SECTION 18:

INFORMATION GOVERNANCE

INDEX

Information Governance Code of Practice

Helping you safeguard Council information, equipment and our reputation

CONTENTS

9. Information Security Incident Management and Reporting Loss of IT Equipment

9.1 Information Security Incident Management Policy

10. Dealing with Personal Data – The Data Protection Act

10.1 Data Protection Policy
10.2 Data Protection Principles

11. Freedom of Information – Environmental Information Regulations

11.1 Freedom of Information / Environmental Information Regulations

12. Information Sharing

12.1 Information Sharing Code of Practice

13. Records Management

13.1 Records Management Policy

14. Retention and Disposal

14.1 Retention and Disposal Policy

15. Confidential Waste

15.1 Confidential Waste Policy

1. Introduction

The information that the Council holds, processes, maintains and shares with other organisations is a valuable asset that, like other important business assets, must be protected and operated in compliance with the policies and procedures set by the Council.

Information security, an integral part of information sharing, is **essential** to achieving the Council's priorities.

The management of personal information has significant implications for individuals and is subject to legal obligations under the Data Protection Act 1998. The consequences of information security failures can be costly, potentially damaging to reputation and time-consuming.

In order to maintain public confidence it is **imperative** that the Council complies with all relevant statutory legislation and any mandatory information security related standards the Council is obliged to comply with.

This Information Governance Code of Practice for Employees identifies the key policies and procedures that staff should adhere to in order to ensure that information/data held by the Council is secure, and appropriately handled in compliance with the relevant legislation.

2. Scope

This code applies to all councillors, committees, departments, partners, Council employees, contractual third parties and agents of the Council who use Calderdale Council provided ICT facilities and equipment, or have access to, or custody of, Calderdale Council information.

All users **must** understand and comply with this code of practice and are responsible for ensuring the safety and security of the Council's systems, information and data they use.

3. Compliance with this Code

Council Employees

Failure to comply with this Policy by Council employees may constitute gross misconduct and could lead to dismissal.

If employees do not understand the implications of this policy or how it may apply to them, employees must seek advice from their line manager.

All Users

Suspected illegal activities may also be reported to the Police.

For further information please refer to the following document: Information Security Policy

4. Information Classification

4.1 Information Protective Marking Policy

Key Messages	Responsibility
• All information assets, where appropriate, will be assessed and classified by the owner in accordance with the **Government Protective Marking Scheme (GPMS).**	**Heads of Service**
• Non-public information **must not be** disclosed to any other person or organisation via any insecure methods**.**	**Information owners**
• Non-public information and ICT equipment used to store and process this information, must be **stored** securely.	**All**
• Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.	**All**
• **PROTECT, RESTRICTED OR COUNCIL - CONFIDENTIAL** information **must not** be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.	**All**
• Where GCSx email is available to connect the sender and receiver of the email message, the connection is accredited to transport PROTECT and RESTRICTED **information** only.	**All GCSX account holders**

For further information please refer to the following documents:

Information Protective Marking Policy
Information Classification Guide to using the Government Protective Marking Scheme

5. Physical and Environmental Security

5.1 Physical and Environmental Security Policy

Key Messages	Responsibility
• PROTECT (IL2) or RESTRICTED (IL3) information and ICT equipment used to store and process this information, must be **stored** securely.	**All**
• Keys to all secure areas housing ICT equipment and lockable ICT cabinets are held centrally by ICT Services, as appropriate. Keys should not be stored near these secure areas or lockable cabinets.	**ICT Service** **All**
• All general computer equipment must be located in secure physical locations.	**All**
• PCs and laptops should not have data stored on the local hard drive.	**All**
• Non-electronic information must be assigned an owner and a classification. PROTECT or RESTRICTED information must have appropriate information security controls in place to protect it.	**All**
• Staff should be aware of their responsibilities in regard to the Data Protection Act.	**All**
• ICT equipment that is to be reused or disposed of must have all of its data and software erased / destroyed.	**All**

For further information please refer to the following documents:

Physical and Environmental Security Policy
Removal of ICT Equipment offsite
Secure Areas
Equipment Security
Secure disposal of ICT equipment and storage media

5.2 Protection against Malicious Code Policy

Key Messages	Responsibility
• It is said, 'Prevention is better than cure'. Good housekeeping and good procedural habits are vital and will lead to detection if a virus strikes.	**All**
• All software must be installed by Corporate ICT. Please refer to the Software installation policy for guidance.	**All**
• Do not use any external removable media on Council ICT equipment without it being virus scanned via the Corporate ICT Service Desk.	**All**
• Treat all email attachments with caution; a malicious piece of computer code could be included within the attachment.	**All**
For Further information please refer to the following detailed documents: Protection against malicious and mobile code policy Protection against malicious and mobile code - staff guide	

6. Communications and Operations

6.1 Information Security Software Installation Policy

Key Messages	Responsibility
• The installation of any software, including programs, applications, screensavers, music, games and animations, onto Council-owned PCs, laptops or servers is not permitted without the authorisation of the **Head of Business Change and Performance Management** and should be carried out only by authorised officers.	**All**
• Authorised officers will normally be those Council staff employed to provide ICT support, with the approval of the **Head of Business Change and Performance Management**	**ICT Services**
• Unauthorised changes to software **must not** be made.	**All**
• Software should not be installed on networked workstations until it has been fully tested and approved for use in the Council by the **Head of Business Change and Performance Management.**	**All** **ICT Services**
• Where software and applications are to be evaluated for work purposes it is permissible for a Council officer to install them on a workstation that is never connected to the Council's corporate network.	**All**
• Every piece of software is required to have a licence and the Council will not condone the use of any software that does not have a licence.	**All**
• The Council complies with the Federation of Software Theft procedures. Illegal reproduction of software is subject to civil damages and criminal penalties.	**ICT Services**

For further information please refer to the following document:

Software installation policy

6.2 Wireless Communications Policy

Key Messages	**Responsibility**
• The introduction and administration of wireless technologies within the Council's networking infrastructure is the responsibility of the Head of Business Change and Performance Management.	**All**
• Any use of wireless connections **must** be supported by a valid Wireless Enabled Application/Disclaimer.	**All** **ICT Service**
• Authorised wireless users must be aware of the physical security dangers (e.g. increased risk of theft) associated with working within any remote office or remote working location.	**All**

For further information please refer to the following document:

Wireless Communication Policy

7. Access Controls

7.1 Network Password Management Policy & Procedures

Key Messages	Responsibility
• All users must use **strong** passwords.	**All**
• Passwords must be protected at all times and must be changed at least every 90 days.	**All**
• User access rights must be reviewed regularly by the nominated officer within the directorate or service.	**Head of Service/ Manager**
• It is a user's responsibility to prevent their user ID (LID) and password being used to gain unauthorised access to Council systems.	**All**
• Partner agencies or 3rd party suppliers must not be given details of how to access the Council's network without permission from the Corporate Information Manager and Head of Business Change and Performance Management.	**ICTCE/ Corporate Information Manager**

