Dover Christ Church
Academy

ONLINE SAFETY POLICY

This policy was ratified by the Governing Body on:	March 2016
This policy will be reviewed in:	February 2017
This policy was reviewed in:	February 2016
This policy is owned by the Designated Safeguarding Lead:	Mr G May

Dover Christ Church
Academy

Canterbury
Christ Church
University

Strategic Framework 2015-2018

MISSION STATEMENT

We are proud to be part of the unique community of Dover Christ Church Academy where everyone is valued, supported and challenged to achieve their very best. Through our partnership with Canterbury Christ Church University, we all work hard to provide the highest quality education. We are committed to excellence, inspiring teaching in outstanding buildings, where students enjoy learning and make excellent progress. We believe that anything is possible and through our high aspirations and everyone's hard work, students will achieve their goals and go on to live full and meaningful lives.

VALUES

- The development of the whole person, respecting and nurturing the inherent dignity and potential of each individual
- The development and delivery of excellent teaching and learning
- The power of education and lifelong learning to transform individuals, communities and nations
- Our friendly, inclusive and professional community of students, staff and families preparing individuals to contribute to a just and sustainable future

The acceptable use of the Internet, Intranet, e-mail, messaging systems and related technologies

This policy sets out the Academy's expectations of staff, students and other users (working for or on behalf of the Academy), in respect to the use of the Internet, Intranet, e-mail, messaging systems and related technologies.

This policy applies to all Internet, Intranet, e-mail, messaging systems and all related technology services provided by the Academy, and to all Academy users accessing these services.

This policy is designed to express the Academy's philosophy with regard to the Internet, Intranet and electronic communication in general and to set forth general principles users should apply when using these services at the Academy. This guidance does not attempt to cover every possible situation.

This policy notes the Common Inspection Framework: Education, Skills and Early Years from September 2015 and its emphasis on online Safety as opposed to e-safety and reflects this new emphasis here in the adoption of that language and in the measures given below to safeguard children and young people online.

Please Note: This online safety Policy has been written by the Academy, building on the Local Authority Model Policy, the London Grid for Learning (LGfL) exemplar policy and Becta guidance. It will be reviewed every twelve months.

1. Introduction

The Internet, Intranet, e-mail, messaging systems and related technologies can be extremely valuable tools in an educational context, encouraging the development of communication skills, and transforming the learning process by opening up possibilities that, conventionally, would be impossible to achieve. The Academy encourages the use of electronic mail as a medium for paper mail replacement and as a means of enhancing communications.

Creating a safe ICT learning environment includes three main elements at the Academy:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- Access to online safety information for students, staff, parents and carers and other users;

2. Context

Harnessing Technology: Transforming Learning and Children's Services [1] sets out the government plans for taking a strategic approach to the future development of ICT.

[1] www.dfes.gov.uk/publications/e-strategy

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.
To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DCFS, e-Strategy 2005

The Green Paper *Every Child Matters*[2] and the provisions of the *Children Act 2004*[3], *Working Together to Safeguard Children*[4] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation;
- safe from accidental injury and death;
- safe from bullying and discrimination;
- safe from crime and anti-social behaviour in and out of Academy;
- secure, stable and cared for

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the Internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the Academy to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as are applied to the Academy's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the Academy and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

3. The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of

[2] See The Children Act 2004 www.opsi.gov.uk/acts/acts2004/20040031.htm

[3] See Every Child Matters website www.everychildmatters.gov.uk

[4] Full title: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children. See Every Child Matters website www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E403514A6C1B17D.pdf

information. Current and emerging technologies used in Academy and, more importantly in many cases, used outside of Academy by children include:

- The Internet
- E-mail and Webmail E.G. *www.hotmail.co.uk, www.yahoo.co.uk;*
- Instant messaging often using simple web cams E.G*. www.msn.com, www.aim.com;*
- Blogs (an on-line interactive diary) E.G. www.blogger.com;
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player);
- Social networking sites E.G. *www.myspace.com, www.bebo.com, www.facebook.com;*
- Video broadcasting sites E.G. *www.youtube.com;*
- Chat Rooms www.teenchat.com, www.habbohotel.co.uk;
- Gaming Sites www.neopets.com, www.miniclip.com/games/en, www.runescape.com;
- Music download sites E.G. www.napster.co.uk, www.limewire.com;
- Mobile phones with, Bluetooth, messaging, camera and video functionality;
- Messaging or Bluetooth communications between systems and mobile devices;
- Smart phones with e-mail, web functionality and cut down 'Office' applications;
- Mobile devices that access the Internet both inside and outside of Academy;
- Remote access to the Academy network
- Academy provided systems such as the Intranet and eZeSchools.

