E-Safety Policy

Reviewed June 2018

Approved by the Governing Body on

Contents

Description
1. E Safety Policy
a) Our Vision and Introduction
b) Ofsted key features of good and outstanding E-Safety practice
c) Creation, Monitoring and Review
d) Policy Scope
e) Roles and Responsibilities
f) Security
g) Risk Assessment
h) Behaviour Online
i) Communications
j) Use of Images and Video
k) Personal Information
l) Education and Training
m) Incidents and Response
2. Email Policy
a) Standards In Email Policy
b) Legal Risks
c) Legal Requirements
d) Best Practices
e) Personal Use
f) Confidential Information
g) System Monitoring
3. Website Policy
a) Aims
b) Procedures
4. Social Networking Policy
a) What is Social Media?
b) Personal Accounts
c) Professional Accounts
5. EYFS Mobile Phone & Camera Policy
a) Introduction
b) Aim
c) Scope
6. Review and consultation
7. Appendices

1. E Safety Policy

a. Our Vision and Introduction

St. Clement's C of E Academy embraces the positive impact and educational benefits that can be achieved through appropriate use of the internet and enhanced opportunities which new technologies offer to teaching and lifelong learning. We are also aware that inappropriate or misguided use can expose both adults and young people to potential risks and dangers, due to the instant accessibility and global nature of the internet and associated learning technologies.

Our approach is to implement appropriate safeguards within the academy while supporting and educating staff and pupils to identify and manage risks safely, through a combination of security measures, training and guidance. The E-Safety policy also includes the following associated sub policies: Email Policy, Social Networking Policy and Website Policy.

This E-Safety policy sets out the framework and expectations that all staff, pupils and the Academy community should adhere to in respect to the use of computing equipment, the internet and all forms of electronic communication such as email, mobile phones, intranets, social media sites and related learning technologies. It is designed to detail the principles all users should adhere to when using these services and should be used as a supporting framework in relation to E-Safety.

b. Ofsted key features of good and outstanding E-Safety practice

From Ofsted's perspective, E-Safety is a critical part of the inspection process. The table below details the key features found when good or outstanding E-Safety practice is in place.

Whole school consistent approach	All teaching and non-teaching staff can recognise and are aware of E-Safety issues. High quality leadership and management make E-Safety a priority across all areas of the Academy. A high priority given to training in E-Safety, extending expertise widely and building internal capacity. The contribution of pupils, parents and the wider school community is valued and integrated.
Robust and integrated reporting routines	Academy-based online reporting processes that are clearly understood by the whole Academy, allowing the pupils to report issues to nominated staff. On-going assemblies highlighting safety and safety procedures including who to approach if children are worried. Clear, signposted and respected routes to key members of staff. Effective use of peer mentoring and support. CPOMs reporting procedures followed.
Staff	All teaching and non-teaching staff receive regular and up-to-date training. At least one staff member has accredited training, for example CEOP, EPICT.

Policies	Rigorous E-Safety policies and procedures are in place, written in plain English, contributed to by the whole Academy, updated regularly and ratified by governors. The E-Safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying. The E-Safety policy should incorporate an Acceptable Usage Policy that is signed by pupils and/or parents as well as all staff and respected by all.
Education	A progressive curriculum that is flexible, relevant and engages pupils' interest; that is used to promote E-Safety through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. Positive rewards are used to cultivate positive and responsible use. Peer mentoring programmes.
Infrastructure	Recognised Internet Service Provider together with active filtering and monitoring.
Monitoring and Evaluation	Risk assessment taken seriously and used to good effect in promoting E-Safety. Using data effectively to assess the impact of E-Safety practice and how this informs strategy.
Management of Personal Data	The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 1998.