For further information please refer to the following document:

Password Management Policy and Procedures

7.2 Remote and Mobile Working Policy

Key Messages	Responsibility
• It is the authorised user's responsibility to use portable electronic devices (PEDs), such as laptop computers, PDAs etc. in an acceptable way. This includes not installing software and taking due care and attention when moving portable computer devices.	**All**
• Authorised users must be aware of the physical security dangers (e.g. increased risk of theft) and risks associated with working within any remote office or mobile working location.	**All**
• It is the authorised user's responsibility to ensure that access to Council information is controlled e.g. do not disclose your passwords to anyone, or allow the device to be used to access Council systems or data by unauthorised persons.	**All**

• All Council-owned portable electronic devices must be encrypted.	**All**
• Users who work remotely must ensure that their Council PED is connected to the corporate network at least once every two weeks to enable software updates (including anti-virus) to be installed.	**All**
• Remote access to the Councils network and systems must be established by the Business Change and Performance management – Corporate ICT Service.	**Corporate ICT**
• Any authorised user accessing GCSx services or facilities, or processing GCSx information of a **Protect** (Impact Level 2) or **Restricted** (Impact Level 3) nature, **MUST** only use Council-owned equipment.	**GCSx Users**

For further information please refer to the following documents:

Remote and Mobile Working Device Policy

7.3 Removable Media Policy

Key Messages	**Responsibility**
• All data stored on removable media devices **must** be encrypted.	**All**
• It is Calderdale Council policy to discourage the use of all unencrypted removable media devices.	**All**
• The use of unencrypted removable media devices will only be granted if a valid business case is completed and authorised by the Head of Service and approved by the Head of Business Change and Performance Management.	**Head of Service/ICT Service**
• Removable media should not be the only place Council data is held, any data stored on removable media must also remain on the Corporate ICT network servers.	**All**
• Damaged or faulty removable media devices must not be used.	**All**
• Removable media devices that are no longer required, or have become damaged, must be returned to the ICT Service Desk to be disposed of securely to avoid potential data leakage.	**All**

For further information please refer to the following documents:
Removable Media Policy
Removable Media Business Case Template

7.4 Clear Desk and Screen Policy

Key Messages	Responsibility
• Protectively marked/personal information (protect (IL2) and Restricted (IL3)) must not be left on desks unattended and must be stored securely when unsupervised.	**All**
• At the end of each day, every desk should be cleared of all protectively marked/personal information.	**All**
• Protectively marked/personal information should be stored in a locked cupboard or drawer overnight and there should be nothing left on desks at the end of the working day. Boxes, folders etc. should not be stored on top of furniture, cabinets, window ledges etc.	**All**
• Nothing should be left lying on printers, photocopiers or fax machines.	**All**
• Users should ensure that screens displaying protective marked/personal information cannot be viewed by unauthorised persons.	**All**
• Users of ICT facilities are responsible for safeguarding data by ensuring that equipment is not left logged-on when unattended, and that portable equipment in their custody is not exposed to opportunistic theft.	**All**

For further information please refer to the following document:

Clear Desk and Screen Policy

7.5 Access to Council Network/Systems by External Parties Procedure

Key Messages	Responsibility
• Access requests by partner organisations require formal assessment in order to protect the Council's assets (IT hardware, networks, software and information). It is important to preserve confidentiality, integrity and availability of the Council's network and systems.	**Head of Service** **All**
• An initial partner request must complete the Access to Council Network/Systems by External Parties Business Case & Computer Security Access Agreement and Access to Council Network/Systems by External Parties ICT Information Security Questionnaire.	**Information Owners**

• Any existing partner agreements entered into requiring additional personnel or changes in access to the Council systems are required to complete the Access to Council Network/Systems by External Parties Business Case & Computer Security Access Agreement.	**Service Managers**

For further information please refer to the following documents:

Access to Council Network and Systems by External Parties Procedure
Access to Council Network and Systems by External Parties ICT Information Security Questionnaire
Access to Council Network and Systems by External Parties Business Case and Computer Security Access Agreement

7.6 Use of Council ICT Equipment outside the UK

Key Messages	Responsibility
• Any use of Council mobile technologies outside of the United Kingdom is barred by default.	**Corporate ICT**
• Authorised users must be aware of the physical security dangers e.g. potential risk from theft, accidental loss, tampering or general damage to any such device.	**All**
• If mobile services are authorised by the Head of Business Change & Performance Management for use outside the UK then users should be aware of the risks of using IT equipment abroad.	**All**

For further information please refer to the following document:
International Roaming Outside the UK

7.7 Internet Usage Policy & Procedures

Key Messages	Responsibility
• Council internet users must familiarise themselves with the detail, essence and spirit of this policy before using the Council's internet facility.	**All**
• The internet facilities provided by the Council are made available for the business purposes of the Council.	**All**
• The Council permits personal use of the internet **in your own time** (for example during your lunch break).	**All**
• Authorised users are personally responsible for the security provided by their network account logon-id and password. Users must not divulge their logon-id and password to any other person or allow another person to use their account.	**All**
• Users **must not** create, download, upload, display or knowingly access, sites that contain pornography or other material that might be deemed illegal, obscene or offensive.	**All**
• Users must assess any risks associated with internet usage and ensure that the internet is the most appropriate mechanism to use.	**All**
• **All internet activity is recorded and monitored**.	

For further information please refer to the following documents:
Internet Usage Policy

7.8 Email Usage Policy & Procedures

Key Messages	Responsibility
• All emails that are used to conduct or support official Calderdale Council business must be sent using a Council provided email account in the format of "@calderdale.gov.uk" or for GCSx "@calderdale.gcsx.gov.uk". **Non-Council** provided email accounts **must never** be used to conduct or support official Calderdale Council business.	**All**
• Emails and attachments should be protectively marked where appropriate in compliance with the Information Classification Guide to using the Government Protective Marking Scheme. Users must never allow anyone else to use their Council provided email account.	**All**
• Care must be taken by users to ensure that all emails are correctly addressed.	**All**
• All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual user. Emails held on Council equipment are considered to be corporate records as well as providing a record of staff activity with regard to email.	**All**
• Emails that evidence an action undertaken by the Council are subject to the respective retention period. Emails to be retained as records should be transferred to the approved record keeping system for that information e.g. EDRMS or structured network folders etc.	**All**
• Users are permitted to use their Council email account for personal purposes **in their own time** (any personal use in work time requires line manager authorisation).	**All**
• Users must **never** use their Council email account for inappropriate purposes.	**All**
• All users must ensure that any emails sent or received externally containing non-public information (identified as PROTECT or RESTRICTED) must be sent securely, using encryption or via GCSx. For further advice please contact the ICT Service Desk on 01422 393423. Council email addresses must not be set to automatically forward email to non-Council email addresses. In addition, automatic forwarding to internal email addresses must be considered carefully, to prevent sensitive information being forwarded inappropriately.	**All**

- Line managers must ensure that they have ‘read only’ access to their employees’ email accounts.

