KIRKLEES COLLEGE

Acceptable use of IT systems for staff and students

September 2019

Contents

1. Introduction

1.1 Purpose

This Acceptable Use Policy applies without exception to all users of IT facilities of Kirklees College be they staff, student, or a visitor with temporary access privileges, and whether registered as a user with Kirklees College. The aim of these guidelines are :

1. To ensure security of College IT systems.
2. To safeguard the College's business.
3. To inform all users (staff and students) of all relevant legislation relating to IT.
4. To provide an appropriate teaching and learning environment for all College IT Users.
5. To ensure all users of College IT systems are aware of the Terms and Conditions laid down by JANET

1.2 Scope

This policy covers users' activities while using any computing facilities owned by Kirklees College wherever those facilities may be located (e.g. a Laptop Computer taken home or accessing the internet via Wi-Fi). This policy also covers any personal devices that contain college data, for example, personal mobile phones that have college email accounts installed on them.

It covers users' activities while using any other computing facilities used on Kirklees college premises and users of Kirklees College facilities who have connected over the internet or via dial-up from off site to access Kirklees College resources.

All users will be deemed to be familiar with and bound by this document, copies of which are on Kirklees College Website and Intranet (KCShare).

Kirklees college complies with the Government PREVENT agenda and as such employs various systems and controls to minimise risk to individuals and the organisation such as web & email filtering, anti-malware protection and systems capable of scanning keywords and content on the local machine or network drives.

1.3 Exceptions

Unless agreed by the Director of MIS,IT and Risk, then there are no exceptions to this policy.

2. Authorisation to use College IT systems

2.1 USE OF E-MAIL

2.1.1 Try not to create e-mail congestion by sending trivial messages or unnecessarily copying e-mails. Employees should regularly delete unnecessary e-mails to prevent over-burdening the system.

2.1.2 E-mails should be drafted with care. Bear in mind that all expressions of fact, intention and opinion via email can be held against you and/or the College in the

same way as verbal and written expressions or statements. Do not include anything in an email which you cannot or are not prepared to account for. It is good practice to re-read each email before sending it. Email messages which have been deleted from the system can be traced and retrieved. Therefore, all persons having a part in creating or forwarding any offending emails can be identified. Emails, both in hard copy and electronic form, are admissible in a court of law.

2.1.3 You may want to obtain e-mail confirmation of receipt of important messages. You should be aware that this is not always possible and may depend on the external system receiving your message. If in doubt, telephone to confirm receipt of important messages.

2.1.4 By sending e-mails on the College's system, you are consenting to the processing of any personal data contained in that e-mail and are explicitly consenting to the processing of any sensitive personal data contained in that e-mail. If you do not wish the College to process such data you should communicate it by other means.

2.1.5 All transmissions of materials using E-mail must carry the name of the sender and must not be used for private commercial purposes.

2.1.6 It is the responsibility of individual staff to ensure that arrangements are made to ensure that e-mails are opened during periods of absence e.g. Illness or holidays. Alternatively an auto reply may be used to inform the sender of when the e-mail will be dealt with

2.1.7 The College will add a disclaimer to all outgoing e-mails. This disclaimer is reproduced below but may change from time to time

'The Information provided in this E-mail is confidential and may be privileged. It is intended for the addressee only. If you are not the intended recipient please delete this E-mail immediately. The contents of this E-mail must not be disclosed or copied without the sender's consent. The statements and opinions expressed in this message are those of the author and do not necessarily reflect those of the College. The College does not take any responsibility for the views of the author. E-mail may be susceptible to data corruption, interception, unauthorised amendment, viruses and delays or the consequences thereof. Accordingly, this E-mail and any attachments are opened at your risk'.

2.1.8 While Kirklees College is a data controller of all personal data processed for the purposes of our business, you will be a data controller of all personal data processed in any personal email which you send or receive. Use for social, recreational or domestic purposes attracts a wide exemption under the Data Protection Act, but if, in breach of this policy, you are using our communications facilities for the purpose of a business which is not Kirklees College business, then you will take on extensive personal liability under the Data Protection Act.