c. Creation, Monitoring and Review

The E-Safety Policy has been prepared with guidance from DofE Principles of E-Safety, JISC Legal, previous E-Safety Policies and advice and guidance from Professional Services and academy colleagues.
It is strongly recommended that an annual review of the E-Safety policy is carried out by a group in the academy that includes, the Designated Senior Lead, a senior leadership team representative, the Network Manager, pupils from the pupil council, a teaching staff representative, a support staff representative, a parent representative, a governor representative and a local community police officer.
The impact of this policy will be monitored regularly with a full review being carried out at least once a year. This policy will also be reconsidered where particular concerns are raised or where an E-Safety incident has been recorded.

d. Policy Scope

The E-Safety policy applies to all users, pupils, staff and all members of the academy community who have access to the Academy computing systems, both on the premises and remotely. Any user of the academy computing systems must adhere to and sign a hardcopy of the appropriate Computing Acceptable Use Agreement. The E-Safety Policy applies to all use of computing equipment (fixed and mobile), the internet and all forms of electronic communication such as email, mobile phones, portals/intranets and social media web sites.

e. Roles and Responsibilities

There are clear lines of responsibility for E-Safety within the academy. The first point of contact should be the E-Safety Officer. All staff are responsible for ensuring the safety of pupils and should report any concerns immediately to their line manager and the E-Safety Officer. All teaching staff are required to adhere to this incident reporting procedure.
When informed about an E-Safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved. All pupils must know what to do if they have E-Safety concerns and who to talk to. In most cases, this will be the E-Safety Officer or the Designated Senior Lead. Where any report of an E-Safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Designated Senior Lead may be asked to intervene with appropriate additional support from external agencies.

These are the roles and responsibilities that are in place in the academy and referred to in the E-Safety Policy:

E-Safety Officer:

The E-Safety Officer (reporting to the Safeguarding Designated Senior Lead) is responsible for keeping up to date with new technologies and their use, as well as attending any relevant training. He/She will be expected to lead the E-Safety agenda, review the E-Safety Policy, deliver staff development and training, manage the reporting procedure, record incidents, report any developments and liaise with external agencies to promote E-Safety within the academy community. He/she may also be required to deliver workshops for parents.

Pupils:

Pupils are responsible for using the Academy's Computing systems, mobile devices and learning technologies in accordance with our E-Safety Policy. Pupils must act safely and responsibly at all times when using the internet and/or mobile/learning technologies. They are responsible for attending E-Safety lessons as part of the curriculum and are expected to know and act in line with other relevant academy policies for example; mobile phone use, sharing images, and cyber-bullying. They must follow the reporting procedures where they are worried or concerned, or where they believe an E-Safety incident has taken place involving them or another member of the academy community.

Staff:

All staff are responsible for using the Academy's computing systems, mobile devices and learning technologies in accordance with the E-Safety Policy and the Staff E-Safety Charter which they must sign and submit to the E-Safety Officer. Staff must act safely and responsibly at all times when using the internet and/or mobile/learning technologies. Staff are responsible for attending training on E-Safety and displaying a model example to pupils at all times through embedded good practice.

All digital communications with pupils must be professional at all times and be carried out in line with our Email Policy. Online communication with pupils is restricted to academy provided systems. External platforms not hosted by the academy (for example social media sites) may only be used where a risk assessment has been completed by the member of staff and submitted to the E-Safety Officer and Head Teacher for approval. If approval is granted, then the Social Networking Policy must be adhered to.

All staff should adhere to the relevant academy policies detailed in the E-Safety Policy and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the E-Safety Officer or line manager without delay.

f. Security

The Academy will do all that it can to make sure the Academy's computing network and systems are safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and firewalls for servers, routers, and all academy provided user devices (desktop/laptop/tablet/mobile etc.) to prevent accidental or malicious access of academy systems and information.

g. Risk Assessment

In making use of new technologies and external online platforms, all staff must first carry out a risk assessment for E-Safety. This consists of a series of questions for the requestor to answer as well as a section in which they can record any relevant comments or evidence. A risk assessment must also be carried out where a pupil is learning off site e.g. on work placement. All forms must be submitted to the E-Safety Officer for consideration and approval.