- **All email activity is recorded and monitored to ensure compliance with this policy.**

All Managers

For further information please refer to the following document:

Email Usage Policy

8. Information Systems Acquisition, Development and Maintenance Including Software and Encryption controls

8.1 The Use of Live Personal Data and Data Carrying a Security Classification in a Test Environment Policy

Key Messages	Responsibility
• All staff must ensure that no personal data or data carrying a PROTECT or RESTRICTED security classification is used for system testing purposes.	**All**
• Using live data in a test environment could severely compromise its confidentiality, and could possibly lead to legal action, fraud or malicious damage to the Council.	**All**
• Data used for testing can become merged with live data, leading to confusion and potential disruption to your business operations.	**All**
• If you are unsure of anything in this document you should ask for advice from the Corporate Information Manager, Democratic and Partnership Services**.**	**All**

For further information please refer to the following document:

Use of Live Personal Data and Data Carrying a Security Classification in a Test Environment

9. Information Security Incident Management and Reporting Loss of IT Equipment.

9.1 Information Security Incident Management Policy

Key Messages	Responsibility
• All staff should report any information security incidents or suspected incidents immediately to the Corporate ICT Service Desk, Business Change and Performance Management Service (01422 393423).	**All**
• The Council will maintain your anonymity when reporting an incident if you wish.	**All**
• If you are unsure of anything in this policy you should ask for advice from the Corporate Information Manager, Democratic and Partnership Services (01422 392298) or the Corporate ICT Service, Business Change and Performance Management Service (01422 393423).	**All**

For further information please refer to the following documents:
Information Security Incident Management Policy,
Information Security Incident Management and Reporting Loss of IT Equipment,
Information Governance Incident Reporting

10. Dealing with Personal Data – The Data Protection Act

10.1 Data Protection Policy

Key Messages	Responsibility
• Personal data means information which relates to a living individual who can be identified from that data or from data and other information.	**All**
• The Data Protection Act gives individuals the right to access their personal data. This is done by making a request in writing (a Subject Access Request).	**All**
• The Act applies to paper and electronic records containing personal data, meaning data which relates to living individuals who can be identified from the data.	**All**

• Everyone who handles personal data as part of their job needs to be aware of his or her responsibilities under the Data Protection Act. Individual employees are personally liable for breaches of the Act.	**All**
• If you receive a request for personal information, you must treat it as a Subject Access Request and pass it to your Access to Information Liaison Officer (AILO).	**All**

10.2 Data Protection Principles

The principles are legally enforceable and state that personal data must be:

- Processed fairly and lawfully
- Obtained for a specified purpose and shall not be processed in any manner incompatible with that process
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Not kept for longer than is necessary for that purpose or those purposes
- Processed in accordance with the rights of the data subject
- Kept secure from unauthorised and unlawful processing and be protected against accidental loss or damage
- Not transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects.

For further information please refer to the Information Management intranet pages.

11. Freedom of Information – Environmental Information Regulations

11.1 Freedom of Information / Environmental Information Policy

Key Messages	Responsibility
• The Freedom of Information Act provides for the general right of access to recorded information held by Public Authorities.	**All**
• Requests for environmental information should be dealt with under the Environmental Information Regulations.	**All**
• Freedom of Information requests must be in writing, which includes emails, and must state the name of the applicant and an address for correspondence. Requests under Environmental Information Regulations can be made verbally but it is good practice to ask for them to be confirmed in writing.	**All**
• Information which is publicly available as part of normal day to day business does not need to be requested under Freedom of Information or Environmental Information Regulations.	**All**
• If you receive a request for information, you must treat it as a request under either the Freedom of Information Act or the Environmental Information Regulations and pass it to your Access to Information Liaison Officer (AILO) or Corporate Information Manager.	**All**

For further information please refer to the Information Management intranet pages.

12. Information Sharing

12.1 Information Sharing Code of Practice

Key Messages	Responsibility
• Sharing information can bring many benefits. It can support more efficient, easier to access services. It can help to make sure that the vulnerable are given the protection they need.	**All**
• Information sharing means two or more organisations sharing information between them. This could be done by giving access to each other's information systems or by setting up a separate shared database.	**All**
• Any request to share information must be assessed in advance by the Corporate Information Manager. This is done by completing an Information Sharing Request Form.	**All**
• No information can be shared before approval has been given and so requests must be made in good time to allow assessment to take place.	**All**
• If you receive a request to share information you must complete an Information Sharing Request Form and take advice from the Corporate Information Manager. An Information Sharing Agreement and a secure transfer will be agreed.	**All**

For further information please refer to the Information Management intranet pages.

13. Records Management

13.1 Records Management Policy

Key Messages	Responsibility
• Records are information, created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transactions of business.	**All**
• Records created as part of Calderdale Council's activities are not the personal property of an individual or team; they belong to the authority as a whole and are part of corporate knowledge.	**All**

• Records must be reliable, useable and accessible. Records must have integrity, structure and context.	**All**
• Wherever possible, records should be stored electronically rather than on paper. Using electronic records reduces storage space and facilitates smarter working.	**All**

For further information please refer to the Information Management intranet pages.

14. Retention and Disposal

14.1 Retention and Disposal Policy

Key Messages	**Responsibility**
• Calderdale Council has a retention schedule for all the records it holds. It is vital that regular programmes of disposal are carried out in line with the schedule and that records of the information disposed of are kept.	**All**
• Disposal of records under the retention schedule should be a regular, business as usual, process as part of a planned and approved programme of records management.	**All**
• Infrequent and irregular patterns of destruction can lead to questions being raised as to why the authority chose to dispose of a document at a given time particularly when the records become the subject of an information request.	**All**
• Under no circumstances should records be disposed of to prevent disclosure under the Freedom of Information Act 2000. This could constitute a serious criminal offence.	**All**

For further information please refer to the Records Management Intranet Pages,

15. Confidential Waste

15.1 Confidential Waste Policy

Key Messages	Responsibility
• Confidential waste is any document / record, physical or electronic, containing any information about any person living or dead. Any document / record containing any information about the operation of council business are also considered confidential.	**All**
• Under no circumstances should confidential waste be disposed of in standard waste bins. This could constitute a breach of the Data Protection Act resulting in a fine of up to £500,000.	**All**
• The responsibility for identifying waste as confidential rests with the disposer.	**All**
• Under no circumstance should confidential waste be transferred from confidential to non-confidential waste facilities.	**All**
• Waste transfer notes must be obtained when confidential waste leaves a council building. Building Managers / Custodians are responsible for maintaining a file of waste transfer notes covering the two previous years.	**Building Managers**

For further information please refer to the Information Management intranet pages.

