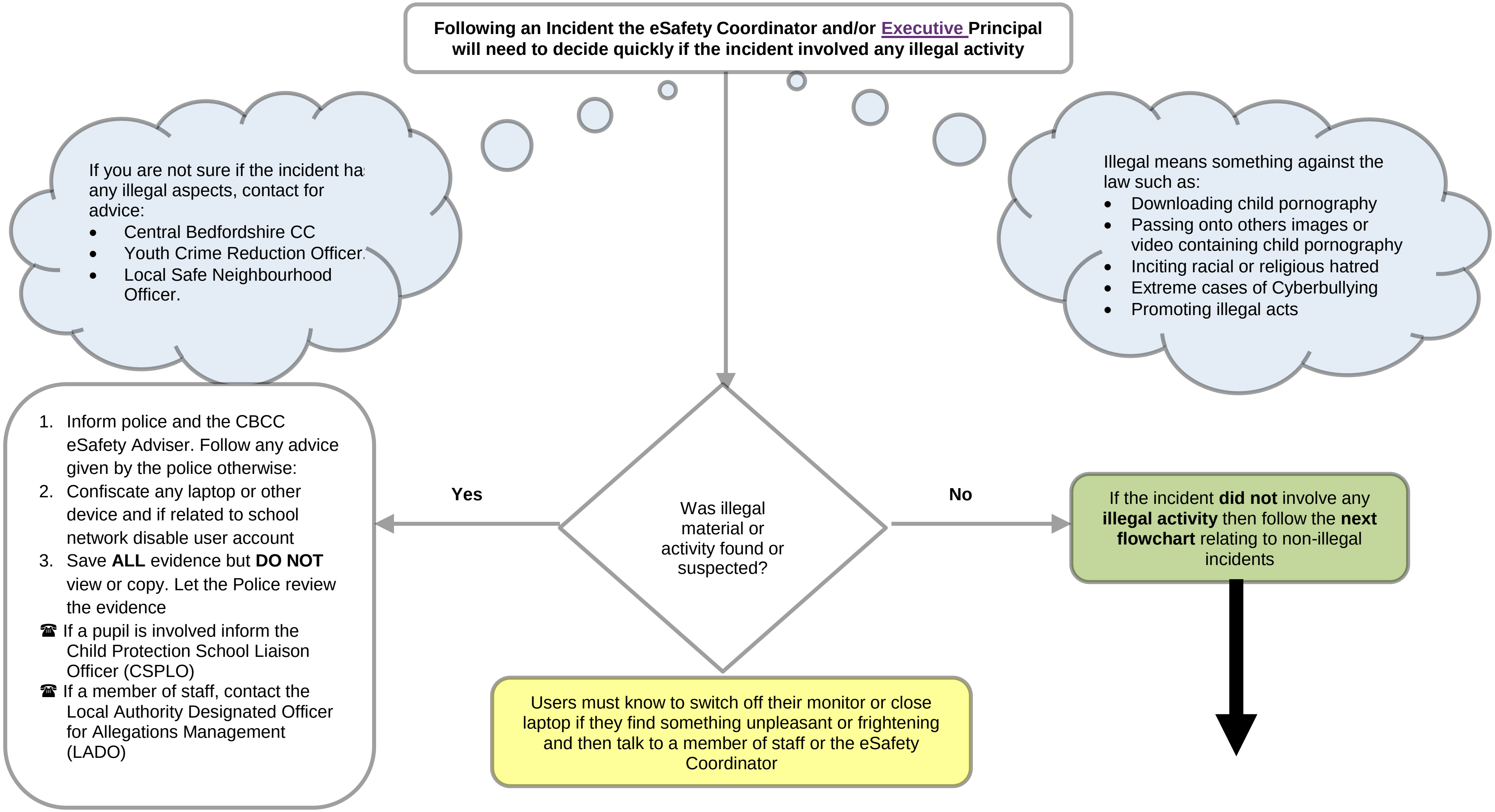
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Executive Principal. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal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

- Users are made aware of sanctions relating to the misuse or misconduct by the Academy Conduct Policy

“Love your neighbor as yourself. There is no commandment greater than this.”
Mark Chapter 12: Verse 31

Flowchart for Managing eSafety Incidents

Flowchart to support decisions related to an illegal eSafety Incident



Following an Incident the eSafety Coordinator and/or Executive Principal will need to decide quickly if the incident involved any illegal activity

If you are not sure if the incident ha any illegal aspects, contact for advice:

- Central Bedfordshire CC
- Youth Crime Reduction Officer.
- Local Safe Neighbourhood Officer.