4. Misuse

The Internet, Intranet, email, messaging systems and related technologies must not be used for knowingly viewing, transmitting, retrieving, downloading or storing any communication that is:

- Discriminatory or harassing;
- Derogatory to any individual or group;
- Obscene or pornographic;
- Defamatory, threatening or seen as cyber bullying;
- Illegal or contrary to the Academy's policy or business interests;
- Subject to Copyright such as music, software or films;
- Likely to cause network congestion or significantly hamper access for other users;
- Any of the above, specifically using mobile devices or similar technologies to store or upload any such materials to the public domain (social networking sites) or to other devices;

Except in cases in which explicit authorisation has been granted by Academy management, users are prohibited from engaging in, or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other users;
- Using other user's log-ins or passwords;
- Breaching, testing, or monitoring computer or network security measures;
- E-mail or other electronic communication that attempts to hide the identity of the sender or represent the sender as someone else;
- Hacking, Blue-jacking or accessing systems or accounts that they are not authorised to use;
- Obtaining electronic access to other companies' or individuals' materials. (Copyright means users cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner);

Law and Academy policy prohibit the theft or abuse of computing resources and includes:

- Unauthorised entry;
- Using, transferring and tampering with other people's accounts and files;
- Interfering with other people's work or computing facilities;
- Sending, storing or printing offensive or obscene material including content that may be interpreted as sexual or racial harassment;
- Mass mailing of messages;
- Internet use for personal commercial purposes;
- Using the internet/intranet facilities or equipment to deliberately propagate any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations;
- Accessing or uploading to any obscene or pornographic sites. Sexually explicit material may not be viewed, archived, stored, distributed, edited or recorded using the Academy's networks or computing resources;

If a user finds himself / herself connected accidentally to a site that contains sexually explicit or offensive material, they must disconnect from that site immediately. Such unintentional access to inappropriate internet sites must be reported immediately to the respective tutor, line manager or Principal. Any failure to report such access may result in disciplinary action.

It is impossible to define all possible unauthorised use, however, disciplinary action may be taken where a user's actions warrants it. Other actions deemed unacceptable, although not exhaustive, include:

- Theft or copying of files without permission;
- Sending or posting the Academy's or local authority's confidential files outside of the organisation or inside the organisation to unauthorised staff, students or other users;
- Refusing to co-operate with reasonable security investigation;

5. E-mail, Messaging and Digital Communication (Social Networking) Use

Those that use the Academy's e-mail, messaging or other digital communication services and messaging services are expected to do so responsibly, comply with all applicable laws, other policies and procedures of the Academy, and with normal standards of professional and personal courtesy and conduct. The Appendix provides an illustration of good practice.

The Academy follows sound professional practices to secure e-mail records, messaging systems, data and system programmes under its control. As with standard paper based mail systems, confidentiality of these cannot be 100% assured. Consequently users should consider the risks when transmitting highly confidential or sensitive information and use the appropriate level of security measure.

Enhancement of the base level security to a higher or intermediate level can be achieved by the use of passwords for confidential files. It should be remembered messages forwarded from another individual can be amended by the forwarder. This possibility should be considered before acting on any such mail.

In order to effectively manage these systems the following should be adhered to:

- Open messages/mailboxes must not be left unattended;
- Care should be taken about the content of a message as it has the same standing as a letter;
- Report immediately to IT Technicians when a virus is suspected in a message;

Users must not

- Ignore messages. These systems are designed for speedy communication. If the message requires a reply, a response should be sent promptly;
- Use anonymous messaging services to conceal identity when mailing through the Internet; falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details;
- Abuse others, even in response to abuse directed at them;
- Use these technologies, either internally or on the Internet, to sexually harass fellow employees, or harass or threaten anyone in any manner;

The transmission of user names, passwords, chain mail or other information related to the security of the Academy's computers is not permitted.