2.1.9 If you undertake an archive of any emails (as opposed to the recommended option of saving essential emails as files and allowing remaining emails to be auto-deleted after 90 days) then you have taken personal responsibility for any legal implications on this data – including freedom of information and data protection. In effect you have taken this information out of the control of Kirklees College.

2.1.10 Email should NOT be used to transmit personal data of either staff or students. Particular care should be taken by individuals where email is accessed over a personal device such as a phone or tablet device connected via the internet. All such

devices should as a minimum have a password or pin enabled to allow access to the device

2.1.11 Any emails sent to multiple external recipients MUST use the BCC facility to keep email addresses private as per the GDPR regulation

2.2 USE OF THE INTERNET

Reasonable private and personal use of the internet is encouraged and permitted for College students and staff within the guidelines as above and providing it is carried out in the user's own time.

2.2.1 any private usage should be kept to a minimum and should not interfere with your work. Excessive private access to the Internet during working hours may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.

2.2.2 The sites accessed by you must comply with the restrictions set out in these guidelines. Accessing inappropriate sites may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct. Internet access is monitored and reported.

2.2.3 Staff who place information on the College Website must ensure that such information is free from inaccuracy or defamatory statements.

2.2.4 To protect staff and students from accidental access to various objectionable sites the College has installed and maintains a Firewall and Content Filter to block access to listed sites. The categories that are blocked are available from the ITSU. Also, the college has implemented the eSafe system, which proactively monitors activity and flags actions that meet predefined criteria for review.

2.2.5 As the JANET network is our Internet Service Provider we are necessarily bound by their policies which are in addition to our own. These are available at

http://www.ja.net/services/publications/policy-documents/terms-for-the-provision-of-the-janet-service.html

2.3 UNACCEPTABLE USE OF IT EQUIPMENT, E-MAIL AND THE INTERNET

When using the internet and/or e-mail, all users have a responsibility to ensure that it is not abused and must comply with this policy at all times. Excessive use during working time and/or failure to comply may result in disciplinary action being invoked, including dismissal.

Unacceptable use of College computers and network resources may be summarised as:

1. Creating, displaying or transmitting material that is fraudulent or otherwise unlawful or inappropriate. This includes pornographic or other obscene material.
2. Threatening, intimidating or harassing employees/students.
3. Using obscene, profane or abusive language.
4. Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights.

5. Defamation (genuine scholarly criticism is permitted).
6. Unsolicited advertising often referred to as "spamming".
7. Sending emails that purport to come from an individual other than the person actually sending the message e.g. a forged address.
8. Attempts to break into or damage computer systems or data held thereon.
9. Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software.
10. Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised.
11. Using the College network for unauthenticated access.
12. Unauthorised resale of College or JANET services or information.
13. Using the ICT Facilities to conduct personal commercial business or trading.
14. Creation or transmission of unsolicited bulk or marketing material.
15. Any other conduct which may discredit or harm the College, its staff or the ICT facilities or is intentionally unethical / illegal even if not specifically listed in this policy is deemed unacceptable.

Under no circumstances should a non-college device be connected to the college network unless it is via the available wifi.

These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of these guidelines :

1. Downloading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid licence or other valid permission from the copyright holder. These circumstances may be treated by the College as gross misconduct. The College reserves the right to use the content of any employee e-mail in any disciplinary process.

2. Giving or entering your personal information on a website, especially your home address, your mobile number or passwords. (applicable only to students). Staff may need to register on certain web sites as a requirement of their role (eg IfL website for CPD purposes)

3. Accessing online gaming sites.

4. Using the Internet to order goods or services from on-line, e-commerce or auction sites unless with the authority of the College, ie a tutor, Financial Services or a Tier 4 manager or above.

5. Distribution or storage by any means of pirated software.

6. Connecting an unauthorised device to the College network, i.e. one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, purchasing policy, and acceptable use.

7 Circumvention of network access control.

8. Monitoring or interception of network traffic, without permission.

9. Probing for the security weaknesses of systems by methods such as port-scanning, without permission.

10. Associating any device to network Access Points, including wireless, to which you are not authorised.

11. Non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of ICT services or which incur financial costs.

12. Excessive personal use of resources such as file store, leading to a denial of service to others, especially when compounded by not responding to requests for action.

