Calderdale College

COMMUNICATION AND INFORMATION TECHNOLOGY POLICY

Approved by IT/HR in August 2018

AUTHOR:	**Human Resources**
DATE:	**August 2018**
VERSION	**1**

COMMUNICATION AND INFORMATION TECHNOLOGY POLICY

1 PURPOSE

This Communication and Information Security Policy has been devised to meet the following aims:

- To outline the guidelines that will govern the use of all communication tools within Calderdale College and this includes E-mail (Business & Personal), Telephone, Intranet, and any other form of communication on the College's premises.

- To encourage the correct use of these tools to facilitate effective communication and to improve efficiency within the College.

- To outline the implications in the event of misuse of any of these tools or systems which allow you to communicate throughout Calderdale College and with external parties.

- To establish eligibility for company-owned Mobile Devices based on job roles and responsibilities, and set out procedures for monitoring and controlling costs related to use of Mobile Devices in connection with College business. It also aims to outline the Mobile Device options supported by Calderdale College, guidelines for acceptable use, and other administrative issues relating to Mobile Device acquisitions and reimbursements.

The purpose of information security management is to preserve:

Confidentiality: data and information can only be seen by those authorised to see it and can only be changed by those allowed to change it

Integrity: the data is complete, accurate, up to date and relevant and the system is operating as per the specification

Availability: information and services are delivered to the right person when they are needed

Accountability: all activity can be traced back to the originator

The College recognises that staff and students will require access to systems, services and data in order to fulfil their roles and responsibilities. Therefore, appropriate procedures and controls have been put in place to enable staff and students to obtain the necessary authorised access so that they are able to carry out their work effectively and efficiently.

The College also recognises that all staff and students are required to comply with the necessary legislation in force at that time. This includes the General Data Protection Regulations 2018, the Copyright Designs and Patents Act, the Computer Misuse Act, the

Human Rights Act and the Health & Safety at Work Act. Further details are available in Appendix 1.

It should be noted that Calderdale College reserves the right to monitor the usage of email, internet activity, phone usage, resources and systems when there is potential or evidence of abuse to these services.

Any breach of this policy may lead to disciplinary action up to or including dismissal and in some cases legal action.

Failure by an individual to adhere to the College Mobile Devices procedures may result in action being taken to withdraw the mobile phone facility.

Please note this policy is not exhaustive in the different forms of communication and a sensible professional approach should be adopted at all times when communicating with colleagues internal or externally.

2 SCOPE

This Policy applies to all staff and students of Calderdale College.

In particular, the mobile devices procedure applies to all staff, contractors, consultants, temporary and other workers at Calderdale College including all personnel affiliated with third parties that maintain a Mobile Device on behalf of Calderdale College. This Policy also applies to all Mobile Devices that connect to a Calderdale College network or reside on Calderdale College sites that provide wireless connectivity including, but not limited to mobile phones, smartphones, tablets, and laptops. This includes any form of wireless communication device capable of transmitting of data.

3 DETAILS OF POLICY

3.1 PC USE

3.1.1 Access to Information

Computers are increasingly being used to both access and process information. As a result, this places certain responsibilities on you as the user of that computer or equipment, therefore:

- Avoid giving unauthorised parties access to your or other Calderdale College computer systems and/or College information (e.g. by logging out or locking your computer when you are away from your desk)

- Avoid unnecessary disclosure of information that may cause embarrassment to Calderdale College, particularly when it relates to personal, or confidential information. Information can only be given to parties authorised to access or view the information. Any information required by external organisations or agencies should first be cleared with the College Data Controller.

- Keep all passwords secure and do not divulge to anyone.

- You must only use authorised and correctly licensed software following guidance from the IT Support Unit.

- Use of Calderdale College computers for personal financial gain is not permitted. In Law, Calderdale College has the Copyright and ownership of all work done on their computers and equipment.

- Electronic copying of copyright material (written, maps, electronic or other) using Calderdale College's computerised equipment is not permitted except where allowed under licence and within the Law.

3.2 EMAIL AND INTERNET USE

The use of Calderdale College e-mail, Internet and Intranet is available for all staff and students. The following guidance should be adhered to:

- Email is recognised as a proper method of communication within Calderdale College and must not be avoided purposely if available. You are expected to reply to your daily email messages in good time and in an appropriate manner.

- Emails should not be used as a way to avoid personal communication where it is more appropriate to use face to face communication such as constructive feedback to staff.

- Email must not be used for the sending/receiving of unauthorised information, pornographic, violent, offensive, abusive, copyright infringement or sexually/racially-harassing content.