6. Use at Home

Students, staff or other users accessing the Internet from home whilst using an Academy owned computer or mobile device or through Academy owned connections must adhere to the policies set out in this document.

7. Personal Use

The Internet, Intranet, e-mail, messaging systems and other related technologies are business tools provided to users at significant cost. Hence, it is expected that this resource will be used primarily for business related purposes. Reasonable access and use of these systems is also available to recognised representatives of professional associations i.e. Union Officers.

These systems may be used for incidental personal purposes, provided that it does not:

- Contravene the statements laid out in the Misuse section;
- Interfere with the Academy's operation of computing facilities or e-mail services;
- Interfere with the user's employment or other obligations to the Academy;
- Interfere with the performance of professional duties;
- Is of a reasonable duration and frequency;
- Is performed in non-work time;
- Does not over burden the system or create any additional expense to the Academy

Such use must not be for:

- Unlawful activities;
- Commercial purposes not under the auspices of the Academy;
- Personal financial gain;
- Personal use inconsistent with other Academy policies or guidelines

All such use should be done in a manner that does not negatively affect the use of the Academy's systems for business purposes. Users are expected to demonstrate a sense of responsibility and not abuse this privilege.

8. Privacy

The Academy respects users' privacy, e-mail content will not be routinely inspected or monitored, nor content disclosed without the originator's consent. However, under the following circumstances such action may be required:

- When required by law;
- If there is a substantiated reason to believe that a breach of the law or Academy policy has taken place;
- When there are emergency or compelling circumstances

The Academy reserves the right, at its discretion, to review any user's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other Academy policies.

Users should not have any expectation of privacy to his or her internet usage. The Academy reserves the right to inspect any and all files stored in computers or on the network in order to assure compliance with this policy. Auditors must be given the right of access to any document, information or explanation that they require.

The use of students, staff or other users designated personal file area[5] on the network server provides some level of privacy in that it is not readily accessible by other users. These file areas will however be monitored to ensure adherence to the Academy's policies and to the law. The user's personal file area (N: Drive) is disk space on the central server and is allocated to that particular user.

Managers will not routinely have access to a user's personal file area. However, usage statistics/management information on usage size of drives or a report outlining the amount of information held on an individual's personal file area will be made available from time to time.

9. Policy Violations

Staff, students or other users who abuse the privilege of Academy-facilitated access to the Internet, Intranet, e-mail, messaging systems or other related technologies face being subjected to disciplinary action, up to and including termination of employment (staff) or exclusion (students), and risk having the privilege removed for themselves and possibly other employees/peers.

10. Roles and Responsibilities

Online safety is recognised as an essential aspect of strategic leadership at an Academy and the Principal, with the support of Governors, aims to embed safe practices into the culture of the Academy. The Principal ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for online safety has been designated to a member of the Senior Leadership Group.

Our Academy online safety Co-ordinator is Gary May, Vice Principal who is also Designated Safeguarding Lead

Our online safety Co-ordinator ensures they keep up to date with online safety issues and guidance through liaison with the Local Authority online safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection service (CEOP)[6]. The Academy's online safety Co-ordinator ensures the Principal, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of online safety issues and strategies at our Academy. We ensure Governors are aware of our local and national guidance [7] on online safety and are updated at least annually on policy developments. Peter Gregory is Designated Online Safety Governor and also Designated Safeguarding Governor.

[5] Before storing confidential information in this way, users are advised to ensure that they understand how to save information to their personal file area.

[6] http://www.ceop.gov.uk/

[7] Safety and ICT - available from Becta, the Government agency at: http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_str_02&rid=10247

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following Academy online safety procedures. Central to this is fostering a ‘No Blame’ culture so students feel able to report any bullying, abuse or inappropriate materials.

All students, staff and other users should be familiar with this policy including:

- E-mail, messaging and digital communication (social networking) use;
- Safe use of Academy network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones, digital cameras and video cameras;
- Publication of pupil information/photographs and use of the Intranet and the Academy website;
- e-Bullying and Cyber-bullying procedures as per the Academy’s Anti-bullying policy;
- Their role in providing/accessing online safety information;

Staff and students are reminded/updated about online safety matters and the Academy’s online safety policy at least once a year.