13. Frivolous use of College owned IT facilities, especially where such activities interfere with others' legitimate use of ICT services.

14. Use of College business mailing lists for non-academic purposes.

15. Use of CDs, DVDs, USB devices and any other storage devices for the purpose of copying unlicensed copyright software, music, etc.

16. Copying of other people's web site material without the express permission of the copyright holder.

Users must not deliberately visit, view, download, print, copy, forward or otherwise transmit any unlawful material. If you mistakenly access such material you should notify ITSS (Ext 7016). You should be aware that you will be held responsible for any claims brought against the College. In the event of any use that could be regarded as giving rise to criminal proceedings the College may inform the police or other law enforcement agency.

Other uses may be unacceptable in certain circumstances. If it in doubt, it is expected that users will take the conservative view and deem that it is unacceptable usage of College ICT system.

2.4 COPYRIGHT AND DOWNLOADING

2.4.1 Copyright applies to all text, pictures, video and sound, including those sent by e-mail or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

2.4.2 Copyrighted software must never be downloaded. Such copyrighted software will include screen-savers.

2.4.3 The maximum file size you are permitted to download is 10mb. – unless you have authority to do otherwise from IT Services

2.4.5 College employees should not import non-text files or unknown messages on to the College's system without having them scanned for viruses. If you have not been properly trained to scan for viruses, do not import such items at all.

2.4.6 College employees must never engage in political discussions through outside newsgroups using the College's computer system.

2.4.7 Personal data must not be stored on any mobile device. All personal data should reside on central systems and be accessed securely across encrypted links

2.5 GENERAL COMPUTER USAGE

2.5.1 You are responsible for safeguarding your password for the system. For reasons of security, your individual password should not be printed, stored on-line or given to others. User password rights given to employees should not give rise to an expectation of privacy.

2.5.2 Your ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so. You should not alter or copy a file belonging to another user without first obtaining permission from the creator of the file.

2.5.3 Staff with a college device should ensure that all necessary precautions are taken when taking equipment offsite to prevent theft. In addition all devices need to be kept up-to-date with antil-malware software

2.6 Bring Your Own Device (BYOD)

In the interests of teaching and learning the College would like to encourage students to use their own electronic devices on campus. WiFi facilities will be available at main campus sites giving students access to the Virtual Learning Environment and filtered access to the wider internet.

The College offers these facilities under the following conditions for students:

- The college is not liable for any loss or damage to personal electronic equipment whilst on or between home and college premises;
- Students will not abuse college policies nor breech the law under the Computer Misuse Act or Data Protection Act whilst on college premises;
- Devices cannot be connected by cable to the college network;
- No support will be given by College IT staff for faults on personal devices;
- Students are encouraged to bring devices fully charged but provision for charging within college is accepted under the following conditions:
    - Charging equipment should be in good condition with no visible defects to wires etc
    - No trailing cables across walkways or where these could cause hazard to other college users
    - A maximum of 1 hours charge is available to students
    - Charging will only be permitted in designated areas
- Adherence to the main policy

Details on how to access the Wireless facilities can be found on the VLE and on KCShare

Failure to adhere to these rules will result in disciplinary action by the college.

2.6 USE OF COLLEGE TELEPHONES/FAX MACHINES

2.6.1 Reasonable use of College telephones is permitted for personal use. It is expected that only essential personal calls will need to be made during normal working hours Where any member of staff is found to be abusing this facility, appropriate action will be taken including formal disciplinary measure.

2.6.2 International calls are only allowed from certain phones and only for College business

2.6.3 Calls to Premium rate lines (09..) are not allowed under any circumstances

2.6.4 Staff who are in possession of and authorised to use 'walkie talkie' equipment around College should be aware that their conversations are audible to both staff and students in the vicinity. Language used should therefore be appropriate and must not be considered obscene, abusive, sexist, racist or defamatory.

2.7 USE OF MOBILE PHONES

2.7.1 College Mobile phones are for College business only and therefore will only be approved for essential users.

2.7.2 Staff are allocated mobile phones for legitimate College business only, and should not use the phone for private purposes. Calls are monitored and where such mis-use occurs the staff member could be subject to disciplinary action.