- Personal emails within work time, whilst not encouraged, are permitted during scheduled breaks only, but use of the system should be reasonable and should not impede service delivery, by taking up staff members' time or the College's resources.

- Any personal use of Internet services must not incur additional costs to the College (e.g. mass printing, downloading huge files thereby reducing bandwidth). It is accepted that over your lunch period, before and after work you can access the Internet briefly for personal interests. This should be outside your agreed working hours.

- Do not download or install unauthorised software. All software installations must be recorded and approved by the IT Support Unit, and logged into the software audit record.

- Be considerate when sending emails. Do not send personal/commercial adverts, unnecessary or junk emails. If you intend to send an email to 'All Users' for non-operational matters, this must be done via the Marketing team and College News.

- Maintenance of your mailbox is essential for effective working. Check your inbox daily or ensure that an 'out of office' reply or redirection is used when you are away. Delete messages, which are not important.

- Do not try to conduct fraudulent activities: e.g. Sending emails using other staff member email names without their knowledge, faking email names, selling illegal items over the internet, giving false details over internet to acquire goods etc.

- **Please Note**: confidentiality of information cannot be guaranteed if it is sent via email or the Internet.

3.3 SOCIAL NETWORKING (EMAILS, BLOGS & SOCIAL MEDIA)

Publication and commentary on social media carries the same obligations as any other kind of publication or commentary. All users of social media must follow the same standards of conduct that Calderdale College staff must follow.

Calderdale College is committed to the responsible use of the Internet, email and social media. The College may routinely monitor social media and it reserves the right to instruct relevant parties to remove unauthorised sites. Any information posted on social media sites must comply with the General Data Protection Regulations.

Staff must keep a professional distance and not interact with students either online, by email, by phone or by text message for non-College related purpose.

3.3.1 Communication with students

Staff are required in all communication with students to comply with the requirements of the following policies:

- Harassment and Bullying Policy
- Staff Code of Conduct
- Disciplinary Policy and Procedure
- Safeguarding Policy
- General Data Protection Regulations

3.3.2 Policy Compliance

- Use your real name, be clear who you are, and identify that you work for Calderdale College.
- Setup your Calderdale College social network site in consultation with Marketing where the site is to be used for marketing and promotional reasons. Access to the site is to be provided to Marketing.
- Ensure your profile on social media sites is consistent with your profile on the Calderdale College website or other Calderdale College publications.
- Point out any misrepresentations made about Calderdale College in the media.
- Respect your audience.

3.3.3 Unacceptable Use of Social Media

- To publish or send unsolicited advertisements, solicitations, personal commercial messages or promotional messages of any kind (known as "spam").
- To say anything that is dishonest, untrue, or misleading. What you publish will be available on the Internet for a long time, so consider the content carefully and be cautious about disclosing personal details.
- To publish or send very large messages or files that disrupts a server, account, newsgroup, or chat service.
- To post any material critical of the College or colleagues on any social media site. Any criticisms of the College or its community members must be made through Calderdale College’s internal procedures.

- To say anything contradictory or in conflict with the Calderdale College website.

- To post comments that recommend, or appear to endorse, law-breaking of any kind.

- To post comments that exhibit or appear to endorse behaviour that could be argued to encourage “copycat” behaviour by students. This would include for example, dangerous driving, alcohol or drug abuse.

- To communicate with students or parents on the Internet other than by emails sent from a…@calderdale.ac.uk address or via an official Calderdale College social media site for College communication purposes.

- To allow students to see staff members own personal social networking sites where permission is required to see those sites.

- To place yourself in a vulnerable position with a student by allowing students to become emotionally dependent on you and not taking action to stop this. This would include conversing with a student on the Internet on any matters other than those that are directly related to College business.

- To participate in using “spyware” software.

- To use any of our mail servers or another site's mail server to relay mail without the permission of the Head of IT.

- To participate in e-mail bombardment i.e. flooding someone with numerous or large e-mail messages in an attempt to disrupt them, their or our site.

- To reference any confidential information about customers, partners or suppliers without their approval.

- To publish confidential information, it is acceptable to talk about the College and have a dialogue with the community but it is unacceptable to publish confidential information. Confidential information includes things such as unpublished details about our software, details of current projects, financial information, research, etc. If you are in any doubt about whether the content of your post/email is confidential, refrain from making the posting until you discuss it with the Marketing Department at Calderdale College.

3.3.4 Process for identifying inappropriate Social Networking Sites

- Identify site and give reasons why the site is inappropriate.

- Inform Marketing/Human Resources or the relevant manager dependent on the content.