Glossary of Terms

Information Governance – Code of Conduct

Term	Description
Data Protection Act 1998	The UK Act of Parliament that identifies the rules that must be followed in order to protect individuals' personal data held by the Council.
Data/Information integrity	Data integrity in its broadest meaning refers to the trustworthiness of data/information over the entire life of the data/information.
Encrypted	Data encryption is a means of scrambling data so that it can only be read by the person(s) holding the key, password or pin. Without the key, password or pin the encryption cannot be broken and the data remains secure. Using the key/password or pin the encryption is de-encrypted and data is returned to its original value.
Environmental Information Regulations 2004	The Environmental Information Regulations 2004 (EIR) give rights of public access to environmental information held by public authorities.
Freedom of Information Act	The UK Act of Parliament gives individuals the right to ask any public body for all the information they have on any subject they choose.
GCSX e-mail account	The Government Connect Secure Extranet (GCSx) is a secure private network which enables secure interactions between local authorities, NHS, Police, Criminal Justice Board and central government departments such as the Department of Works & Pensions. A secure email account can be established to send emails up to the protective marking level of 'Restricted'.

Term	Description
Government Protective Marking Scheme	The Government Protective Marking Scheme is the method by which the information owner ('originator') indicates to others, the levels of protection required when handling the information in question, in terms of its sensitivity, security, storage, movement both within and outside the Council and its ultimate method of disposal. The Protective Marking System comprises five markings, however the Council only deals with four levels of information which are: **CMBC - 'Confidential' Information** Highly sensitive internal documents e.g. pending partnerships, investment strategies, plans or designs that could seriously damage the Council if such information were lost or made public. Personal information or details of vulnerable people or minors, or sensitive information relating to any person. Information classified as CMBC Confidential has very restricted distribution and must be protected at all times. Security at this level is the highest possible. **'Restricted' Information** Information that, if made public or even shared around the Council, could seriously impede the Council's operations and is considered critical to its ongoing operations. Information would include accounting information, business plans, sensitive customer information, Social Services records and similar highly sensitive data or general information about identifiable staff and citizens. Security at this level should be very high. **'Protect' Information** **Business Sensitive –** Information of a proprietary nature e.g. procedures, operational work routines, project plans, designs and specifications that define the way in which he Council operates. Security at this level is high. **Locally Sensitive –** Information not approved for general circulation outside the Council where its loss would inconvenience the Council or management, but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include internal memos, minutes of meetings and internal project reports. **Not Protectively Marked** Information that anyone is permitted to see such as planning applications, job vacancies and the library catalogue.

Term	Description
Information Governance Board	The Information Governance Board oversees the implementation and delivery of the approved Information Governance Framework and ensures the effective implementation of Information Governance into all directorates within the Council.
Information owner	The person who creates, or initiates the creation or storage of information.
Live data	Data on a system that is currently being used to process business transactions/information.
Metadata	Data held as part of an electronic file describing various properties of that computer file. For example, a picture file may contain metadata describing the type of camera used to take the picture, the resolution, the colour depth etc.
Non-public information	Information about the Council that is not known by the public and if released would have an impact on the Council's reputation.
Portable Electronic Device (PED)	Portable devices that are used to store electronic data. Examples of PEDs include laptops, tablets, smart phones, cameras, USB drives etc.
Record keeping system	A record keeping system ensures records are preserved for evidential purposes, accurate and efficient updating, timely availability and control of access to them only by authorised personnel.
Records management	The practice of maintaining the records of an organisation from the time they are created up to their eventual disposal. This may include classifying, storing, securing and destruction (or in some cases, archival preservation) of records. A record can be either a tangible object or digital information: for example, birth certificates, office documents, application data and email.
Remote Working Location	Remote working location refers to any time spent working from a location other than the normal office base. For example, the location could be a school, care centre, employee's home, community work office etc.
Retention period / retention schedule	The period of time a document should be kept or "retained". At the end of the retention period, the document is usually destroyed, which is determined by the retention schedule.
Standard naming conventions	Naming records consistently, logically and in a predictable way will distinguish similar records from one another at a glance, and by doing so will facilitate the storage and retrieval of records, which will enable users to browse file names more effectively and efficiently. Naming records according to agreed conventions should also make file naming easier for colleagues because they will not have to're-think' the process each time.

Term	Description
'Strong' password	A 'strong' password is a password that has been constructed in order that it is not easily guessed or hacked. For more information please read the Password Management Policy & Procedures.
Subject Access Request	A request made under the Data Protection Act 1998, by an individual for information held about them by an organisation.
Test data	Data which have been specifically identified for use in tests, typically of a computer program. Some data may be used in a confirmatory way, typically to verify that a given set of input to a given function produces some expected result. Other data may be used in order to challenge the ability of the program to respond to unusual, extreme, exceptional or unexpected input.
Version control	Numbering of a document to identify the version of that document. This is used to identify current and outdated versions of a particular document.

Document Control Information				
Issue No	Version 1			
Issue Date	September 2011			
Status	DRAFT			
Approved By	Information Governance Board			
Next Review Date				
Authors	Janette Pashley, Vyvian Lewis, Andrew Metcalfe, Tracie Robinson			
Service	Chief Executive/Deputy Chief Executive			
Distribution	Information Governance Board – ICT Control Environment Group – Corporate Information Manager – Tracie Robinson Business Change & Performance Management – ICT Service – Iain Bowie, Pam Plant, Forensic Team Management Auditor(Computers) – Andrew Metcalfe			
CHANGE HISTORY:-				
Rev	Rev Date	Rev By	Issue Date	Description

Internet Acceptable Usage Policy

Document Control Information	
Issue No	Version 1.4
Issue Date	March 2011
Status	FINAL
Approved By	Information Governance Board – 12 May 2011 Governance and Business Committee – 24 October 2011
Next Review Date	January 2013
Authors	Andrew Metcalfe and Janette Pashley
Service	Internal Audit and Business Change and Performance Management
Distribution	Information Governance Board ICT Control Environment Corporate Support Group Corporate Information Manager – Tracie Robinson Business Change & Performance Management – ICT Service – Pam Plant, Jon Smith Forensic Team Management Auditor(Computers) – Andrew Metcalfe

CONTENTS

Key Messages

- Council internet users must familiarise themselves with the detail, essence and spirit of this policy before using the Council's internet facility.
- The internet facilities provided by the Council are made available for the business purposes of the Council.
- The Council permits personal use of the internet **in your own time** (for example during your lunch break).
- Authorised users are personally responsible for the security provided by their network account logon-id and password. Users must not divulge their logon-id and password to any other person or allow another person to use their account.
- Users **must not** create, download, upload, display or knowingly access, sites that contain pornography or other material that might be deemed illegal, obscene or offensive.
- Users must assess any risks associated with internet usage and ensure that the internet is the most appropriate mechanism to use.
- All internet activity is recorded and monitored.
- **Failure to comply with this Policy and Procedure document may constitute gross misconduct and could lead to dismissal. Suspected illegal activities may also be reported to the Police.**

1. Policy Statement

1.1 The internet facility is made available for the business purposes of the Council. The internet service is managed and operated in a secure manner in order to protect the Council's information and users.