Illegal means something against the law such as:

- Downloading child pornography
- Passing onto others images or video containing child pornography
- Inciting racial or religious hatred
- Extreme cases of Cyberbullying
- Promoting illegal acts

Was illegal material or activity found or suspected?

Yes

1. Inform police and the CBCC eSafety Adviser. Follow any advice given by the police otherwise:
2. Confiscate any laptop or other device and if related to school network disable user account
3. Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence

☎ If a pupil is involved inform the Child Protection School Liaison Officer (CSPLO)

☎ If a member of staff, contact the Local Authority Designated Officer for Allegations Management (LADO)

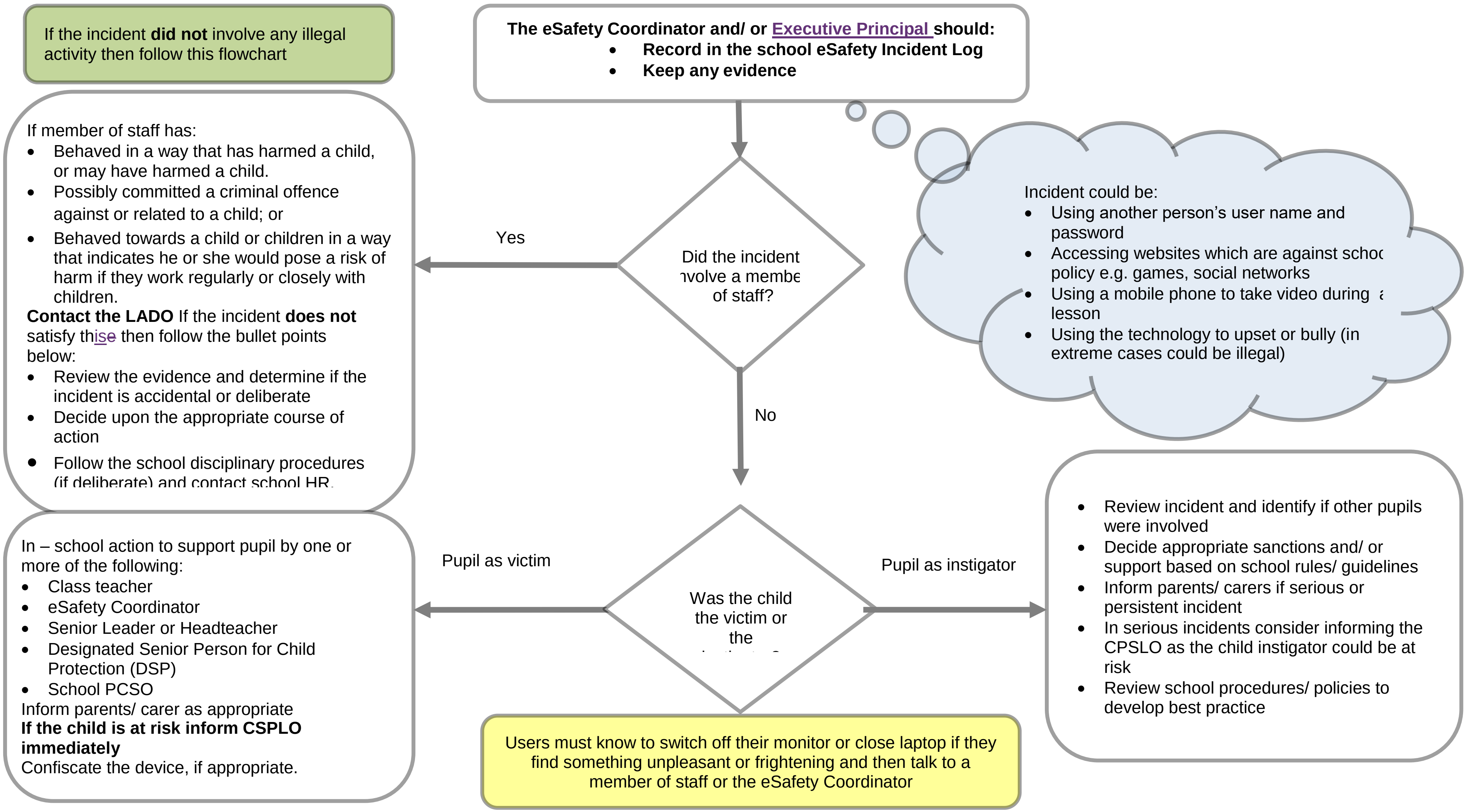
No

If the incident **did not** involve any **illegal activity** then follow the **next flowchart** relating to non-illegal incidents

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator

“Love your neighbor as yourself. There is no commandment greater than this.”
Mark Chapter 12: Verse 31

Managing an eSafety Incident



If the incident **did not** involve any illegal activity then follow this flowchart

The eSafety Coordinator and/ or Executive Principal should:

- **Record in the school eSafety Incident Log**
- **Keep any evidence**

Incident could be:

- Using another person’s user name and password
- Accessing websites which are against schoo policy e.g. games, social networks
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully (in extreme cases could be illegal)

Did the incident ɿvolve a membe of staff?

Yes

If member of staff has:

- Behaved in a way that has harmed a child, or may have harmed a child.
- Possibly committed a criminal offence against or related to a child; or
- Behaved towards a child or children in a way that indicates he or she would pose a risk of harm if they work regularly or closely with children.

Contact the LADO If the incident **does not** satisfy thi~~se~~ then follow the bullet points below:

- Review the evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow the school disciplinary procedures (if deliberate) and contact school HR.

No

Was the child the victim or the

Pupil as victim

In – school action to support pupil by one or more of the following:

- Class teacher
- eSafety Coordinator
- Senior Leader or Headteacher
- Designated Senior Person for Child Protection (DSP)
- School PCSO

Inform parents/ carer as appropriate
If the child is at risk inform CSPLO immediately
Confiscate the device, if appropriate.