h. Behaviour Online

Communication can take many forms, whether it is by email, text, webcam or instant chat. It is essential that all staff and pupils are aware of the academy policies that refer to acceptable behaviours when communicating online. The Academy will ensure that all users of technologies sign and adhere to the standard of behaviours set out in the Staff E-Safety Charter, and it will not tolerate any abuse of its Computing network, infrastructure or cloud based systems, whether offline or online. All communications by staff and pupils should be courteous and respectful at all times as detailed in the Email Policy. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes. Where conduct is found to be unacceptable, the academy will deal with the matter internally. Where conduct is considered to be illegal, the academy will report the matter to the police and other relevant external organisations as required / instructed.

i. Communications

The Academy requires all users of computing to adhere to the appropriate E-Safety charter which states clearly when email, mobile phones, social media sites, games consoles, chat rooms, video conferencing and web cameras may or may not be used during the academy day. Any required change or extension to these charters will require the permission of the Head Teacher with advice provided by the E-Safety Office.

j. Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or pupils.

All staff and pupils should receive training on the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe. Approved photographs should not include names of individuals without consent.

k. Personal Information

Personal information is information about a particular living person. The Academy collects and stores the personal information of staff and pupils regularly e.g. names, dates of birth, email addresses,

assessed materials and so on. The Academy will keep that information safe and secure and will not pass it onto anyone else without the express consent of the individual or pupils ' parent/carer as appropriate.

No personal information can be posted to the website. Only names and work email addresses of staff will appear on the academy website and no pupils' personal information will be available on the website without parental consent.

Staff must keep pupils personal information safe and secure at all times. When using any online or cloud platforms, all personal information must be password protected. No personal information of individuals is permitted off-site unless the member of staff has the written consent from that individual and the written permission of the Head Teacher.

l. Education and Training

With the current unlimited nature of internet access, it is impossible for the academy to eliminate all risks for staff and pupils. It is our view therefore, that the academy will ensure staff and pupils stay e-Safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

For pupils:

Pupils will attend E-Safety lessons with the first of these will taking place at the beginning of each new academic year, with follow up lessons carried out via the curriculum. Issues associated with E-Safety apply across the curriculum and pupils will receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies.

Pupils should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. A link to the academy E-Safety Policy will be available on the academy network and with the rules highlighted in posters and leaflets around Computing areas and classrooms. Within classes, pupils will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

For staff:

Staff will take part in mandatory annual E-Safety training. This will be led by or under the guidance of the E-Safety Officer. Further resources and useful guidance and information will be issued to all staff following the session. Each member of staff must record the date of the training attended.
Any new or temporary staff users will receive training on the Academy's computing network system and Google Apps for Education platform led by the E-Safety Officer. They will also be asked to sign our Staff E-Safety Charter.

m. Incidents and Response

Where an E-Safety incident is reported to the Academy this matter will be dealt with very seriously. The Academy will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a pupil wishes to report an incident, they can do so to their teacher or to the academy E-Safety Officer.

Where a member of staff wishes to report an incident, they must complete a CPOMs report and contact the DSLs as soon as possible. Following any incident, the Academy will review what has

happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. This is in line with the Staff E-Safety Charter.

Serious incidents will be dealt with by the SLT- Senior Leadership Team, in consultation with appropriate external agencies.

2. Email Policy

a. Standards in Email Policy

The purpose of this policy is to ensure the proper use of the St. Clement's C of E Academy email system and make users aware of what is deemed acceptable and unacceptable use. We reserve the right to amend this policy at our discretion, in which case users will be informed appropriately.

b. Legal Risks

Email is a business communication tool and users are obliged to use it in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of e-mail:

- If you send or forward emails with any libellous, defamatory, offensive, racist or obscene remarks, you and St. Clement's C of E Academy can be held liable.
- If you unlawfully email or forward confidential information, you and St. Clement's C of E Academy can be held liable.
- If you unlawfully forward or copy messages without permission, or you send an attachment that contains a virus, you and St. Clement's C of E Academy can be held liable.