1.2 Council internet facilities are widely used to help manage and deliver Calderdale Council's services. Users of the Council internet should read this policy in conjunction with the Council's other Information Governance and ICTCE policies and the Council's Code of Conduct for Employees.

2. Purpose

2.1 This policy document tells you how you should use your Council internet facility. It outlines your personal responsibilities and provides guidance on the acceptable and unacceptable use of Council internet facilities.

2.2 This policy updates the Council's Policy on internet and E-Mail Usage.

3. Scope

3.1 This policy covers the Council internet facility provided by Calderdale MBC for the purpose of conducting and supporting official business activity through the Council's network infrastructure.

3.2 This policy is intended for all Calderdale MBC, Council Committees, Scrutiny Panels, Councillors, Directorates, Service areas, Partners, Employees of the Council, contractual third parties and agents of the Council who have been designated as authorised users of Council internet facilities.

4. Definition

4.1 This internet Acceptable Usage Policy should be applied at all times whenever using the Council provided internet facility. This includes access via any device including a desktop computer, laptop, smart phone or any other computing device.

4.2 Council "employees" who are using internet facilities of partner organisations are also subject to this policy and the Policy of the partner organisation. See Appendix A for further details.

5. Risk Management

5.1 Calderdale MBC recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

5.2 This policy aims to mitigate the following risks:

- Time wasting
- Data leakage
- Illegal activities
- Council reputational damage

5.3 Non-compliance with this policy could have a significant effect on the efficient operation of Council business and may result in financial loss, reputational damage and an inability to provide essential services to our customers.

6. Applying the Policy

6.1 What is the Purpose of Providing the Internet Service?

6.1.1 The internet service is primarily provided to give Council employees:

- Access to and/or provision of information that is pertinent to fulfilling the Council's business obligations.
- The capability to post updates to Council owned and/or maintained web sites.
- Electronic commerce facilities (e.g. purchasing for the Council).

6.2 Internet Access and Usage Management

6.2.1 In order to protect users and the Council, computer network access to some categories of websites are blocked (see Appendix B for a summary of blocked websites). Blocked categories will occasionally change and there will be some users who have access to some sites which are blocked for others.

6.2.2 In order to ensure that Calderdale MBC is protected adequately from the misuse of the Council provided internet facilities the following controls must be observed:

6.2.3 Acceptable Use:

Where 'work time' is stated this means the time you are working for the Council – **not just core hours.**

✓ **Use of the Council's internet facilities for work purposes.**
✓ **Use of the Council's internet facilities for personal purposes outside work times**
✓ **Use of the Council's internet facilities, with the prior approval of you manager, for personal purposes in work time**

6.2.4 Unacceptable Use:

Where 'work time' is stated this means the time you are working for the Council – **not just core hours**.

The list below gives examples of "*inappropriate*" usage but is neither exclusive nor exhaustive. *"Inappropriate"* material would include data, images, audio files or video files the transmission of which is illegal under British law, and material that is against the rules, essence and spirit of this and other Council policies.
Do Not Allow: × **Anyone else to use your internet access or provide any other person with the means to access these facilities e.g. by disclosing your user ID and password etc.**
Do Not Attempt to: × **To gain unauthorised access to (hack) any server/facility whether inside or outside the Council.**
Do Not: × **Use web-based email services such as Hotmail for Council business purposes.** × **Subscribe to or enter or utilise real time chat facilities.** × **Enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.**
Do Not Download: × **Any unauthorised programs/software, such as screen savers, onto to Council's ICT equipment.** × **Any personal media such as personal music tracks, video, images etc. onto the Council's ICT equipment.**
Do Not Knowingly × **Create, download, upload, display or access, material which is obscene, sexually explicit, offensive, defamatory, racist or homophobic in nature, or any material which is intended to cause the receiver or anyone who sees the material harassment, alarm or distress.** × **Use the facilities for any activity which is illegal or fraudulent.** × **Engage in any activity which threatens the integrity or availability of the Council's systems.** × **Infringe copyright or intellectual property rights.**
Do Not Use the: × **Facility to pursue personal business interests, such as gambling or for political purposes not directly related to your job.** × **Facilities to upload to any external website PROTECT or RESTRICTED material concerning the business/activities of the Council.** × **Facility to watch or record television programmes, as they are shown on TV, regardless of which television channel they are being received from unless this usage is for business purposes and a valid TV licence is held.** × **Facility for personal purposes in work time, UNLESS usage is in compliance with the Green Acceptable Use in Section 6.2.3 above.**

6.2.5 In order to enforce the Policy and to protect staff from inadvertently accessing inappropriate material and/or breaching the **Software Installation Policy. Appendix B** highlights the categories of websites/activities the Council's filtering software does not allow.

6.3 Personal Use of the Council's Internet Service

6.3.1 The Council permits personal use of the internet **in your own time** (for example during your lunch break).

6.3.2 **With the prior approval of your manager** the Council also permits personal use of the internet in work time.

6.3.3 The Council is not, however, responsible for any personal transactions you enter into - for example in respect of the quality, delivery or loss of items ordered. You must accept responsibility for, and keep the Council protected against, any claims, damages, losses or the like which might arise from your transaction - for example in relation to payment for the items or any personal injury or damage to property they might cause.

6.3.4 If you purchase personal goods or services via the Council's internet service you are responsible for ensuring that the information you provide shows that the transaction is being entered into by you personally and not on behalf of the Council.

6.3.5 You should ensure that personal goods and services purchased are not delivered to Council property. They **should** be delivered to your home or other personal address or if in electronic form to your home/personal PC.

6.3.6 All personal usage must be in accordance with this policy. Your computer and any data held on it are the property of Calderdale MBC and may be accessed at any time by the Council to ensure compliance with all its statutory, legal, regulatory and internal policy requirements.

6.4 Logging, Monitoring and Investigations

6.4.1 All users must be made aware that internet activity is logged and monitored.

6.4.2 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 - *SI 2000/2699* permit the Council, without further authorisation, to lawfully intercept its employees' email or telephone communications and monitor their internet access for the following purposes:

- The prevention or detection of crime
- The detection of unauthorised use of these systems (e.g. hacking)
- To check whether a communication relates to the Council
- To check compliance with internal/external rules or procedures
- To establish the existence of facts
- To check for viruses

6.4.3 Authorised users are personally responsible for the security provided by their network account logon-id and password. Users must not divulge their logon-id and password to any other person or allow another person to use their account.

6.4.4 Where a line manager suspects misuse of the internet facility, further advice must be obtained from the officer designated as the Directorate Responsible Officer (for Anti-Fraud and Corruption). **If any serious abuse or criminal activity is suspected the Management Auditor (Investigations) must be informed immediately (01422 393593).**

Under no circumstance should a line manager attempt an investigation without obtaining advice.