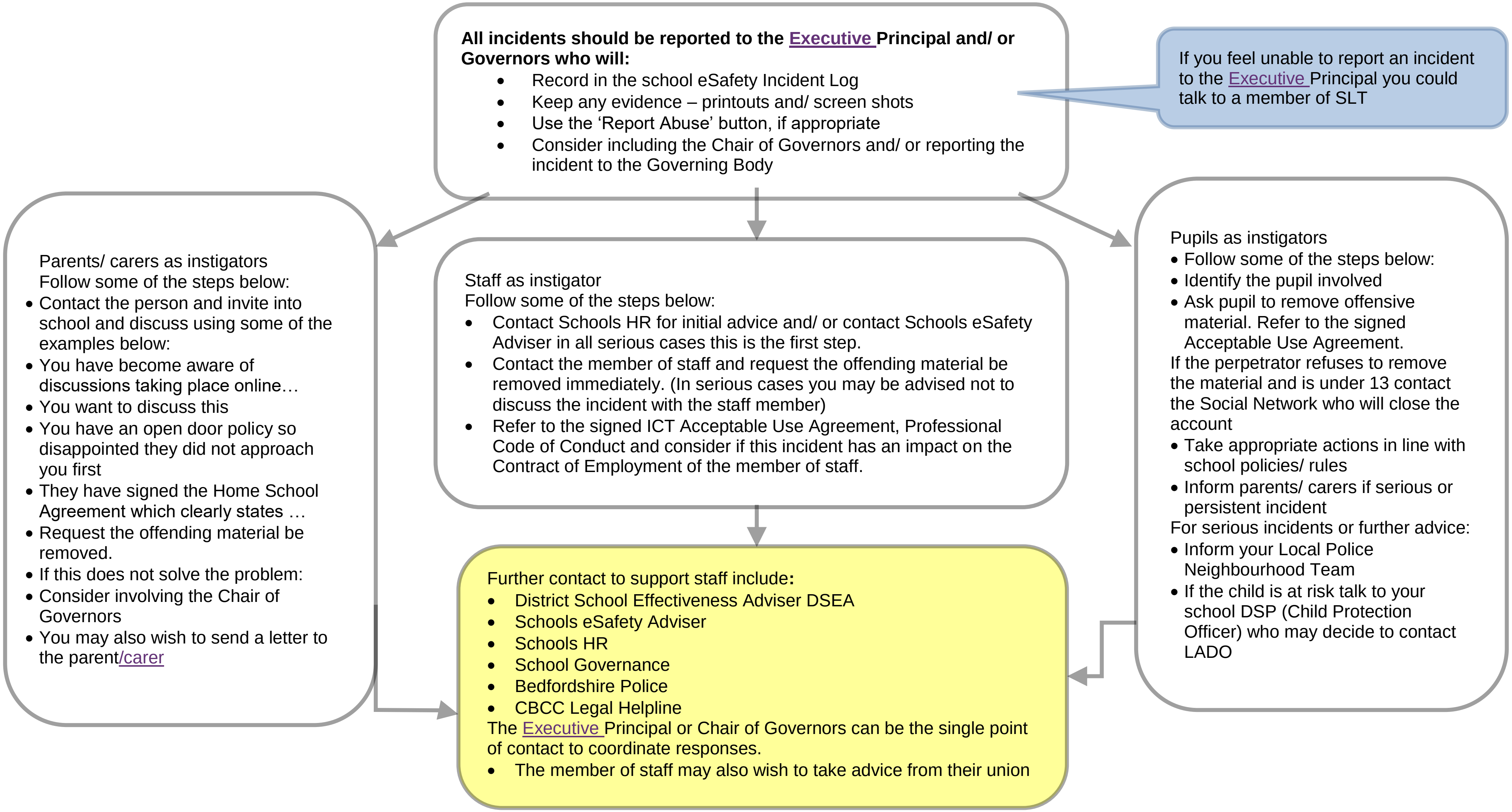
Pupil as instigator

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions and/ or support based on school rules/ guidelines
- Inform parents/ carers if serious or persistent incident
- In serious incidents consider informing the CPSLO as the child instigator could be at risk
- Review school procedures/ policies to develop best practice

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator

“Love your neighbor as yourself. There is no commandment greater than this.”
Mark Chapter 12: Verse 31

Managing an eSafety Incident involving staff as victims



All incidents should be reported to the Executive Principal and/ or Governors who will:

- Record in the school eSafety Incident Log
- Keep any evidence – printouts and/ screen shots
- Use the ‘Report Abuse’ button, if appropriate
- Consider including the Chair of Governors and/ or reporting the incident to the Governing Body

If you feel unable to report an incident to the Executive Principal you could talk to a member of SLT

Parents/ carers as instigators
Follow some of the steps below:

- Contact the person and invite into school and discuss using some of the examples below:
- You have become aware of discussions taking place online…
- You want to discuss this
- You have an open door policy so disappointed they did not approach you first
- They have signed the Home School Agreement which clearly states …
- Request the offending material be removed.
- If this does not solve the problem:
- Consider involving the Chair of Governors
- You may also wish to send a letter to the parent/carer

Staff as instigator
Follow some of the steps below:

- Contact Schools HR for initial advice and/ or contact Schools eSafety Adviser in all serious cases this is the first step.
- Contact the member of staff and request the offending material be removed immediately. (In serious cases you may be advised not to discuss the incident with the staff member)
- Refer to the signed ICT Acceptable Use Agreement, Professional Code of Conduct and consider if this incident has an impact on the Contract of Employment of the member of staff.