- Agreement to be given by the relevant manager and Head of IT, and where relevant, the Safeguarding Co-ordinator.

- The Marketing Department or Head of IT contacts the individual or Facebook to authorise Calderdale College’s decision to remove the Facebook Site.

3.4 AUTHORISED USE OF COMMUNICATION

The College provides you with a number of tools such as e-mail and telephones to enable you to communicate on matters directly concerned with the College. Staff using this equipment or systems should give particular attention to the following points.

- **The standard of presentation**. Please remember that during all forms of communication you are representing Calderdale College and as such a professional business-like style must be adopted at all times. All telephone, direct and e-mail communications should be treated in the same way. The standards that Calderdale College expects from written communications should be professional and business-like at all times. The official font used by Calderdale College is Arial. E-mail signatures should also be in line with the College's standard.

- **The appropriateness of e-mail**. E-mail should not be used as a substitute for face-to-face communication. "Flame-mails" (e-mails that are abusive) can be a source of stress and can damage work relationships. Hasty messages sent without proper consideration, can cause unnecessary misunderstandings.

- **The extent of circulation**. Please ensure that all communications or messages are sent to those staff members for whom they are particularly relevant. Please try and refrain from College wide communications unless agreed with your Line Manager or IT as an appropriate communication for the College.

- **The visibility of e-mail**. If the message is confidential, the user must ensure that the necessary steps are taken to protect confidentiality. The College will be liable for any defamatory information circulated either within the College or to external users of the system.

3.4.1 USER TIPS FOR DO's & DON'T's:

- Please take care of the equipment provided to you by regular cleaning, reporting any damage or faults to the IT Support Unit.

- Please follow the College procedures such as login in and off your PC under your own user sign-on and passwords.

- Do not give any one your PC password

- Please ensure that all Emails are monitored, received, dealt with and deleted (if appropriate) on a daily basis. This will help increase the efficient working of the systems.

- Please ensure that your out of office tools are kept up to date with your daily activities.

- Please do not send/forward or design emails with huge attachments such as photo's/fun mail or anything derogatory which is not meant for College purposes. If you receive anything of this nature please inform your manager and do not forward on the content. If you have a large work document please contact the IT Support Unit who will assist you in transferring this data in the most appropriate way.

3.5 UNAUTHORISED USE

Calderdale College will not tolerate the use of any communication tools or systems that are in breach of the College's policies or indeed government legislation. Below are some examples of how we would identify misuse:

- Take part in any illegal activity.
- Create, download, transmit or view data or images which are offensive, obscene, indecent or which advocate violent, illegal or discriminatory activities.
- Store, e-mail or publish comments which are defamatory to others, or which could constitute bullying or harassment or discrimination in any form.
- Excessive personal use, e.g. social invitations, personal messages, chat, jokes, cartoons, games or chain letters.
- On-line gaming or gambling.
- Downloading the Tor software bundle and accessing the Tor network using College computers and networks.
- Access chat-rooms (text or voice) or online games.
- Accessing pornography or any inappropriate materials that could cause harm, injury to feelings or break the law.
- Damage caused to College property through intentional attack, vandalism or general damage to our property.
- Downloading or distributing copyright information and/or any software available to the user.
- Allowing others to misuse your systems / equipment.
- Posting confidential information about other staff member, the College or its customers or suppliers.
- Disclose private information about other people. Please be careful about giving other people personal information about yourself – they may not be who they say they are.
- Intentionally disturbing or executing computer viruses, malicious software or creating hoax virus warnings.
- Waste College resources including disk space, paper, computer time and internet capacity by for example viewing streaming video unrelated to your work
- Any other item, which ITSU deems to be a risk to the College Computer System.
- Sending a large number of unsolicited e-mails (spamming).
- Attempt to gain unauthorised access to Calderdale College systems or external networks (Hacking)

If you receive an unauthorised email containing inappropriate materials or jokes please do not forward these onto your colleagues. Please raise any nuisance communications with

ITSU immediately so they can consider blocking this material and delete it from your machine.

3.6 MONITORING OF EMAIL AND THE INTERNET

Regular monitoring of e-mail messages and mailboxes will be carried out on an automated basis by ITSU. Hard copies of e-mail messages will be used as evidence in disciplinary proceedings.

A scanning tool, which stops mail containing designated criteria, will check all messages carrying attachments of any kind, whether incoming or outgoing and this filter is provided by a third party and is updated frequently. However, it should be noted that the College reserves the right to alter the criteria at any time without notice. The senders of e-mails with banned attachments may be subject to disciplinary action.