6.4.5 Interrogation of internet activity logs will **only** be carried out where proper considerations of the merits of an investigation have been assessed. This will include a full and proper assessment of necessity and proportionality and consideration by the Head of the Forensics Team. Investigations will only be carried out where the actions are fully documented and have been authorised by the Head of the Forensics Team.

6.5 Authorised User Responsibilities

6.5.1 Authorised users must:

- Familiarise themselves with this policy before using the internet facility provided for their work.
- Assess any risks associated with internet usage and ensure that the internet is the most appropriate mechanism to use.
- Know that you may only use the Council's internet facility within the terms described herein.
- Read and abide by the policies detailed in Section 9.

6.6 Line Manager Responsibilities

6.6.1 It is the responsibility of Line Managers to ensure that the use of the Council's internet facility is in line with this policy and:

- Within an authorised user's work time is relevant and appropriate to the Council's business and within the context of the user's responsibilities.
- When used within an authorised user's own time is subject to the rules contained within this policy.
- Only approve personal usage of the facility in work time where there are exceptional circumstances and the length of time using the facility is minimal and justified.

6.6.2 Line Managers must also ensure that, for any Council building where television receiving equipment (e.g. TV's, computers, laptops, tablets, mobile phones etc.) is used to watch or record television programmes as they are being shown on TV, **a valid TV licence is held**. This applies regardless of which television channels are being received or how those channels are received and includes services provided over the Internet.

Please note that it is a criminal offence to watch or record television programmes as they are being shown on any channel and on any broadcast platform (terrestrial, satellite, cable and the internet) without a valid TV licence. This is mandated by law under the Communications Act 2003 and Communications (Television Licensing) Regulations 2004 (as amended).

6.7 Whom Should I Ask If I Have Any Questions?

6.7.1 In the first instance you should refer questions about this policy to your Line Manager.

6.7.2 You should refer technical queries about the Council's internet service to the ICTServiceHelpDesk Tel: 01422(393423) or email **icthelpdesk@calderdale.gov.uk**.

6.8 Acceptable Usage Policy

6.8.1 Each user must read, understand and verify that they have read and accepted this policy.

6.8.2 A screen requiring users to confirm this will be displayed each day on first use of the internet. This screen requires positive confirmation of compliance with the Policy before the user can proceed to the internet see **Appendix C**.

6.8.3 In addition each workstation displays a 'Conditions of Use' message that requires positive confirmation that the user will comply with this and other associated policies. Users **must only press the OK button and continue** to sign on to their Council computer where they agree to comply with the conditions of use. See **Appendix A** for 'Conditions of Use' Message.

7. Policy Compliance

7.1 **Failure to comply with this Policy may constitute gross misconduct and could lead to dismissal. Suspected illegal activities may also be reported to the Police.**

7.2 **If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager.**

8 Review

8.1 The Corporate Lead for HR is the owner of this document and is responsible for ensuring that this document is reviewed on an annual basis.

8.2 A current version of this document and related documents will be available to all members of staff on the corporate intranet.

8.3 This document has been approved by the Information Governance Board on 12th May 2011 and the Governance and Business Committee on the 24 October 2011 and is issued on a version controlled basis.

8.5 The Governance and Business Committee agreed on the 24 October 2011 that the Corporate Lead for HR be authorised to agree any future minor/housekeeping changes required to the internet and e-mail usage policies, with any proposed major/fundamental changes being referred to the Government and Business Committee for approval.

9. Associated References

The following Calderdale documents are directly relevant to this policy:

- Email Usage Policy & Procedures
- ICT Code of Practice for Employees
- ICTCE Standard on the Download of Software
- Remote and Mobile Working Device Policy
- Physical & Environmental Security Policy
- ICT Information Security Incident Reporting Procedure.
- ICT Information Security Incident Management Procedures
- Information Governance Incident Reporting - Breach of Non-Technical Data
- Anti Fraud & Corruption Strategy
- Whistle Blowing Policy
- Data Protection Policy

10. List of Appendices

Appendix A – Conditions of Use Message

Appendix B – Internet Filtering Controls

Appendix C – Internet Warning Message

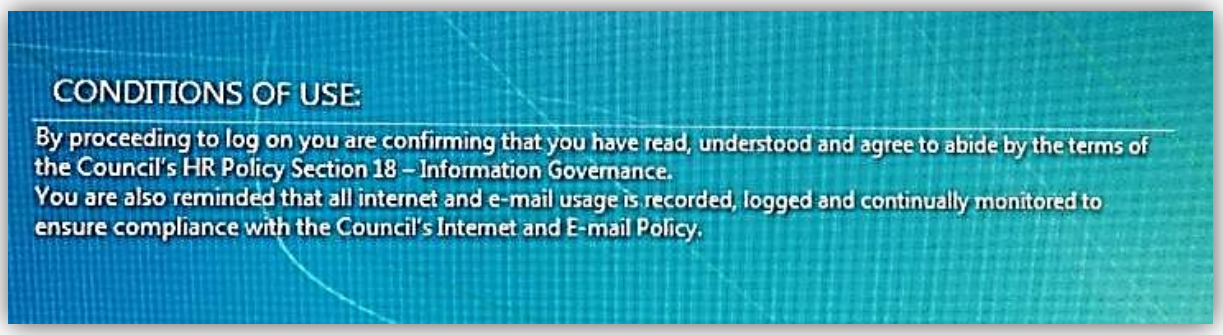
11. Change History

Rev	Rev Date	Rev By	Issue Date	Description
1.0	*December 2004*		*December 2004*	*Internet Warning Message*
1.0	*December 2004*	*Standards Committee*	*December 2004*	*Internet filtering Configuration*
1.0	*September 2006*	*S Westbrook*	*September 2006*	*ICTCE Standard Internet Filtering*
1.1	*October 2006*	*S Westbrook*	*October 2006*	*Amendments following discussion*
1.2.1 *1.2* *1.3*	*May 2007*		*May 2007*	*Policy on Internet and E-Mail Usage Email & Internet Usage*
	January 2011	*Andrew Metcalfe/Janette Pashley*	*February 2011*	*Review the current policy/standard documentation to produce one document within a standard format*
1.4	*Feb 2011*	*Bob Wright/Iain Bowie/S Milner/T Robinson/C Yates*	*Feb 2011*	*Suggested amendments incorporated by AM.*
1.4	*12th May 2011*	*Information Governance Board*	*May 2011*	*Approved for Submission to Members for Approval.*
1.4	*24 November 2011*	*A Metcalfe*	*Nov 2011*	*Amended to reflect approval at the Council's Governance and Business Committee.*
1.4	*27 January 2012*	*A Metcalfe*	*Jan 2012*	*Slight amendments to grammar per recommendations from Communications Section. No changes to content or meaning of the document.*
1.4	*20 January 2015*	*Janette Pashley*	*Jan 2015*	*Additional paragraph added to section 6.2.4 and additional point added 6.6.2 to take into account the need for a TV License when watching TV on a computer, laptop or mobile phone.*

Appendix A

Conditions of Use Message

The following Conditions of Use message will be displayed at each log-on to a Council PC or Laptop.