By following the guidelines in this policy, the email user minimizes the legal risks involved in the use of e-mail. If any user disregards the rules set out in this Email Policy, the user will be fully liable and St. Clement's C of E Academy will disassociate itself from the user as far as legally possible.

c. Legal Requirements

The following rules are required by law and are to be strictly adhered to:

- It is strictly prohibited to send or forward emails containing libellous, defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify your line manager.
- Do not forward a message without acquiring permission from the sender first.
- Do not send unsolicited email messages.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person's email account unless this forms an essential part of your job role and has been agreed by the Head Teacher.
- Do not copy a message or attachment belonging to another user without permission of the originator.
- Do not disguise or attempt to disguise your identity when sending mail.

d. Best Practices

St. Clement's C of E Academy considers email (& messaging) as an important means of communication and recognises the importance of appropriate email content so users need to adhere to these guidelines:

Replying	When replying to a message sent to more than one person, be careful not to reply to all recipients of the original message by accident. Consider who needs to read your reply.

Evidential Record	Never forget that electronic conversations can produce an evidentiary record which is absent in a telephone conversation. Comments made by an employee during the course of an exchange of Emails could be used in support, or in defence, of the Academy's legal position in the event of a dispute.
Legal records	Computer generated information can now be used in evidence in the courts. Conversations conducted over the Email can result in legally binding contracts being put into place.
Forwarding Emails	Consideration should be given when forwarding Emails that it may contain information that you should consult with the originator before passing to someone else.

e. Personal Use

St. Clement's C of E Academy's email system is meant for business use only. We allow the reasonable use of personal email if certain guidelines are adhered to:

- Personal use should not interfere with work and must also adhere to the guidelines in this policy.
- The forwarding of chain letters, junk mail and executables is strictly forbidden.
- All messages distributed via the company's email system are St. Clement's C of E Academy's property, and are therefore subject to monitoring as with business emails.

f. Confidential Information

Avoid sending confidential information by email. Users should refer to the St. Clement's C of E Academy Data Security Policy with regards to sending confidential or personal information email.

g. System Monitoring

You must have no expectation of privacy in anything you create, store, send or receive on the Academy's computer system. Your emails can be monitored without prior notification if St. Clement's C of E Academy deems this necessary. If there is evidence that you are not adhering to the guidelines set out in this policy, St. Clement's C of E Academy reserves the right to take disciplinary action, including termination and/or legal action.

3. Website Policy

St. Clement's C of E Academy's website aims to share the learning journeys and achievements of all our pupils to all its stakeholders. It aims to raise the profile of the Academy in and beyond the local community.

a. Aims

The aims of this policy are to ensure that:

- The website complies with the St. Clement's C of E Academy, DfE and Ofsted statutory requirements.
- The website has up to date information published to it.
- The content is relevant to the community and is a resource for useful Academy documentation.
- All staff know their responsibilities for the selection and publication of material to the website.
- All staff understand the process of submitting material for the website.
- All staff understand who is responsible for the management of the website.
- The website enhances communication, supports accessibility and is easy to navigate.
- The website presents St. Clement's C of E Academy's face to the world.
- Pupils' work and activities are showcased.

b. Procedures

- The Network Manager, in consultation with the Senior Leadership Team, is responsible for website development, with day to day responsibility for quality assurance of all materials submitted.
- Staff should ensure that they collect content during events, trips and other Academy activities. This should then be posted to the academy website via the relevant blog.
- It is the responsibility of staff who are taking photographs/videos for use on the website to ensure they do not include individuals without consent. Should such a photo be mistakenly published or noticed on the Academy website, the photo must be removed immediately and the Computing coordinator, line manager or Designated Senior Lead be notified immediately and a record kept.
- The Head Teacher will have the ultimate decision on material uploaded to the site and will make the decision based on the aims of this Policy.
- The Policy will be reviewed every 1 year.

4. Social Networking Policy

a. What is Social Media?

Social Media is an online platform which connects many different users instantly for the purpose of social networking. Social Media has many different forms, and there are many different websites, which are classified as Social Media, such as Facebook, Instagram, Twitter, Google+, YouTube, LinkedIn (general age limit: 12-13+).