All e-mail messages are retained within the College for a period of 1 year, even when they have been deleted from staff Inboxes.

All e-mail users will be issued with a unique individual password, which is tied to the Windows password and is confidential to the user. Access to the e-mail system using another staff member's password without prior authorisation may result in disciplinary action.

Users must ensure that critical information is not stored solely within the e-mail system.

Please note that the College will not allow any risk of viruses, transferring of confidential or sensitive information internal or external from Calderdale College and if such information is found in the logs then IT have the College's permission to access this information/attachment to ensure that this item will not cause damage to the College.

3.6.1 Software

Only software approved, scanned for viruses and installed by ITSU is to be used on official equipment. The use of unauthorised software, including screensavers, or the unauthorised copying of any software is strictly forbidden.

3.6.2 Prevent

Prevent is part of the overall Government counter-terrorism strategy with the aim of reducing the threat to the UK from stopping people becoming terrorists or supporting terrorism. The strategy has three specific strategic objectives:

- respond to the ideological challenge of terrorism and the threat we face for those who promote it:
- prevent people from being drawn into terrorism and ensure that they are given appropriate advise and support; and
- work with institutions where there are risks of radicalisation that need to be addressed

The College is required to undertake the following as part of the Prevent Duty Guidance:

- Implement a prevent strategy in a proportionate and risk-based way

- Ensure active engagement by Governors, managers, staff and external partners including the police
- Engage and consult students on plans for implementing the duty
- Carry out a risk assessment which assess where and how students or staff may be at risk from being drawn into terrorism
- Implement staff training so staff have an understanding of the factors that make people vulnerable to being drawn into terrorism and to challenge extremist ideas.
- Have procedures for sharing information about vulnerable individuals
- Have measures in place to monitor and report suspicious use of IT systems, the internet and social media etc.

3.7 PERSONAL PHONE USAGE

3.7.1 Personal Calls

All personal calls on College phones are to be kept to a strict minimum and should only be made after seeking permission first from a line manager. It is recognised that most businesses, such as banks and medical surgeries, are only open from 9.00am to 5.30pm Monday to Friday and so it is permissible to make a brief call to them to book an appointment etc. Where possible, staff should make the call using their own personal mobile either at lunchtime or outside of their business unit's core hours.

Incoming personal calls are also similarly discouraged to College phones and staff receiving one during core business hours should ask the caller to be brief or to call back at a more convenient time

3.7.2 Personal Mobiles at Work

The use of personal mobile phones at work should be limited to scheduled break times, where possible, to avoid disruption to work. This includes the use of text messages, social media and access to online facilities. The College acknowledges that there will be occasional times for emergency calls outside of scheduled break times; we ask that these could be as brief as possible.

Calderdale College reserves the right to charge for any calls made to local, national or international numbers.

3.7.3 Monitoring of Staff Members Telephone Calls

Staff should be aware that the call traffic generated by any extension number is electronically logged by the current telephone system.

The phone system records the numbers dialled by all extensions, the duration of all calls and the time calls are made. Conversations are not recorded.

Managers will receive a log of all calls made in their departments and staff found to be frequently misusing the College's systems or equipment will be monitored and managed in line with the disciplinary policy.

All calls made by staff should obviously comply with the College Policies on bullying and harassment i.e. the telephone must not be used as a means of harassing another staff member.

Communication Skills Academy - The academy operate on a separate phone system to that of the College. Apprentices, students and staff who operate from within the Communications Skills Academy must be aware that all phone conversations are recorded and stored for training and quality purposes

3.8 COLLEGE MOBILE DEVICES

Calderdale College will, at its discretion and in accordance with this policy, provides staff with mobile devices ("Mobile Devices") and mobile provider services, at Calderdale College's expense, for the primary purpose of conducting College business. All Mobile Devices that are paid for by Calderdale College are the property of Calderdale College and the staff member is responsible for ensuring the appropriate use of the Mobile Device, as well as the security and safe keeping of the Mobile Device. For audit purposes, or in the event of lost/stolen equipment, the College reserves the right to remotely track and locate mobile devices.

This part of the policy applies to all staff, contractors, consultants, temporary and other workers at Calderdale College including all personnel affiliated with third parties that maintain a Mobile Device on behalf of Calderdale College. This Policy also applies to all Mobile Devices that connect to a Calderdale College network or reside on Calderdale College sites that provide wireless connectivity including, but not limited to mobile phones, smartphones, tablets, and laptops. This includes any form of wireless communication device capable of transmitting of data.

3.8.1 Eligibility

The College will only provide a mobile phone or device if there is an essential business need specific to the individual role.