Internet Filtering Controls

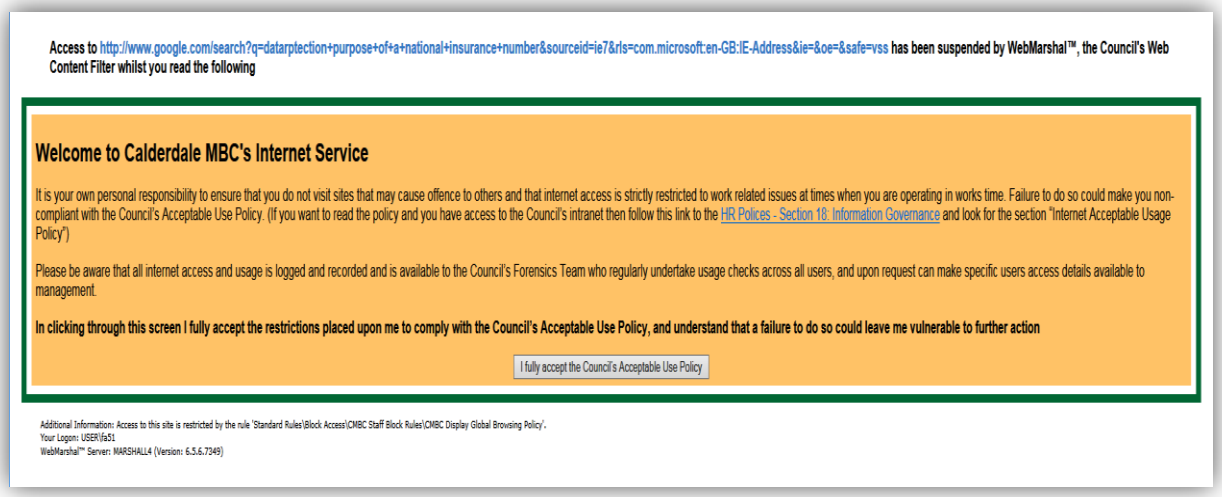
Appendix B

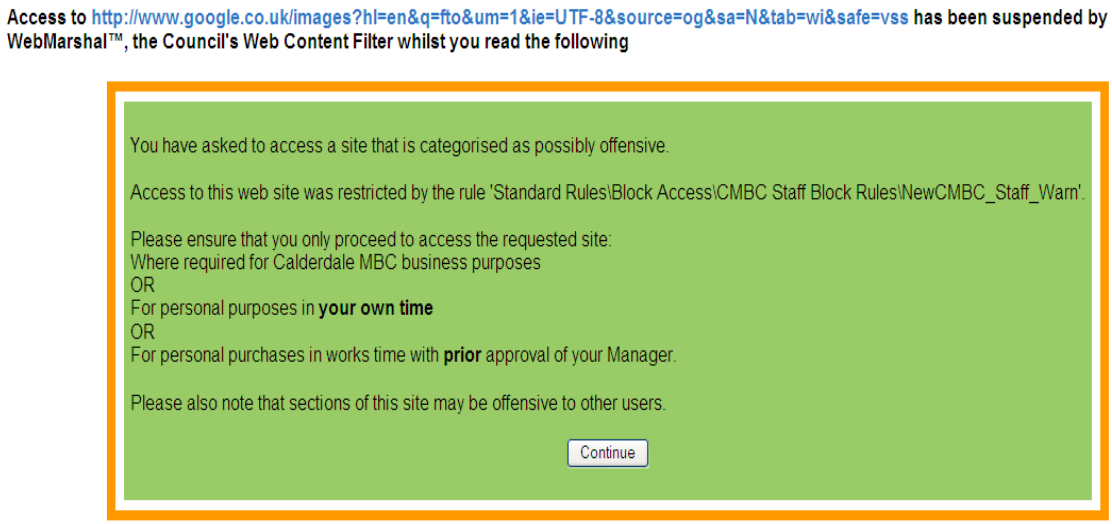
CMBC INTERNET FILTER SCHEME (23/2/2010)			
Internet and Email Usage Policy/ICTCE Standard Ref.	**Main Category**	**Sub Category**	**Employees**
Sexually explicit material	Adult Content	Child Pornography	BLOCK
	Adult Content	Explicit Art	BLOCK
	Adult Content	Pornography/Adult Content	BLOCK
	Adult Content	R Rated	BLOCK
Illegal material activity (including hacking)	Ilegal/Questionable	Criminal Skills	BLOCK
	Security	Hacking	BLOCK
	Security	Malicious Code/Virus	BLOCK
	Security	Phishing	BLOCK
	Security	Spyware	BLOCK
	Security	Botnet	BLOCK
	Security	Bad Reputation Domains	BLOCK
	Ilegal/Questionable	Illegal Drugs	BLOCK
Fraudulent material /activity	Security	Web Based Proxies	BLOCK
Obscene material	Adult Content	Obscene/Tasteless	BLOCK
	Ilegal/Questionable	Terrorist/Militant/Extremist	BLOCK
	Adult Content	Obscene/Tasteless	BLOCK
	Ilegal/Questionable	Dubious/Unsavory	BLOCK
	Society/Lifestyles	Weapons	BLOCK
Racist/Homophobic material	Ilegal/Questionable	Hate & Discrimination	BLOCK
Gambling	Entertainment	Gambling	BLOCK
Activity (knowingly engaged in) which may threaten the integrity or availability of the Councils systems.			WARN D
Infringing intellectual property rights/ copyright	Ilegal/Questionable	School Cheating	BLOCK
Breach of the ICTCE Standard: "The Installation			WARN D
Activities which could be used to circumvent filtering rules (not specifically mentioned in Policy)	Internet Communication?	Chat	BLOCK
	Infornation Technology	Web-based Newsgroups	WARN C
KEY:			
BLOCK = Site not accessible			
WARN C = Warning message displayed that content could be offensive to some			
WARN D = Media download Warning message			
The URL filters are backed up by text based filters, where one is available e.g. for pornography etc.			

Appendix C

Internet Warning Message

The following messages will be displayed when you access the internet. The specific messages will depend on the time of day and particular sites you try to access.





Access to http://www.apple.com/itunes/ has been suspended by WebMarshal™, the Council's Web Content Filter whilst you read the following

You have asked to go to site that provides downloads of software and/or media. You may not be able to install any software you download. Attemptint to install or installing any non standard Software breaches the ICT CE policy.

Access to this web site was restricted by the rule 'Standard Rules\Block Access\CMBC Staff Block Rules\CMBC_Staff_Media_Warn'.

Please ensure that you only proceed to access the requested site:
Where required for Calderdale MBC business purposes
OR
For personal purposes in **your own time**
OR
For personal purchases in works time with **prior** approval of your Manager.

Please also note that sections of this site may be offensive to other users.