Pupils as instigators

- Follow some of the steps below:
- Identify the pupil involved
- Ask pupil to remove offensive material. Refer to the signed Acceptable Use Agreement.

If the perpetrator refuses to remove the material and is under 13 contact the Social Network who will close the account

- Take appropriate actions in line with school policies/ rules
- Inform parents/ carers if serious or persistent incident

For serious incidents or further advice:

- Inform your Local Police Neighbourhood Team
- If the child is at risk talk to your school DSP (Child Protection Officer) who may decide to contact LADO

Further contact to support staff include**:**

- District School Effectiveness Adviser DSEA
- Schools eSafety Adviser
- Schools HR
- School Governance
- Bedfordshire Police
- CBCC Legal Helpline

The Executive Principal or Chair of Governors can be the single point of contact to coordinate responses.

- The member of staff may also wish to take advice from their union

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 Academy network is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The Academy provides pupils with 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 discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents/carers recheck these sites and supervise this work. Parents/carers will be advised to supervise any further research
- 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 gaming is not allowed
- It is at the Executive Principal’s discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- The Academy also employs web-filtering which is the responsibility of the Network Manager
- All Saints Academy is aware of its responsibility when monitoring staff communication under current legislation and takes into account; GDPR, 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 can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- The Academy uses management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- 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 Academy’s responsibility nor the Network Manager’s to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the IT Team for a safety check first
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from Network Manager/Technician.
- If there are any issues related to viruses or anti-virus software, the Network Manager should be informed via email.

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.

- At present, the Academy 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 Academy
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Executive Principal
- When signing up to online services that require the uploading of what could be deemed as **personal or sensitive data**, schools should check terms and conditions regarding the location of storage. All transfers should be compliant with the guidance on ico. at: International data transfer agreement and guidance | ICO
- Services such as Facebook, Instagram and Tik Tok have a 13+ age rating which should not be ignored

Parental involvement

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

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy.
- Parents/carers are asked to read through and sign acceptable use agreements 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 (e.g., on school website)

- Parents/carers are expected to sign a Home School agreement containing the following statement(s)

    - **I/we will support the school approach to online safety and not upload or add any text, image, sound or videos that could upset or offend any member of the school community, or bring the school name into disrepute.**

    - **I/we will ensure that my/our online activity would not cause the school, staff, pupils or others distress or bring the school community into disrepute.**

    - **I/we will support the school’s policy and help prevent my/our child/children from signing up to services such as Facebook, Instagram, Snapchat and YouTube whilst they are underage (13+ years in most cases).**

    - **I/we will close online accounts if I/we/teachers find that these accounts are active for our underage child/children.**

- The school disseminates information to parents/carers relating to eSafety where appropriate in the form of;

    - Information evenings
    - Practical training sessions e.g. current eSafety issues
    - Posters
    - School website information
    - Newsletter items

Passwords and password security

Passwords

- **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
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on 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 Network Manager immediately**
- Passwords must contain a minimum of six characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and pupils who have left the school are removed from the system within two months.

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team.

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

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school’s e-Safety Policy and Data Security
- Users are provided with an individual network, email, learning platform and Management Information System log-in username. From Year 7 they are also expected to use a personal password and keep it private
- Pupils are not permitted to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network applies for students and is at 16:30, but computers will lock after 10 minutes of inactivity. Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer)
- In the Academy, all ICT password policies are the responsibility of the Network Manager and all staff and pupils are expected to comply with the policies at all times

Zombie Accounts

Zombie accounts refers to accounts belonging to all users who have left the school and therefore no longer have authorised access to the school’s systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorised access
- Regularly change generic passwords to avoid unauthorised access

Personal or sensitive information

Protecting Personal or Sensitive 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
- Ensure the accuracy of any personal or sensitive 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 or sensitive 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 your manager
- You must not post on the internet personal or sensitive 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 document labeling

Storing/Transferring Personal or Sensitive Information Using Removable Media

- Ensure removable media is purchased with encryption or any data stored on a non-encrypted device is itself encrypted.