Social Media is used by a large number of adults and is fast changing/evolving so requires regular review. Information posted on social media is immediately out in the public domain forever no matter how securely you delete it. These guidelines are in place to ensure that all staff and pupils are protected online at all times, and has been designed to cater for all staff and includes members of the Boards of Governors. It is split into two different sections which detail the basic social media "do's and don'ts" for both personal and professional accounts. If you have any questions with regards to the policy, please do not hesitate to contact our Designated Senior Lead.

b. Personal Accounts

We firmly encourage the use of social media websites personally as well as professionally, however it is important that such technologies are managed in both a secure and professional way. We ask all staff members to remember that we work within an educational environment with young children and to:

We advise that St. Clement's C of E Academy staff do not follow/send/accept friend requests from any pupils (past or present) of parents or carers thereof on their personal accounts.

Maintain professional conduct with anything that is posted on social media networking sites.

Be careful what you write online – as soon as you have posted something on the it is often the case that may never be able to delete it. Remember you are representing St. Clement's C of E Academy online as others will more than likely be aware of where you work.

Ensure that any inappropriate content is removed immediately if requested.

Consider the potential impact when posting pictures and videos online - are they appropriate?

Consider the appropriateness of any comment you post about your work, and ensure that any such comments do not bring St. Clement's C of E Academy or your colleagues in to disrepute. If you are in any doubt you are best advised not to post any such comment.

St. Clement's C of E Academy reserves the right to decide on what is considered appropriate and what is not. If inappropriate content is noted, St. Clement's C of E Academy will take action, and, where appropriate, will contact the colleague in question to ensure the content is immediately deleted.

c. Professional Accounts

St. Clement's C of E Academy strongly encourages the use of social media within a professional environment – it is an extremely good communications tool, and a great way to keep parents/pupils/teachers and the general public up to date with what is going on at our Academy (live events, celebrations, closures, etc). It is important that social media accounts used within the Academy

are managed in an efficient and beneficial way, whilst also protecting the security of the personnel running the accounts. We have set out the following guidelines must follow at all times:

- *We ask that any class accounts setup on social media sites are setup using your Academy email accounts, and that account login details are shared with the Network Manager.*
- *Do not post pictures/videos of pupils who have not already agreed and signed any photo release forms beforehand.*
- *Do not post pictures/videos of colleagues on either personal or professional accounts where the colleague in question has not agreed for the photo to be posted without their express permission, or if the colleague has not signed the relevant release forms.*
- *Any inappropriate behaviour* is reported to the Academy with evidence (generally a screenshot) of the offending content. The Academy should take appropriate action in response to this, and, if in breach of St. Clement's C of E Academy policy, inform the appropriate line management.*
- *We ask that you do not post or forward anything unsuitable or inappropriate. If you are unsure on whether content is suitable or not, please seek advice from your Designated Senior Lead or the appropriate line manager, who will be able to advise further on this matter.*
- *Do not intentionally troll/provoke arguments with other users online, nor engage in inappropriate* conversations with pupils on social media.*
- *Do not upload content that is deemed inappropriate for public display or content which either reflects badly on yourself, or where it could be deemed to bring St. Clement's C of E Academy into disrepute.*
- *Do not use material (text, photos, videos, etc) without permission from the owner of the material. For example, pupils own the copyright to their own work therefore you should refer to the Academy policy on copyright.*
- *Do not assume that you can post photos, videos, music, etc created/captured by yourself as part of your work in the public domain, without seeking written permission first. Copyright laws state that your employer owns this content, so please seek consent in the first instance.*

***Inappropriate behaviour can include, but is not limited to:**

- *Discrimination - comments/content that could be deemed as racist, sexist, ageist, class, ethnicity, national origin, religion, sexual preference, disability or any other classification.*
- *Violent behaviour - This can include such things as threats, abusive/offensive language.*
- *Bullying & Harassment - This includes teasing, name calling, targeting specific users, etc.*
- *Explicit Content - can be any type of media including photos, videos, text or audio.*
- *Trolling - Intentionally provoking a negative response from someone.*
- *Negative content - Any content that could potentially reflect badly on the Academy.*

5. EYFS Mobile Phone & Camera Policy (The use of mobile phones & cameras in EYFS)

a. Introduction

The use of mobile technology should be considered an essential and integral part of everyday life. As such, children and young people, early years practitioners and their managers are to be encouraged to use such technology in a positive and responsible way.