2.7.3 The use of mobile phones are monitored by the Director of IT. Allocation is dependent upon set criteria and where there is no longer a need or usage is minimal the phone should be returned to IT for cancellation or reallocation.

2.7.4 The member of staff to whom a mobile phone has been allocated will be responsible for its proper use, care, maintenance and safe keeping.

2.7.5 Mobile phones cannot be transferred to another user without the express permission of the Finance Director who must then inform IT so that the College records can be updated.

2.7.6 Staff must not use mobile phones for business purposes whilst driving to either make a phone call, text or access any other data source. The use of a mobile phone whilst driving will lead to disciplinary action.

2.7.7 Whilst it is still unproven the College recommends that all calls from mobile telephones are kept to a minimum call time on Health and Safety grounds.

Access to internet and data services from mobiles should be purely for business purposes and not for private use. Where such mis-use occurs the staff member could be subject to disciplinary action.

2.8 USE OF THE COLLEGE POSTAL SERVICE

2.8.1 The College postal service is an essential part of operations and may only be used for personal use to despatch mail with the appropriate postage in place. In no circumstances must personal mail be franked using College equipment. Personal mail without postage will be intercepted and returned to the sender.

2.8.2 It is the responsibility of individual staff to ensure that arrangements are made to ensure that post is opened during periods of absence eg. Illness or holidays

3 CCTV

Close Circuit Television (CCTV) is in operation in public areas at all times for the safety and protection of employees and students. Covert monitoring may from time to time be necessary, where supported by known/evidence of previous criminal activity, for the prevention or detection of crime.

Access to CCTV images are protected by law and any request should be made via the Head of Health and Safety.

4. IT Support Unit

The IT Support Unit is there to assist you. If you require any information or help about the use or set up of your computer you should contact any of the Unit's members of staff. The primary point of contact should always be the IT Service Desk via the self service portal or if urgent via the IT Helpdesk phone on 7016

5 Authorisation for use of College ICT Systems

In order to use the ICT Facilities of Kirklees College an individual must first be properly registered to use such services. Use of College ICT facilities will be deemed to be acceptance of the terms and conditions of this policy. It is expected that all users will adhere to the College's password policy and guidelines, data protection policies in addition to all relevant College, regulatory and legal requirements.

6 Privacy and Monitoring

6.1 Kirklees College recognises that individuals may conduct personal use of email and the Internet. However this must be kept to a minimum and be compliant with the various College and legislative requirements. The College reserves the right

to revoke such permission if, in the judgement of the College, these facilities are abused.

6.2 The College reserves the right for appropriately authorised staff to examine any data including personal data held on College systems or, when operationally necessary, for example to give access to a private account to a line manager or colleague. Certain staff within the College have been authorised to examine files, emails, data within individual accounts and network traffic, but will only do so when operationally necessary

6.3 The College reserves the right to monitor email, telephone and any other electronically mediated communications, whether stored or in transit, in line with the relevant regulatory and legislative rules/laws. This may be undertaken internally within college or via an external organisation.

6.4 Reasons for such monitoring include the need to:

- Establish the existence of facts (e.g. to provide evidence of commercial transactions in cases of disputes);

- Investigate or detect unauthorised use of the College's telecommunications systems and ensure compliance with this policy or other College policies;

- Ensure operational effectiveness of services (e.g. to detect viruses or other threats to the systems);

- Prevent a breach of the law or investigate a suspected breach of the law, the College's policies and contracts;

- Comply with the Government's PREVENT agenda;

- Monitor standards and ensure effective quality control.

College staff that have access to personal data (as defined under the Data Protection Act 1998) are responsible for ensuring that such data is not made available to unauthorised individuals and that the security of all systems used to access and manage this data is not compromised.

The College has the right to access the personal account after the staff member leaves for operational reasons and for the continuing delivery of services.

Users of ICT Facilities should be aware that the College conducts monitoring of communications from college devices, regardless of whether the use is business or personal. This includes the use of external partners.

Monitoring may involve:

1. Examining the number and frequency of emails;
2. Viewing sent or received e- mails from a particular mailbox or stored on any server;
3. Examining logs of ICT facility usage.
4. Monitoring the amount of time spent on the Internet;
5. Internet sites visited and information downloaded.

