Clifton All Saints Academy

ACCEPTABLE USE AND E-SAFETY POLICY

Version date: November 2020

Review date: September 2021

CONTENTS PAGE

DEFINITIONS

The following terms shall have the following meanings for the purposes of this document:

the School	means Clifton All Saints Academy
the Act	means the Data Protection Act 2018
the ICT Support Provider	means DWM Technical Solutions Ltd
E-safety Coordinator	means the Headteacher of the School
Information Asset Owner	means the Headteacher of the School
Network Manager	means DWM Technical Solutions Ltd
Relevant Responsible Person	means the Headteacher or the Business Manager
CBICS	means Central Bedfordshire Internet Connectivity Service
CEOP	means Child Exploitation and Online Protection
ICT	means Information and Communications Technology
MIS	means Management Information System(s)
PAT	means Portable Appliance Testing
PSHCE	means Personal, social, health and citizenship education

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 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 **the School** we understand the responsibility to educate our pupils on E-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.

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 the School to use technology to benefit learners.

Everybody in the School 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 and pupils) are inclusive of both fixed and mobile internet; technologies provided by the School (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto the School premises (such as laptops, mobile phones and other mobile devices).

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.

For staff, any policy breach is grounds for disciplinary action in accordance with the School's 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 6th 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;

For pupils, reference will be made to 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 (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 Persons in the School are as follows: the Headteacher, the School Business Manager.

ACCEPTABLE USE AGREEMENT: PUPILS -PRIMARY

Primary Pupil Acceptable Use Agreement / E-safety Rules

- I will only use ICT in School for school purposes
- I will only use my class e-mail address or the School e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the School approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the School community.
- I know that my use of ICT can be checked and my parent/carer contacted if a member of the School's staff is concerned about my safety.
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher.
- I will not bring a Smart Watch to School because I am not allowed to wear one during the School day.
- I will not sign up to online services until I am old enough.

CLIFTON ALL SAINTS ACADEMY

Dear Parent/Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning in the School. The School expects all children to be safe and responsible when using any ICT.

Please read and discuss these E-safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact the Headteacher.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

Yours faithfully

Carol Ward
Headteacher

✂---

PARENT/CARER SIGNATURE

We have discussed this document with ……………………………………........ (child's name) and we agree to follow the E-safety rules and to support the safe use of ICT at the School.

Parent/ Carer Signature ……………………………………………………………………………………………………….

Class …………………………………………………………………………. Date ……………………………………………………………

ACCEPTABLE USE AGREEMENT: - STAFF, GOVERNORS AND VISITORS

Staff, Governor and Visitor -Acceptable Use Agreement/Code of Conduct

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 sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the School.

- I will only use the School's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Headteacher 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, personal Twitter account, or any other social media link, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS 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 Headteacher or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with the School's policy and with written consent of the parent, carer or staff member.
- 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 upload or add any images, video, sounds or text linked to or associated with the School or its 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 activity, both in School and outside school, will not bring the School, my professional reputation, or that of others, into disrepute.
- I will support and promote the School's e-Safety and Data Security Policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will not use personal electronic devices (including smart watches) in public areas of the School between the hours of 8.30am and 3.30pm, except in the staff room and where there are signs to indicate this.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the School

Signature …… Date ……

Full Name …….. (printed)

Job title ……

STAFF PROFESSIONAL RESPONSIBILITIES

PROFESSIONAL RESPONSIBILITIES

When using any form of ICT, including the Internet, in school and outside school

For your own protection we advise that you:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.
- Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, **both in school and outside school**, will not bring your organisation or professional role into disrepute.

You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

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 the School's provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on the 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 of the School's 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 accessing and appropriate use of the School data is something that the School 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 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, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used.
- Anyone sending a confidential or sensitive fax should notify the recipient before it is sent.

PROTECTIVE MARKING OF OFFICIAL INFORMATION

Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them, in line with local business processes.