It has to be recognised however, that digital technology has increased the potential for cameras and images to be misused and inevitably there will be concerns about the risks to which children and young people may be exposed. Practical steps must be taken to ensure that the use of cameras and images will be managed sensitively and respectfully. A proactive and protective ethos is to be reflected which will aim to promote effective safeguarding practice. Technology itself will not present the greatest risks, but the behaviours of individuals using such equipment.

b. Aim

The aim of the Mobile Phone/Camera Policy is to protect children from harm, by ensuring the appropriate management and use of mobile phones/cameras/mobile devices by all individuals who come into contact with the setting.

c. Scope

The Mobile Phone/Camera Policy will apply to all individuals who are to have access to and/or users of personal and/or work-related mobile devices within the setting environment. This will include, parents and carers, early year's practitioners and their managers, volunteers and students.

- **Staff's use of their own personal mobile within the setting.**

When at work staff mobile phones should be kept away from children in the store cupboard or locker.

Staff can make personal calls before and after the school day and during their break.

If staff are expecting an emergency call they should notify the EYFS or senior leader.

Staff can use their mobile phones during school trips e.g. to keep in touch with the Academy, each other, emergency services.

Staff should use Academy cameras, memory cards and ipads to take photos for Academy use eg blogs, display, assessment, special events.

If a camera from home is used the memory card must be cleared afterwards.

Photographs should only be stored on Academy equipment.

- **Parents use of their mobiles in the setting**

Parents are asked not to take phone calls in the setting. If they need to take calls they are asked to do so in the fenced areas where they enter away from children.

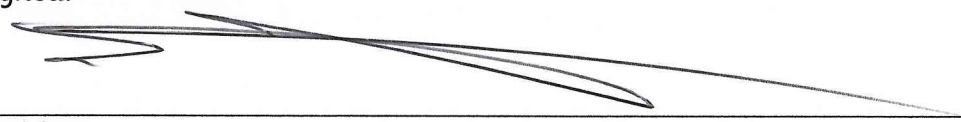
Parents are asked not to take photos on their phone unless there is a special reason eg first day of school, special dressing up day. On such an occasion, they should make a staff member aware and should only take a photo of their own child.

Parents are made aware of this at the July induction meeting and again in September at the Key worker consultation meeting or home visit.

6. Review and consultation

The Governing Body will review this policy at least annually.

This policy was adopted by Governing Body of St Clement's C. of E. Academy
On 14/6/2018

Signed: 
Position: Chair of Committee
Date: 14/6/2018

7. Appendices

Data Protection:

The Data Protection Act 1998 prohibits the disclosure of personal data except in accordance with the principles of the Act. This prohibition applies to Email in the same way as to other media. Information gathered on the basis that it would be seen by specified employees must not be given to a wider audience. In accordance with the provisions of Article 8 of the European Convention on Human Rights, the Academy respects the right to privacy for employees who use IT equipment but does not offer any guarantee of privacy to employees using IT equipment for private purposes.
As data controller, St. Clement's C of E Academy has responsibility for any data processed or stored on any of its equipment. Any employee monitoring will be carried out in accordance with the principles contained in the Code of Practice issued by the Information Commissioner under the provisions of the Data Protection Act 1998.

In order to comply with its duties under the Human Rights Act 1998, St. Clement's C of E Academy is required to show that it has acted proportionately, i.e. are not going beyond what is necessary to deal with the abuse and that the need to investigate outweighs the individual's rights to privacy, and that the need for any monitoring must be reasonable and proportionate.