Applications for a mobile phone must be made by completing the mobile phone application form found on the Finance Moodle page. Upon receipt of an application, Finance will seek authorisation for purchase from either the line manager and / or relevant budget holder.

Applications that are not approved will not be processed and the applicant will be informed.

3.8.2 Handsets and Usage

Mobile equipment issued by the College has to be used primarily for work-related communications. The number of calls made should be limited to those necessary for effective business. Calls should be brief. A limited range of handsets will be offered with the College's choice of mobile phone tariff and service provider. Handset allocation is determined on the basis of cost effectiveness and not personal choice. The College will redeploy College owned Mobile Devices not in use prior to ordering new devices.

Accessories such as Bluetooth headsets, are not provided by the College. Staff may, at their own expense, purchase other enhanced accessories.

Staff may be asked to justify monthly bills. The College reserves the right to make the appropriate deductions from payroll for any amounts in excess of the monthly threshold. Staff may be asked to justify specific single call charges.

College sponsored mobile phones should not normally be used for text messaging except for business purposes only. Text Messaging or SMS is provided in all packages. Text Messaging costs count towards the Fair Usage part of the College's mobile phone tariff and, therefore, text messaging should be minimised. Staff may be asked to justify the charges apportioned to text messages on the monthly bill. Only incidental personal use is allowed.

Under no circumstances should staff members make calls to premium rate numbers. International dialling from within the UK is not permitted, but this can be requested for business use via the Finance department.

Mobile Device spend will be monitored on a monthly basis, including reviewing consumption & trend analysis reports at the individual level. Mobile Device usage reports will be communicated to the individual member of staff on a monthly basis to create cost awareness.

Staff should not use the device for personal software, apps, email, web-browsing or data storage.

Use of and subscription to, premium and or interactive mobile services using a College mobile phone and tariff is strictly prohibited. This includes (but is not limited to) the downloading of ring tones, videos, applications not related for College business.

Staff may use secure corporate Wi-Fi networks at corporate locations and their Service Provider's network. Staff must never use any other public networks.

When travelling abroad not on College business, staff should be mindful that roaming charges vary considerably and are generally expensive. Signed Executive approval should be sought to take a College mobile aboard. Every effort should be made to minimise costs during that time. International Calling can be very costly and these features are only included in a select number of packages. Usage of a College phone whilst abroad should not be used if an member of staff is abroad on annual leave. Roaming and data access should be switched off.

Sim Swapping -The College does not permit the transfer of the College sim card from the supplied handset to a personal device or visa-versa. This may incur substantial costs for incorrect tariff usage and the College will seek full recompense for additional charges incurred due to this action. This type of action may cause serious security breaches where data based devices carry sensitive College information.

3.8.3 User Responsibility

Staff who hold College sponsored mobile phones are reminded that the mobile phone is company property and ultimate liability for its misuse rests with the user and the College. Calls made or text messages/images sent from the mobile phone are to be treated in the same way as e-mail technology. In other words, staff should not access, store or distribute any offensive or inappropriate (e.g. defamatory or racist) material with the mobile phone. Non-adherence to this rule will carry serious consequences, up to and possibly including dismissal.

Members of staff who are allocated a mobile device will be held responsible for the handset and all calls made and other charges incurred. It is therefore essential that devices must be kept secure at all times and use by anyone other than the named individual is prohibited.

The handset / Sim PIN code or other security locking system should always be used. Sensitive information should not be stored unsecured on a mobile device. Staff should consider the impact of retrieving their e mail on mobile devices.

Handsets that are lost or stolen must be reported immediately to the O2 Business Service Desk on 0845 741 7417 and request a temporary bar to prevent any unauthorised usage. At your earliest opportunity you must also report the event to the Finance team on extension 9348. Steps will be taken to remotely locate the device or wipe any data, in conjunction with the College IT Support Unit.

If a member of staff loses a handset then the College reserves the right to refuse to issue further devices to that individual. Equipment provided to staff that is lost, broken, or stolen may be repaired or replaced and charged to the staff members cost centre unless it is a proven defect of the equipment. Lost, broken or stolen devices must be reported to Finance immediately by either the member of staff or their manager.

If staff report a lost, broken or stolen device they may be subject to appropriate disciplinary action regarding the misuse of a company asset. This action may include a deduction from the member of staffs pay for replacement of the hardware.

Mobile devices remain the property of the College at all times and should be surrendered when a member of staff leaves employment or on demand of the Head of Unit, HR, Finance or IT.