- There is no requirement to mark routine OFFICIAL information.
- Optional descriptors can be used to distinguish specific type of information.
- Use of descriptors is at an organisation's discretion.
- Existing information does not need to be remarked.

In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE'**

RELEVANT RESPONSIBLE PERSONS

Senior members of staff should be familiar with information risks and the School's response:

- they lead on the information risk policy and risk assessment;
- they advise School staff on appropriate use of School technology;
- they act as an advocate for information risk management.

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.

INFORMATION ASSET OWNER (IAO)

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. A responsible member of staff 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.

As a result, this manager is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

However, it should be clear to all staff that the handling of secured 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 over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. The School 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 2018
  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 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

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

T***he Waste Electrical and Electronic Equipment Regulations 200***6
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/

Data Protection Act – data protection guide, including the 8 principles
https://ico.org.uk/for-organisations/education/

PC Disposal – SITSS Information
http://www.thegrid.org.uk/info/traded/sitss/services/computer_management/pc_disposal

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 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. The School recognises that pupils need to understand how to style an e-mail in relation to their age and how to behave responsible online.

MANAGING E-MAIL

- The School gives all staff 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 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 or conduct any School business using personal e-mail addresses.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on School headed paper.
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher.
- Pupils may only use School approved accounts on the School system and only under direct teacher supervision for educational purposes.
- 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
  - Delete all e-mails of short-term value.
  - Organise e-mail into folders and carry out frequent housekeeping on all folders and archives.

- All pupil e-mail 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 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.
- Staff must inform the E-safety Coordinator (the Headteacher) if they receive an offensive e-mail.
- Pupils are introduced to e-mail as part of the Computing Programme of Study.
- However, you access your School e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the School e-mail policies apply.

SENDING E-MAILS

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section .
-
- E-MAILING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION.
- Use your own School e-mail account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of e-mail 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 e-mail is not to be used for personal advertising.

RECEIVING E-MAILS

- Check your e-mail regularly.
- Never open attachments from an untrusted source; consult your Network Manager first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- The automatic forwarding and deletion of e-mails is not allowed.

E-MAILING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION

- Where your conclusion is that e-mail must be used to transmit such data:
    - Obtain express consent from your 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:
    - 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.

- Confidential governor communication is carried out via the secure area of the Governor Portal.
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone).
- 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 E-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 E-safety issues.

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

E-SAFETY

E-SAFETY - ROLES AND RESPONSIBILITIES

As E-safety is an important aspect of strategic leadership within the School, the Headteacher and the Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-safety Co-ordinator in the School is the Headteacher 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 E-safety Co-ordinator to keep abreast of current issues and guidance through organisations such as Central Beds LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Headteacher/ E-safety co-ordinator and all Governors have an understanding of the issues and strategies at the School in relation to local and national guidelines and advice.

This policy, supported by the School'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) policy and PSHCE.

E-SAFETY IN THE CURRICULUM

ICT and online resources are increasingly used across the curriculum. The School believes it is essential for E-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within the curriculum and the School continually look for new opportunities to promote E-safety.

- The School has a framework for teaching internet skills in Computing lessons and across the Curriculum as appropriate.
- The School provides opportunities within a range of curriculum areas to teach about E-safety..
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the E-safety curriculum.
- 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 Cyber mentors, Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through the cross curricular teacher models, discussions and via the Computing curriculum.

E-SAFETY SKILLS DEVELOPMENT FOR STAFF

- The School staff receive regular information and training on E-safety and how they can promote the 'Stay Safe' online messages.
- 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 E-safety and know what to do in the event of misuse of technology by any member of the School community (see E-safety Coordinator).
- All staff are encouraged to incorporate E-safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

MANAGING THE SCHOOL E-SAFETY MESSAGES

- The School endeavour to embed E-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The E-safety policy will be introduced to the pupils at the start of each school year.
- E-safety posters will be prominently displayed.

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 E-safety 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.

MISUSE AND INFRINGEMENTS

Complaints

Complaints and/or issues relating to E-safety should be made to the E-safety Co-ordinator or Headteacher. Incidents should be logged and the **Academy Flowcharts for Managing an E-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 E-Safety 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 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 by staff meetings.