Where staff have concerns about the safety of students online, or about unsafe use of technology these concerns should be shared with the Online Safety Lead/DSL or online safety co-ordinator/Deputy DSL via our existing Green Form procedures.

11. How Will Complaints Regarding online safety be Handled?

The Academy will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a Academy computer or mobile device. Neither the Academy nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Students and staff have access to information about infringements in use and possible sanctions.

Sanctions available include:

- Interview or counselling by Tutor/Year Heads/online safety Co-ordinator/Vice Principal;
- Informing parents or carers of students;
- Removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including staff files or student examination coursework

Our online safety Co-ordinator acts as first point of contact for any complaint. However, any complaint about staff, student or other users misuse can also be referred to the Principal.

Complaints of Cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with Academy/LA child protection procedures.

Appendix

1. 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[8], 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, the 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, the 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, taking into account the Academy's wider business interests. In drawing up and operating this policy the Academy recognises that the need for any monitoring must be reasonable and proportionate.

Auditors (internal or external) are able to monitor the use of the Academy's IT equipment and the storage of data. They are nevertheless bound by the provisions of the Human Rights Act 1998, the Data Protection Act 1998, associated codes of practice and other statutory provisions and guidance, including the Regulation of Investigatory Powers Act 2000 in respect of any activity that could be classed as directed surveillance[9]. (See Appendix 2)

2. Email e-mail and messaging good practice guide

	Good Practice
Read Receipt	When it is important to know that a recipient has opened a message, it is recommended that the sender invoke the 'read receipt' option.
Attachment Formats	When attaching a file it will have a specific format. Be aware of the possibility that a recipient may not have the software

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[9] Directed Surveillance' is defined as surveillance which is covert (i.e. carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place) but not intrusive, for the purpose of a specific investigation in such a manner as is likely to result in the obtaining of private information about a person.

	necessary to read the attachment. Format incompatibility can occur even between successive versions of the same software, e.g. different version of Microsoft Word.
Email Address Groups	If messages are regularly sent to the same group of people, the addressing process can be speeded up by the creation of a personal group in the personal address book.
Message header, or subject	Convey as much information as possible within the size limitation. This will help those who get a lot of Emails to decide which are most important, or to spot one they are waiting for.
Subject	Avoid sending messages dealing with more than one subject. These are difficult to give a meaningful subject heading to, difficult for the recipient to forward on to others for action, and difficult to archive.
Recipients	Beware of sending messages to too many recipients at once. When sending messages for more than one-person's use be sure to indicate people for whom there is some expectation of action or who have central interest. cc to indicate those who have peripheral interest and who are not expected to take action or respond unless they wish to do so.
Replying	When replying to a message sent to more than one person, do not routinely reply to all recipients of the original message. Consider who needs to read your reply, e.g. if the sender is organising a meeting and asking you for availability dates, you need only reply to the sender.
Absent	If you have your own Email address, it is possible, for users of MS Exchange or have local enhancements to MS-mail, to set the 'out of office' message when you are going to be away for some time, e.g. on annual leave. You won't lose your messages, they will await your return, but the sender will know that you're not there and can take alternative action if necessary.
Evidential Record	Never forget that electronic conversations can produce an evidential 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.
Distribution Lists	Keep personal distribution lists up-to-date and ensure you remove individuals from lists that no longer apply to them.
Email threads	Include the previous message when making a reply. This is called a thread. Threads are a series of responses to an original message. It is best that a response to a message is continued by using reply accessed on the quick menu bar, rather than start an entirely new message for a response.

	Keep the thread information together. It is easier for the participants to follow the chain of information already exchanged. If the message gets too long the previous parts can be edited while still leaving the essence of the message.
Context	Email in the right context, care should be taken to use Email where appropriate. There may be occasions when a telephone call would be more appropriate especially on delicate matters. Beware of the use of excessive use of capitals. It can be interpreted as SHOUTING so consider how the style of your email may be interpreted by its recipient.
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.
Large Emails	For larger Emails, particularly Internet Emails, where possible send at the end of the day as they may cause queues to form and slow other peoples Email.

3. 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).

4. 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, ie 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.

5. 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.

6. Telecommunications (Lawful Business Practise) (Interception of communications) Regulations 2000

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.

7. 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 communications including those that are Internet based, by fax and by email.