Allowance for reasonable use is an inclusive charge and is now included in most phone tariffs as an allowance for reasonable use. Exceptional high usage charges exceeding this limit are made by the mobile service provider. Staff will no longer have to contribute £5 a month for personal usage, but if it is felt that excess charges do not represent reasonable usage, the user may be asked to refund the College.

No member of staff is to use College-owned Mobile Devices for the purpose of illegal transactions, harassment, or obscene behaviour, in accordance with other existing staff policies.

3.8.4 Contract Obligations

Having placed an order for a mobile device, the cost centre responsible enters into a 24 month contract with the service provider. The user will be issued with a device for a minimum period of 24 months. The device is available to the user as long as they remain at the College and as long as their role requires then to be available for contact outside office hours.

Users, budget holders or line managers of the original user must not under any circumstances re-allocate a mobile device to others without seeking authorisation from Finance. In the event that Finance authorise the re-allocation of a device to another individual, all elements of the contract including phone number will be transferred.

Anyone unsure of their obligations should consult Finance.

3.8.5 Managing Contracts

The cost centre budget holder for each mobile device is responsible for:

- Reviewing the ongoing requirement / eligibility for each mobile device funded from their budget
- Reviewing summary bills and addressing high call and data usage

- Consulting Finance regarding user charges

If a user changes role, responsibility for the contract will remain with the originating department unless:

- The user's Head of Department indicates that a mobile is required in their new role
- Finance are made aware of a new cost centre for charging purposes. This should be done before the user changes role
- If no details are supplied of a change in circumstances then the device will continue to be charged to the old cost centre and this cost centre will continue to carry the costs until the end of the billing period after which notification occurs or until the contract ends.

The College will not transfer ("Port") personal cell phone numbers to a College Mobile Device. Exceptions may be made if not Porting a number would negatively impact the College's customers. In addition, the College will not Port existing College mobile phone numbers between service providers. Exceptions may be made if not Porting a number would negatively impact the College's customers. The College mobile phone numbers will not be ported to personal cell phone devices.

3.8.6 Safety

Extreme care should be exercised when using mobile phones in cars. By law mobile phones can only be used when connected to a "hands free" unit. However if a telephone conversation is becoming protracted, you should stop the car in a safe place and continue the conversation. Using a hand held mobile device while driving, is not allowed by the company, as it is considered a serious risk and constitutes an offence under Road Traffic legislation. Remember that staff who are found using a hand held mobile device may receive penalty points on their licence.

Mobile phone manufacturers' manuals contain safety and operating instructions, which should be read and adhered to at all times.

The safety of College's staff is critical to our ongoing success. Therefore, when driving on college business only voice calling with hands-free equipment is permitted. When dialling a number, staff should pull over to the side of the road for safety. Staff may also use voice activated calling or pre-programmed numbers providing it does not distract from safe driving. Any other Mobile Device enabled activity that prevents a staff member from focusing on driving such as surfing the internet, text messaging, checking email, use of applications, or other activities, is prohibited. The Company requires its members of staff to adhere to all UK laws and regulations regarding the use of Mobile Devices.

Mobile phones must be kept switched on at all times during working hours and kept in the member of staff's possession. They are not to be left in the car when the car is unattended and should not be switched off, except when absolutely necessary. While in meetings, mobile phones should be switched to silent tones so as not to disrupt proceedings.

The phone's voicemail must be activated at all times.

3.9 SECURITY

If a computer and/or other related equipment have been provided for your work then you must take all reasonable steps to ensure that the equipment and information stored on there is protected from theft, accidental/malicious loss, and/or improper disclosure:

- Ensure that unauthorised persons cannot gain access to your computer by following Calderdale College's good practices e.g. always lock/log off or shutdown the computer if you are going to be away from your desk for any length of time.

- You must take any reasonable precaution to ensure that sensitive data is adequately protected. Do not save valuable data on your PC drives, save it to the network. This will ensure that it is always backed up.

- Calderdale College's computers are protected from virus infection. It is your responsibility to ensure that you do not introduce a virus to your computer by use of unauthorised data software on CD's, floppy disks or other media. Always be certain that any data you wish to share with other users is virus free. Any virus found must be reported to the IT Support Unit immediately.

- When disposing of computer media ensure that the media and data is completely destroyed by formatting and shredding.

- Computer hardware must be security marked. Report to IT items that are not. If you are concerned about the physical security of your equipment then you must refer the matter to ITSU.

3.10 IMPLEMENTATION OF THE POLICY

3.10.1 Management of the Communications and systems.

The College will appoint nominated individual(s) to be responsible for the management and monitoring of these systems, which will be ITSU/Estates & Facilities and Human Resources.