Clifton All Saints Academy Flowchart to support decisions related to an illegal E-Safety Incident
For Headteachers, Senior Leaders and E-Safety Coordinators

Following an Incident the E-Safety Coordinator and/or Headteacher will need to decide quickly if the incident

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

- Bedfordshire Police
- 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 Beds E-safety Adviser (above). 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

☎ 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 E-safety Coordinator

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

Clifton All Saints Academy
Managing an E-safety Incident Flowchart
For Headteachers, Senior Leaders and E-safety Coordinators

The E-safety Coordinator and/ or Headteacher should:

- **Record in the school E-safety Incident Log**
- **Keep any evidence**

Did the incident involve a member 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 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

Incident could be:

- Using another person's user name and password
- Accessing websites which are against school 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)

No

Was the child the victim or the instigator?

Pupil as victim

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

- Class teacher
- E-safety Coordinator
- Senior Leader or Headteacher
- Designated Safeguarding Lead

Inform parents/ carer as appropriate

If the child is at risk inform DSL 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 DSL 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 E-safety Coordinator

Clifton All Saints Academy
Managing an E-safety Incident Flowchart involving staff as victims
For Headteachers, Senior Leaders and E-safety Coordinators

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

- Record in the school E-safety 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 your HT 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

Staff as instigator
Follow some of the steps below:

- Contact Schools HR for initial advice and/ or contact Schools E-safety 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
- Anti-Bullying Adviser
- If the child is at risk talk to your school DSL (Child Protection Officer) who may decide to contact LADO

Further contact to support staff include**:**

- Schools E-safety Adviser
- Schools HR
- School Governance
- Bedfordshire Police

The HT 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 CBICS 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 School 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 recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute the 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 Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

INFRASTRUCTURE

- School internet access is controlled through the School's Broadband web filtering service.
- The School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018, 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 School 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 School's responsibility to install or maintain virus protection on personal systems.
- Pupils are not permitted to download programs or files on School based technologies.
- If there are any issues related to viruses or anti-virus software, the Network Manager should be informed.

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, the School encourages its 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 School endeavours 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).
- The School's 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.
- 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 the School learning platform or other systems approved by the Headteacher.
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm.

PARENTAL INVOLVEMENT

The School believes that it is essential for parents/carers to be fully involved with promoting E-safety both in and outside of school and to be aware of their responsibilities. The School regularly promote E-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 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 the School website).
- Parents/carers are expected to sign a Home School agreement containing the following statement(s):

AS A PARENT/CARER I AGREE TO*:*

→ **Make sure my child attends regularly, arrives on time and is properly equipped for the day.**

→ **Phone the School if my child is late or absent, on each day of absence, prior to 9.30am.**

→ **Let the School know of any concerns or problems that might affect my child's work or behaviour.**

→ **Support the School's values, policies and guidelines for behaviour.**

→ **Support my child to complete his/her homework and ensure that it is done to the best of their ability and handed in on time.**

→ **Attend consultation evenings to support my child.**

→ The School disseminates information to parents relating to E-safety where appropriate through:

- Information evenings
- Practical training sessions e.g. current E-safety 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 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 the Headteacher immediately.**
- 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 3 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.
- Pupils are provided with a class log-in for use on the School system. From ***Year*** 4 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.
- 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).

ZOMBIE ACCOUNTS

Zombie accounts refers to accounts belonging to 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 unauthorized access.
- Regularly change generic passwords to avoid unauthorised access.

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.
- 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 copiers (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, 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 document labelling.

STORING/TRANSFERRING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION USING REMOVABLE MEDIA

- Ensure removable media is purchased with encryption.
- 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 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 the School 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 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 Headteacher, images can be taken provided they are transferred immediately and solely to the School's network and deleted from the staff device.
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication

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 the 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. E-mail 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 Headteacher or Business Manager has authority to upload to the internet.