- Store all removable media securely

- Securely dispose of removable media that may hold personal data

- Staff are strongly discouraged from using removable media to transfer data and, where this is the only option, a password protected zip file must be used. USB storage is disabled on student laptops.

- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Remote access

- 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 Academy systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone

- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers

- 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 Academy 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/carers (on behalf of pupils) and staff, the Academy 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 Executive Principal, images can be taken provided they are transferred immediately and solely to the Academy's network and deleted from the staff device

- Pupils are not permitted to use personal digital equipment (including mobile phones and cameras) or their Academy iPads to record images/videos of pupils, staff and others without advance permission from the Executive Principal

- Pupils and staff must have permission from the Executive Principal before any image can be uploaded for publication

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
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the school's learning platform or Virtual Learning Environment
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. 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, e.g. 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 and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Network Manager and IT Technician has authority to upload to the internet.

Storage of Images

- Images/ films of children are only stored on the Academy’s network. Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Executive Principal
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource
- The Network Manager has the responsibility of deleting the images when they are no longer required, or when the pupil has left the school

Webcams and Surveillance Cameras

- The school uses surveillance cameras for security and safety. The only people with access to this are **SLT and HOYs.** Notification of camera use is displayed at the front of the school. Please refer to the ICO website for further information.
- We do not use publicly accessible webcams in school
- Webcams will not be used for broadcast on the internet without prior parental consent
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ‘ inappropriate materials’ section of this document)
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images
- Webcams include any camera on an electronic device which is capable of producing video. ~~School~~ Academy policy should be followed regarding the use of such personal devices

Video Conferencing

- 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 Executive Principal is sought prior to all video conferences within school to end-points beyond the school
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

Academy ICT equipment including portable & mobile ICT equipment & removable media

Academy ICT Equipment

- As a user of the Academy ICT equipment, you are responsible for your activity
- The Academy logs ICT equipment issued to staff and records serial numbers as part of the school’s asset register
- Do not allow your visitors to plug their ICT hardware into the Academy 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
- 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 Academy’s network. You are responsible for the backup and restoration of any of your data that is not held on the Academy’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
- It is recommended that 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 Academy network
- On termination of employment, resignation or transfer, return all ICT equipment to the Network 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 appropriate Line Manager. Authorising Managers are responsible for:
    - maintaining control of the allocation and transfer within their unit
    - 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 GDPR

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 Academy systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all Academy data is stored on the Academy 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 Academy 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 Smartphones, iPads, games players, 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. All students in KS3 and KS4 are issued with an iPad to aid with learning. This will be managed by the Academy meaning that only the Network Manager will be able to download Apps and only with the permission of the Executive Principal.

Personal Mobile Devices (including phones)

- The Academy allows staff to bring in personal mobile phones and devices for their own use. If, due to an exceptional circumstance, a member of staff has to contact a parent/carer on a personal device they must block their number.
- Pupils are allowed to bring personal mobile devices/phones to school but must not use them within the Academy. At all times the device must be switched onto silent and placed into a Yondr pouch. If a student does not have a Yondr pouch, the phone must be handed in.
- The Academy is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the Academy community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the Academy community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

Telephone services

- You may make or receive personal telephone calls in designated places, provided:

    1. They are infrequent, kept as brief as possible and do not cause annoyance to others
    2. They are not for profit or to premium rate services
    3. They conform to this and other relevant HCC and Academy policies.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- Ensure that you are available to take any pre-planned incoming telephone calls

- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask the Academy Services Manager

Removable Media

If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section '**Storing/Transferring Personal or Sensitive Information Using Removable Media**'

- Always consider if an alternative solution already exists
- Only use recommended removable media
- Encrypt and password protect
- Store all removable media securely
- Removable media must be disposed of securely by the ICT support team

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
- Backup tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Backup tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure
- Newly installed Office Master PCs acting as servers and holding personal data should be encrypted, therefore password protecting data.