3.10.2 Monitoring of Communication systems and tools.

The College will carry out regular monitoring of all communications both internal and external to Calderdale College on a random basis. ITSU will carry this out and will highlight any breaches or concerns to Human Resources. Hard copies of e-mail messages will be used as evidence in disciplinary proceedings.

The College has systems and technologies in place which monitor, track, manage and scan all communications both internal and external to increase efficiency and to keep our systems free of misuse, viruses, inappropriate materials and any items, which could disrupt or damage the College.

3.10.3 General Data Protection Regulations.

Calderdale College will monitor emails and Internet usage and phone logs, in accordance with guidelines.

This means that the College will have due regard for confidentiality and security when monitoring information. Furthermore, we will ensure that staff have the opportunity to see and, if necessary, explain and challenge the results of any monitoring, if disciplinary action is under consideration.

All data that you hold on any computer system must be lawfully collected and held securely.

Staff may wish to take the opportunity to familiarise themselves with the requirements of the **General Data Protection Regulations** and to ensure that they operate in accordance with the requirements of them. In particular, to the sharing of personal or sensitive data to ensure an individual's data is protected/secure. Further clarification can be obtained from the General Data Protection Regulations Policy.

3.10.4 Grievances

Staff who feel that they have cause for complaint as a result of E-mail / Telephone or any College communications should raise the matter initially with their line manager and/or the Human Resources Unit. If necessary, the complaint can then be raised through the formal Grievance Procedure.

4 MONITORING

This policy will be reviewed regularly to ensure it is effective and still appropriate in all aspects.

5 RELATED POLICIES/PROCEDURES/DOCUMENTS

General Data Protections Regulations

6 POLICY REVIEW

Change(s) Made	Reason for Change

Review Date	Reviewed by:	Initial Approval by:	Final Approval by:	Next Review Date:	Review Period
Aug 2018	HR Business Partner	IT/HR	Policies and Procedures Committee	Aug 2021	2 Years

7 EQUALITY IMPACT ASSESSMENT

First Assessment Conducted by:	Date:	Final/Approved Assessment Conducted by:	Date:
HR Business Partner	August 2018	David Ellis Quality Systems Manager	19/09/2018

8 PUBLICATION

Audience:	Published:
Staff	Staff Internet

Appendix A

Legal issues

Computer Misuse Act 1990

This was introduced as a means of prosecuting individuals who commit some form of computer crime. Hacking, eavesdropping, deliberate virus attacks or malicious actions are covered. Unauthorised access to a computer is the most likely offence within Calderdale College. Only use computers and systems you are authorised to use.

The Act created three new offences:

- Unauthorised access to computer material
- Unauthorised access with intent to commit or facilitate commission of further offences
- Unauthorised modification of computer material.

Unauthorised access to computer material

This offence includes, for example, finding or guessing someone's password, then using that to get into a computer system and have a look at the data it contains. This is an offence even if no damage is done, and no files deleted or changed. The very act of accessing materials without authorisation is illegal. This offence carries a penalty of imprisonment up to six months and/or a fine.

Unauthorised access with intent to commit or facilitate commission of further offences

The key here is the addition of 'intent to commit...further offences'. It therefore includes guessing or stealing a password, and using that to access, say another person's on-line bank account and transferring their money to another account. For this offence the penalty is up to five years' imprisonment and/or a fine.

Unauthorised modification of computer material

This could include deleting files, changing the desktop set-up or introducing viruses with the intent to impair the operation of a computer, or access to programs and data. This also includes using a centre's computer to damage other computers outside the centre. This offence carries a penalty of up to five years and/or a fine.

General Data Protection Regulations

Individuals have rights about personal data recorded on computer and in manual files. Don't put personal data in the subject line of emails; be careful about including it in the body of the text. An individual can request access to his/her personal data and this includes email. There are regulations about direct marketing via email.

Copyright, Design & Patents Act 1988

It is an offence to copy or install software without the author's permission or valid licence. Downloading application software without permission or forwarding programs in attachments may put you in breach of this act. This also includes music, images, video clips and various publications. Some Internet sites will not let you copy material you find there. Take Care.

The Defamation Act 1996

Facts concerning individuals or organisations must be accurate and verifiable views or opinions must not portray their subjects in a way, which could damage their reputation. This applies to internal as well as external email. Organisations in the UK have lost court cases where internal email systems were used to defame other organisations and heavy fines were imposed.