Legislative Framework - The Human Rights Act 1998:

This provides for the concept of privacy giving a 'right to respect for private and family life, home and correspondence'. The provision is directly enforceable against public sector employers, and all courts must now interpret existing legislation in relation to the Human Rights Act. Halford v UK 1997 suggests that employees have a reasonable expectation of privacy in the workplace, and employers are recommended to provide workers with some means of making personal communications which are not subject to monitoring, for instance a staff telephone line or a system of sending private Emails which will not be monitored.

Covert monitoring is likely to be unlawful unless undertaken for specific reasons as set out in the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (see below). Employers should make sure workers know of any monitoring or recording of correspondence (which includes Emails, use of Internet, telephone calls, faxes and so on).

Regulation of Investigatory Powers Act 2000

This Act covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications system, and applies to public and private communication networks. It gives the sender or recipient of a communication the right of action for damages against the employer for the unlawful interception of communications. There are two areas where monitoring is not unlawful. These are: where the employer reasonably believes that the sender and intended recipient have consented to the interception; without consent, the employer may monitor in the following circumstances, as set out in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. These include:

- to ensure compliance with regulatory practices e.g. Financial Services Authority requirements
- to ensure standards of service are maintained, e.g. in call centres
- to prevent or detect crime
- to protect the communications system this includes unauthorised use and potential viruses
- to determine the relevance of the communication to the employer's business i.e. picking up relevant messages when someone is away from work.

However, the employer is expected to make all reasonable efforts to ensure system users know that communications may be intercepted, and any such monitoring must also comply with the provisions of the Data Protection Act 1998 (see below), and in particular the Data Protection principles on fair processing.

Data Protection Act:

The Information Commissioner - responsible for enforcement of the Data Protection Act - is publishing four codes of practice to help employers comply with the provisions of the data Protection Act. These codes clarify the Act in relation to processing of individual data, and the basis for monitoring and retention of email communications.
The code of practice monitoring at work: an employer's guide states that any monitoring of emails should only be undertaken where:

- The advantage to the business outweighs the intrusion into the workers' affairs
- Employers carry out an impact assessment of the risk they are trying to avert workers are told they are being monitored
- Information discovered through monitoring is only used for the purpose for which the monitoring was carried out
- The information discovered is kept secure
- Employers are careful when monitoring personal communications such as emails which are clearly personal
- Employers only undertake covert monitoring in the rarest circumstances where it is used for the prevention or detection of crime.

Telecommunications:

This Act empowered the Secretary of State to make regulations, which allow businesses to intercept communications in the course of lawful business practice and in specific circumstances without the express consent of either the sender or the recipient. Under the Regulations, businesses are required to make all reasonable efforts to inform users of their own systems that such interceptions might take place.

Contract law:

It is just as possible to make a legally binding contract via Email as it is by letter or orally. Workers need to be aware of the danger of inadvertently making contracts on behalf of their employer, or varying the terms of any existing contract.

Copyright law:

The Copyright, Designs and Patents Act 1988 (as amended) gives the same protection to digital and electronic publications as it does to printed books and other forms of publication. Many websites carry warnings that the information given is copyright and should not be downloaded without agreement from the copyright holder. Similarly copyright exists over software, which should not be downloaded without license.

Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988
These Acts are concerned with material that might be criminal, cause harm to young persons or be otherwise unlawful. In the workplace the downloading of certain images from the Internet might subject a worker to charges of criminal behaviour.

Computer Misuse Act 1990:
This Act is mainly concerned with the problems of 'hacking' into computer systems.

Lawful Business Practice Regulations (LBP):

- *The LBP Regulations authorise employers to monitor or record communications without consent for a number of purposes, including the following:*
- *To establish the existence of facts relevant to the business.*
- *To ascertain compliance with the regulatory or self-regulatory practices or procedures relevant to the business.*
- *To ascertain or demonstrate standards which are, or ought to be, achieved by persons using the system.*
- *To prevent or detect crime.*
- *To investigate or detect the unauthorised use of telecommunication systems.*
- *The Regulations cover all types of online communications including email.*