Social media, including Facebook and Twitter

- The Academy uses Twitter to communicate with parents and carers. The Senior Leadership 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 Academy equipment ***during school hours***
- 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 whilst at school
- Pupils in **Years 12 and 13** are permitted to access their personal social media account using their own device (i.e. mobile phone) outside of lessons
- 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 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 aware that their online behaviour should at all times be compatible with UK law

SMILE AND STAY SAFE POSTER

eSafety guidelines to be displayed throughout the Academy

SMILE **and stay safe**

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)
Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you
Information online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'
Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply

Systems and access

- You are responsible for all activity on Academy systems carried out under any access/account rights assigned to you, whether accessed via Academy ICT equipment or your own PC
- Do not allow any unauthorised person to use Academy 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 Academy ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the Academy or may bring the Academy 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 Academy systems, hardware or used in relation to Academy 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 a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

Writing and reviewing this policy
Staff and Pupil Involvement in Policy Creation

- Staff, governors and pupils have had the Policy for ICT Acceptable Use shared with them through *assemblies, tutor periods and meetings.*

Review Procedure
There will be on-going opportunities for staff to discuss with the eSafety coordinator any eSafety issue that concerns them
There will be on-going opportunities for staff to discuss with a member of SLT any issue of data security that concerns them
This policy will be reviewed every 2 years 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

Further help and support

For more information visit the website of the Information Commissioner's Office https://ico.org.uk/

Test your online safety skills http://www.getsafeonline.org

Information Commissioner's Office – www.ico.org.uk

“Love your neighbor as yourself. There is no commandment greater than this.”
Mark Chapter 12: Verse 31

Cloud (Educational Apps) Software Services and the Data Protection Act – Departmental advice for local authorities, school leaders, school staff and governing bodies, October 2015. This is an advice and information document issued by the Department for Education. The advice is non-statutory, and has been produced to help recipients understand some of the key principles and their obligations and duties in relation to the Data Protection Act 1998 (the DPA), particularly when considering moving some or all of their software services to internet-based “cloud” service provision –
https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

Current legislation

Acts Relating to Monitoring of Staff email

General Data Protection Regulation 2018
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.
https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

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 eSafety

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)

“Love your neighbor as yourself. There is no commandment greater than this.”
Mark Chapter 12: Verse 31

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 (email) 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 the 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 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.

Relating to the Protection of Personal Data

"Love your neighbor as yourself. There is no commandment greater than this."
Mark Chapter 12: Verse 31

General Data Protection Regulation 2018
https://www.gov.uk/government/publications/data-protection-toolkit-for-schools
The Freedom of Information Act 2000
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/
Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance
https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services

APPENDIX 1: Acceptable Use Agreement: Pupils

To ensure the safety and security of everyone at the Academy, all staff and students must agree to the IT Acceptable Use Policy

Equipment

- Never attempt to install or store programs of any type on the computers
- All maintenance should be carried out by IT support staff
- Do not eat or drink in the vicinity of the IT equipment or in IT suites
- Turn off any equipment when you have finished using it, unless you are instructed otherwise by a member of staff

Security and Privacy

- Protect your work by keeping your password to yourself; never share a logon name/password
- If you find that another user has forgotten to log off, inform a member of staff
- To protect yourself and the systems, you should respect the security on the computers.
- Your files and communications will be monitored to ensure that you are using the system responsibly
- Do not use your Academy email address to sign up to sites, mailing lists, etc, unless instructed to do so by a member of staff
- Report any suspicious looking emails to a member of staff immediately so that they can inform IT Support

Email

- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The sending of an email containing content likely to be unsuitable for young people or Academies is strictly forbidden
- The *@asadunstable.org* account provided by IT support should be used for all communications with Academy staff and for communicating with other students for Academy work purposes
- Webmail, such as Hotmail, should not be used at all in the Academy
- The use of email for bullying will be investigated and dealt with in accordance with the Academy Bullying Policy

Licences

- All Software, Music, Images, Videos MUST have a licence that covers use in the Academy
- A copy of this must be given to the Network Manager
- No iTunes or other music, files, images can be attached to the Academy network at any time unless a licence can be produced

Internet

Users shall not visit unsuitable Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- any other information which may be offensive to other users in the Academy community

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the police:

- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative

- adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material in the UK

If inappropriate material is accessed accidentally, users should immediately report this to the Network Manager so that this can be taken into account in monitoring.