Protection from Harassment Act 1997
Sex Discrimination Act 1975
Race Relations Act 1976

Accessing or distributing material, which may cause offence to individuals or damage Calderdale College's reputation, may lead to a prosecution under these Acts. The fact that it is electronic does not prevent action.

Human Rights Act 1998

The present Government's commitment to incorporating the European Convention on Human Rights into domestic law has led to the introduction of the Human Rights Act 1998. This Act will come into force in 2000. In future, a UK citizen would be able to assert their Convention rights through the national courts without having to take their cases to the European Court of Human Rights.

Protection of Children Act 1978;
Criminal Justice Act 1988

These Acts make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under 16 that are indecent.

Obscene Publications Act 1959

All computer material is subject to the conditions of this Act, under which it is a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it.

'Publish' has a wide meaning and is defined as including distributing, circulating, selling, giving, lending and offering for sale or for lease. It seems clear that material posted to a newsgroup or published on a World Wide Web page falls within the legal definition of publishing and is therefore covered by the Act.

Telecommunications Act 1984

The transmission of an obscene or indecent image from one computer to another via a 'public telecommunications system' is an offence under section 43 of this Act. For traditional mail, the same sort of offence is created under the Post Office Act 1953.

Appendix B
HOW TO USE SOCIAL MEDIA – GUIDELINES FOR STAFF

Background
Social media provides opportunities to staff and students for life and for learning. The term social media describes the online tools, websites and services that people use to share content, profiles, opinions, insights, experiences, perspectives and media itself. These tools include social networks, blogs, message boards, forums, podcasts, microblogs, lifestreams, virtual worlds, social bookmarking and tagging, wikis and vlogs. The feature that all these tools, websites and services have in common is that they facilitate conversations and online interactions between groups of people.

These guidelines are not intended to deter individuals from using these communication tools but are necessary to help protect staff and students and prevent them bringing the College into disrepute either inadvertently or intentionally.

The widespread use of social media such as Facebook, You Tube and Twitter raises issues for the College in terms of interactions between students and between students and staff. Students and staff may be unaware of the implications of their comments/postings. Internet interactions between staff and students have the potential to be much less professional than they would in other contexts.

These guidelines have been developed to:

- Give members of the College the tools to use social media responsibly
- Make clear to staff and students the limits of “free speech” on the Internet
- Draw clear boundaries that it would be inappropriate for staff to cross
- Lay out the potential penalties for breaking the guidelines or the attendant policies.

Mindfulness around all aspects of internet communication is recommended as it must be remembered that all communication on the Internet must be considered as in the public domain and can be difficult to remove. Therefore staff should be aware of their personal, as well as their professional, use of social media.

Social media in relation to staff

Most staff will, of course, exercise appropriate discretion but sometimes it may not be understood that there must be a clear professional distance between staff and students in the use of social media.

Staff are also referred to the following policies: Safeguarding Policy, Harassment and Bullying, Staff Code of Conduct, and the Disciplinary Policy and Procedure. These policies remind staff that they should not abuse the trust relationships they have with young people and vulnerable adults. This would include any form of sexualised or bullying conversation or comment through the medium of the Internet.

Guidelines for staff use of social media sites Setting up an official College social media presence	An official Calderdale College site is any site with Calderdale College in the title. For these sites then Calderdale College must always come first in the title, eg Calderdale College, Creative Arts. Social media identities, logon IDs and user names may not use Calderdale College's name without prior approval from the Marketing Department.
Recommended privacy settings	It is recommended that for private profiles staff members have a profile that has all privacy settings adjusted to customise and 'only me' visible but for public Calderdale College profiles then they should be open and transparent. It is recommended that default Facebook pages do not allow users to post photographs/video to the site. If staff wish visitors to the page to interact (comment/upload photos etc), there should be a justifiable reason and permission requested.
Action in event of misuse of social media sites	Any abuse of social media will be dealt with via the Disciplinary Policy and Procedure and may, in serious cases, be treated as gross misconduct resulting in summary dismissal. The College will remove/disable pages that are deemed unsuitable.

Controversial Issues
If you speak about others, make sure what you say is factual and that it does not disparage or defame that party. Avoid arguments. Make sure what you are saying is factually correct.

Disclaimers
Many social media users include a prominent disclaimer saying who they work for, but that they're not speaking officially. This is good practice and is encouraged; however, you and/or the College may still be liable for the contents. Therefore, wherever practical, you must use a disclaimer saying that while you work for / attend Calderdale College, anything you publish is your personal opinion, and does not represent the opinion of Calderdale College.

You should ensure that your profile(s) and any content you post is/are consistent with the professional image you present to other staff and students of the College.