STORAGE OF IMAGES

- Images/ films of children are stored on the School'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 Headteacher.
- 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 Business Manager has the responsibility of deleting the images when they are no longer required, or when the pupil has left the School.

WEBCAMS AND CCTV

- The School uses CCTV for security and safety. The only people with access to this are the Headteacher and the Business Manager. Notification of CCTV use is displayed at the front of the School.
- The School do not use publicly accessible webcams in the School.

SCHOOL ICT EQUIPMENT - INCLUDING PORTABLE AND MOBILE ICT EQUIPMENT AND REMOVABLE MEDIA

SCHOOL ICT EQUIPMENT

- As a user of the School ICT equipment, you are responsible for your activity.
- It is recommended that schools log ICT equipment issued to staff and record 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.
- 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 drive of desktop PCs, laptops, USB memory sticks 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 School's network.
- 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 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 Data Protection Act (DPA).

PORTABLE AND 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 the 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 Smartphones, Blackberries, 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. Emerging technologies will be examined for educational benefit and the risk assessed before use in School is allowed. The School chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

PERSONAL MOBILE DEVICES (INCLUDING PHONES)

- The School allows staff to bring in personal mobile phones and devices for their own use. However, they must not be used outside of the staff room or offices. Under no circumstances does the School allow a member of staff to contact a pupil or parent/carer using their personal device.
- The School 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 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.

- All visitors to the School must leave their mobile phone in the school office and are not permitted to have it on their person whilst in the School building unless it is an emergency situation, and it has been expressly agreed with the Headteacher beforehand.
- Parents visiting for the purpose of performances e.g. Christmas, Class Assembly, will be clearly reminded of their duty not to share photos on any Social Media sites.

SCHOOL PROVIDED MOBILE DEVICES (INCLUDING PHONES)

- 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, only this device may be used to conduct School business outside of School.
- Never use a hand-held mobile phone whilst driving a vehicle.

TELEPHONE SERVICES

- You may make or receive personal telephone calls 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.
- 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 your incoming telephone calls can be handled at all times.
- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout the School.

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

SMILE AND STAY SAFE POSTER

E-safety guidelines to be displayed throughout the School

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 my 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 (instant messaging) 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.

SOCIAL MEDIA - including Facebook and Twitter

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

- Staff *are not* permitted to access their personal social media accounts using the School equipment at any ***time.***
- Pupils are not permitted to access their social media accounts whilst at School.
- 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.

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 the School ICT equipment or your own PC.
- Do not allow any unauthorised person to use the 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 the 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 or LA 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 the 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. 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

REVIEW PROCEDURE

There will be on-going opportunities for staff to discuss with the E-safety Coordinator any E-safety issue that concerns them.

There will be on-going opportunities for staff to discuss with the Headteacher or Business Manager any issue of data security that concerns them.

This Policy will be reviewed every 12 months 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.

This Policy has been read, amended and approved by the staff, headteacher and governors on 18th November 2020

FURTHER HELP AND SUPPORT

The School has a legal obligation to protect sensitive information under the Data Protection Act 2018 and the General Data Protection Regulations 2018. For more information visit the website of the Information Commissioner's Office https://ico.org.uk/

School's toolkit is available - Record Management Society website – http://www.rms-gb.org.uk/resources/848

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

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

Cloud (Educational Apps) Software Services and the Data Protection Act – Departmental advice for local authorities, school leaders, school staff and governing bodies, October 2014. 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 2018 (the DPA), particularly when considering moving some or all of their software services to internet-based "cloud" service provision – https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/404098/Cloud-services-software-dept-advice-Feb_15.pdf

CURRENT LEGISLATION

ACTS RELATING TO MONITORING OF STAFF EMAIL

Data Protection Act 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.

http://www.hmso.gov.uk/acts/acts2018/19980029.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 (RIP)

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 the 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 E-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 Computer Misuse 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)

The Public Order Act 1986 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 2018

http://www.opsi.gov.uk/acts/acts2018/ukpga_19980029_en_1

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