Users shall not:

- Use the All Saints Academy facilities for running a private business
- Enter into any personal transaction that involves All Saints Academy or the Local Authority in any way
- Visit sites that might be defamatory or incur liability on the part of All Saints Academy or the Local Authority or adversely impact on the image of All Saints Academy
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of All Saints Academy, or to All Saints Academy itself
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
    - financial information
    - personal information
    - databases and the information contained therein
    - computer/network access codes
    - business relationships
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet

Monitoring

- The Academy reserves the right to monitor electronically all activity on its network and any device attached to it. This includes computers, laptops, flash drives, MP3s etc, whether they belong to the Academy or not

Please read this document carefully. If you violate these provisions you may be subject to disciplinary action. Additional action may be taken by the Academy.

I agree to the full Terms & Conditions as clearly depicted in the ***E-Learning, E-Safety and ICT for Learning Policy*** and specifically in relation to pages 14 through to 18 which can be viewed on the Academy’s website.

APPENDIX 2: Acceptable use Agreement: Staff, Governors & Visitors

Acceptable Use Agreement: Staff, Governors and Visitors

The Academy has provided IT facilities for your use, offering access to a vast amount of information & Resources for use in your role at the academy.
The IT facilities are provided and maintained for the benefit of the entire Academy community, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all.
You are responsible for good behaviour with the resources and on the Internet, just as you are with any other Academy equipment.
I understand that using the computer network is a privilege and that when using the Academy computers I will:

- Always behave in a sensible manner, respecting others at all times
- Only log on using my own username and keep my password secret
- Report any suspected breach of network security (whether by myself or others) to my line manager or IT support.
- Refrain from accessing any newsgroups, links, web pages or other areas of cyberspace that would be considered offensive because of pornographic, racist, violent, illegal or illicit content
- Never use my Academy email address to sign up to social networking sites such as Facebook, Twitter etc.
- Never harass or abuse other members of staff or students through the use of obscene or offensive language or images, either on the Academy network itself or via external social networking sites, and will report any cases of such usage against me
- Only use the Academy computer network for Academy-related work
- Use email for appropriate educational purposes only
- Not attempt to access banned sites through the use of proxy websites or seek other ways of avoiding the Academy internet filtering system.
- Never use Mobile Internet devices in the Academy to access the internet or email without the permission of the IT Support Department and then only to connect to the specific Wi-Fi access directed by the IT Support Department
- Always be courteous and use appropriate language both to those around me and those I contact through the network
- Not allow copyrighted material to enter the Academy network e.g. MP3 files, videos etc.
- Not download software, games, music, graphics or videos without first checking copyright and asking my line manager
- Use any downloaded material in an appropriate manner in my work
- Never reveal personal information including names, addresses, credit card details, telephone or fax numbers and photographs of myself or others

- Never subscribe to auto-mailing systems
- Only use the Academy address where I have permission and will never give other details about the Academy, including telephone numbers
- Not interfere with, damage or in any other manner compromise the Academy computers or peripherals, Academy systems or network
- Report any accidental damage immediately to a member of IT Support
- Report any misuse of the Internet or email to a member of IT Support or your line manager

Declaration:

In signing the below I acknowledge that I will abide by the requirements set out.
Any usage of the Academy IT equipment or facilities, including email, website access, use of software etc. can and will be monitored and/or recorded by the IT Support Department, details of which will be made available to both the Academy and, in serious cases, external law enforcement agencies.
The Academy has the right to remove any material from Academy computers that is deemed inappropriate or not in keeping with our educational mission. The Academy administration and Governing Body are solely responsible for deciding what constitutes appropriate use and what defines acceptable content.
Due to the unregulated and ever changing nature of the Internet, we assume no liability for any damages a user may incur as a result of inappropriate Internet access.
I am responsible for data protection and will not store any sensitive information on the device which could breach the Data Protection Act if the device is stolen or lost.

Name ______________________________________
Signature ______________________________________ Date ______________________