Where abuse is suspected (especially criminal activity and/or gross misconduct), the College may conduct a more detailed investigation involving further monitoring and examination of stored data (including employee-deleted data) held on servers/disks/drives or other historical/archived data.

Where disclosure of information is requested by the police (or another law enforcement authority) the request where possible will be handled by the College's Data Protection Officer or other relevant person.

Appendix 1 - Legal constraints

Introduction

Any software and / or hard copy of data or information which is not generated by the user personally and which may become available through the use of College computing or communications resources shall not be copied or used without permission of the College or the copyright owner.

In particular, it is up to the user to check the terms and conditions of any licence for the use of the software or information and to abide by them. (This can be done through reference to the Software Licence Administrator.) Software and / or information provided by the College may only be used as part of the user's duties as an employee or student of the College or for educational purposes.

The user must abide by all the licensing agreements for software entered into by the College with other parties, noting that the right to use any such software outside the College will cease when an individual leaves the institution. Any software on a privately owned computer that has been licensed under a College agreement must then be removed from it, as well as any College-owned data, such as documents and spreadsheets.

When a computer ceases to be owned by the College, all data and software must be permanently removed, in accordance with the College's policies and contractual obligations.

In the case of private work and other personal use of computing facilities, the College will not accept any liability for loss, damage, injury or expense that may result.
The user must comply with all relevant legislation and legal precedent, including the provisions of the following Acts of Parliament, or any re-enactment thereof:

1. Copyright, Designs and Patents Act 1988
2. Malicious Communications Act 1988
3. Computer Misuse Act 1990
4. Criminal Justice and Public Order Act 1994
5. Trade Marks Act 1994
6. General Data Protection Regulation 2018
7. Data Protection Act 2018
8. Human Rights Act 1998
9. Regulation of Investigatory Powers Act 2000
10. Freedom of Information Act 2000
11. Communications Act 2003

12 Defamation Act 1996

13 Discrimination/Harassment legislation

For reference, the main points of these acts are,

1. Copyright, Designs and Patents Act 1988

This Act, together with a number of Statutory Instruments that have amended and extended it, controls copyright law, making it an offence to copy all, or a substantial part,

Acceptable Usage Policy which can be a quite small portion, of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, sound, moving images, TV broadcasts and many other media.

2. Malicious Communications Act 1988

Under this Act it is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person. Additionally under the Telecommunications Act 1984 it is a similar offence to send a telephone message, which is indecent, offensive, or threatening.

3. Computer Misuse Act 1990

This Act makes it an offence:

(i) erase or amend data or programs without authority;
(ii) to obtain unauthorised access to a computer;
(iii) to "eavesdrop" on a computer;
(iv) to make unauthorised use of computer time or facilities;
(v) maliciously to corrupt or erase data or programs;
(vi) to deny access to authorised users.

3. Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

(i) use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
(ii) display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

5. Trade Marks Act 1994

This Act provides protection for Registered Trade Marks, which can be any symbol (words or images) or even shapes of objects that are associated with a particular set of goods or services. Anyone who uses a Registered Trade Mark without permission can expose himself or herself to litigation. This can also arise from the use of a Mark that is confusingly similar to an existing Mark.

6. Data Protection Act 2018 & General Data Protection Regulation 2018

The College has a Data Protection Policy which applies to all staff and students of the

College. Any breach of the Data Protection Act 2018, the General Data Protection Regulation 2018 or the College Data Protection Policy is considered to be an offence and in that event, disciplinary procedures will apply.

6. Human Rights Act 1998

This act does not set out to deal with any particular mischief or address specifically any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the context of the College, important human rights to be aware of include:

(i) the right to a fair trial
(ii) the right to respect for private and family life, home and correspondence
(iii) freedom of thought, conscience and religion
(iv) freedom of expression
(v) freedom of assembly
(vi) prohibition of discrimination
(vii) the right to education

These rights are not absolute. The College, together with all users of its ICT services, is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations which arise from other relevant legislation.

8. Regulation of Investigatory Powers Act 2000

The Act states that it is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic (including telephone) communications to is permitted, in order to:

(i) Establish the facts;
(ii) Ascertain compliance with regulatory or self-regulatory practices or procedures;
(iii) Demonstrate standards, which are or ought to be achieved by persons using the system;
(iv) Investigate or detect unauthorised use of the communications system;
(v) Prevent or detect crime or in the interests of national security;
(vi) Ensure the effective operation of the system.
(vii) Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.

The College reserves the right to monitor e-mail, telephone, and any other communications in line with its rights under this act.

9. Freedom of Information Act 2000

The Act, intended to increase openness and transparency, obliges public bodies, including Higher Education Institutions, to disclose a wide range of information, both proactively and in response to requests from the public.

There is an obligation to disclose any recorded information held by the College which is properly requested unless this falls within very limited exemptions and circumstances.

The types of information that may be have to be found and released are wide-ranging, for example minutes recorded at a board meeting of the institution or documentation relating to important resolutions passed. Retrieval of such a range of information places a considerable burden on an institution subject to such an information request. In addition to setting a new standard of how such bodies disseminate information relating to internal affairs, the Act sets time limits by which the information requested must be made available, and confers clearly stated rights on the public, regarding such information retrieval. Therefore all staff have a responsibility to know what information they hold and where and how to locate it.

10. Communications Act 2003

This act makes it illegal to dishonestly obtain electronic communication services, such as e-mail and the World Wide Web.

11. Defamation Act 2013

It is unlawful to make an untrue statement, published to a third party, which damages the reputation of a person or company or holds them up to hatred, ridicule or contempt. It need not be obviously insulting. It could, for example, be a suggestion that a competitor is in financial difficulties or is unprofessional in the conduct of its business. Facts concerning individuals or organisations must be accurate and verifiable and views or opinions must not portray their subjects in any way that could damage their reputation.

12 Discrimination/Harassment Legislation

In general terms, harassment is unwanted conduct affecting the dignity of men and women in the workplace. It may be related to age, sex, race, disability, ethnic or national origins, political or religious beliefs and activities, or any personal characteristic of the individual.

There is a range of legislation which makes it an offence to discriminate on the grounds of the above. Harassment, such as unwelcome emails or copying of such material from the Internet, is not permitted and could result in legal action against you.

Appendix 2 – Digital Communication Code of Conduct for Students

Digital technology is powerful because once text or an image is created and made available then there is no control over what happens to it. It can be shared by others in a variety of different ways and it cannot be recalled or retrieved by the creator or sender. A personal issue between individuals can move beyond their control very quickly. The impact can continue to grow and involve others who sustain the conflict.

Students have told us that the College has a right and a responsibility to set standards and guidelines about conduct. Learners feel we should take action against those who misuse digital technologies to bully and harass their student colleagues - even if this behaviour takes place out of College and during evenings and weekends. Their view is that, if the impact of the behaviour is felt in College then we have the right and duty to act. To support students and staff in managing this problem, the College has developed a code of conduct.

• Use all digital technologies and communication with consideration for others
• If you feel you are being bullied by email, text or online then tell a member of staff. (The College will take disciplinary action where this has an impact on behaviour in the College or affects a learner's ability to succeed.)
• Never send any bullying or threatening messages. This is against the law.
• Don't reply to any bullying or threatening messages - this could make things worse because a bully is looking for a response
• Don't challenge a bully (or encourage others to challenge them) as it may make the problem
worse - report it to your tutor or support worker
• Don't give out your personal details on line - especially your email address or mobile number
• Don't forward abusive texts or messages to anyone. If they are about someone else, delete them and don't reply to the sender. If they are about you, keep them as evidence and don't reply to the sender.
• Never give out passwords to your mobile or email account
• Be careful about who you give your personal details to (email, phone, MSN) - students often get bullied by people they were friends with at one time.
• You may decide to report very serious bullying to the police after consultation with College staff - e.g. any sexual or physical threats - but please take advice first
• Keep and save any bullying texts, emails or images - it could help to identify the bully
• Keep a note of the date and time you received any messages - note any details of the sender
• Contact the service provider to tell them about the bullying - they may be able to block or identify the person responsible
• Use a different user name or ID. Change your mobile number. Stop using a chat room for a while.
• Use blocking - block instant messages from the people you don't want to hear from. You can
also use mail filters to block specific email addresses
• Don't put up with it - Get help from your tutor or support worker