Continue

Calderdale Council

Your Attempt to Access to http://www.playboy.com/ has been blocked by WebMarshal™ - The Council's Web content Filter

SITE BLOCKED

Access to this site is currently blocked according to the Council's policy.

If you wish to check why this site has been blocked this click here for the Site Checker.
Enter the URL shown above (the blue text), in the URL box on the page that is displayed.

If you believe that this site has been blocked in error, please provide relevant details (including the site name), via your Head of Service, to the Forensics Group (forensics@calderdale.gov.uk)

Your attempt to access this site has been recorded.

Internet Acceptable Use Policy (2015)
Quick Reference Guide

The following is a quick reference guide to the key points and details of appropriate and inappropriate usage. Further information can be found in the full version of the Internet Acceptable Usage Policy document available on the Council's Intranet.

Key Messages:

> Council internet users must familiarise themselves with the detail, essence and spirit of this policy before using the Council's Internet facility.
> The internet facilities provided by the Council are made available for the business purposes of the Council.
> The Council permits personal use of the internet **in your own time** (for example during your lunch break).
> Authorised users are personally responsible for the security provided by their network account logon-id and password. Users must not divulge their logon-id and password to any other person or allow another person to use their account.
> Users **must not** create, download, upload, display or knowingly access, sites that contain pornography or other material that might be deemed illegal, obscene or offensive.
> Users must assess any risks associated with internet usage and ensure that the internet is the most appropriate mechanism to use.
> All internet activity is recorded and monitored.
> **Failure to comply with this Policy and Procedure document may constitute gross misconduct and could lead to dismissal. Suspected illegal activities may also be reported to the Police.**

Appropriate Usage

✓ Use of the Council's internet facilities for work purposes.
✓ Use of the Council's internet facilities for personal purposes outside work times
✓ Use of the Council's internet facilities, with the prior approval of you manager, for personal purposes in work time

Where 'work time' is stated this means the time you are working for the Council – **not just core hours.**

Inappropriate Usage

The list below gives examples of "*inappropriate*" usage but is neither exclusive nor exhaustive. *"Inappropriate"* material would include data, images, audio files or video files the transmission of which is illegal under British law, and material that is against the rules, essence and spirit of this and other Council policies.

Do Not Allow:

× Anyone else to use your internet access or provide any other person with the means to access these facilities e.g. by disclosing your user ID and password etc.

Do Not Attempt to:

× Gain unauthorised access to (hack) any server/facility whether inside or outside the Council.

Do Not:

× Use web-based email services such as Hotmail for Council business purposes.
× Subscribe to or enter or utilise real time chat facilities.
× Enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.

Do Not Download:

× Any unauthorised programs/software, such as screen savers, onto to Council's ICT equipment.
× Any personal media such as personal music tracks, video, images etc. onto the Council's ICT equipment.

Do Not Knowingly:

× Create, download, upload, display or access, material which is obscene, sexually explicit, offensive, defamatory, racist or homophobic in nature, or any material which is intended to cause the receiver or anyone who sees the material harassment, alarm or distress.
× Use the facilities for any activity which is illegal or fraudulent.
× Engage in any activity which threatens the integrity or availability of the Council's systems.
× Infringe copyright or intellectual property rights.

Do Not Use the:

× Facility to pursue personal business interests, such as gambling or for political purposes not directly related to your job.
× Facilities to upload to any external website PROTECT or RESTRICTED material concerning the business/activities of the Council.
× Facility to watch or record television programmes, as they are shown on TV, regardless of which television channel they are being received from unless this usage is for business purposes and a valid TV licence is held.
× Facility for personal purposes in work time, UNLESS usage is in compliance with the Green Acceptable Use in Section above.

Where 'work time' is stated this means the time you are working for the Council – **not just core hours.**

Email Usage Policy & Procedures

CONTENTS

Key Messages

- All emails that are used to conduct or support official Calderdale Council business must be sent using a Council provided email account in the format of "@calderdale.gov.uk" or for GCSx "@calderdale.gcsx.gov.uk". **Non-Council** provided email accounts **must never** be used to conduct or support official Calderdale Council business.
- Emails and attachments should be protectively marked where appropriate in compliance with the Guide to using the Government Protective Marking Scheme.
- Users must never allow anyone else to use their Council provided email account.
- Care must be taken by users to ensure that all emails are correctly addressed.
- All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual user. Emails held on Council equipment are considered to be corporate records as well as providing a record of staff activity with regard to email.
- Emails that evidence an action undertaken by the Council are subject to the respective retention period. Emails to be retained as records should be transferred to the approved record keeping system for that information e.g. EDRMS or structured network folders etc.
- Users are permitted to use their Council email account for personal purposes **in their own time** (any personal use in works time requires line manager authorisation).
- Users must **never** use their Council email account for inappropriate purposes.
- All users must ensure that any emails sent or received externally containing non-public information (identified as PROTECT or RESTRICTED) must be sent securely, using encryption or via GCSx. For further advice please contact the ICT Service Desk on 01422 393423.
- Council email addresses must not be set to automatically forward email to non-Council email addresses. In addition, automatic forwarding to internal email addresses must be considered carefully, to prevent sensitive information being forwarded inappropriately.

  Auto forward received emails from any non-Council email account to your Council email account.
- Line managers must ensure that they have 'read only' access to their employees email accounts.
- All email activity is recorded and monitored to ensure compliance with this policy.

- **Failure to comply with this Policy and Procedure document may constitute gross misconduct and could lead to dismissal. Suspected illegal activities may also be reported to the Police.**

1. Policy Statement

1.1 The Council encourages users to make effective use of email. Such use must always be lawful. The use of email must not compromise the Council's information and computer systems/networks.

1.2 Users should read this policy in conjunction with the Council's other Information Governance and ICT Control Environment policies and the Council's Code of Conduct for employees.

2. Purpose

2.1 The purpose of this Policy is to provide guidance about acceptable and unacceptable use, regarding the sending or receiving email messages and attachments by:-

- Providing standards that users are expected to observe when using email, and ensuring that users are aware of the legal consequences attached to inappropriate use of Council email facilities.
- Setting down the actions that may be taken to monitor the effectiveness of this policy.
- Warning users about the consequences of inappropriate use of the email service.

2.2 This policy updates and replaces the Council's Policy on Internet and Email Usage.

3. Scope

3.1 This policy covers all email systems and facilities that are provided by Calderdale Council for the purpose of conducting and supporting official business activity through the Council's network infrastructure and portable computer devices.

3.2 This policy is intended for all Calderdale Council, Council Committees, Scrutiny Panels, Councillors, Directorates, Service areas, Partners, Employees of the Council, contractual third parties and agents of the Council who have been designated as authorised users of the Council's email facilities.

4. Definition

4.1 All emails prepared and sent from Calderdale Council email addresses or mailboxes using ICT facilities are subject to this policy.

5. Risk Management

5.1 Calderdale Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

5.2 This policy aims to mitigate the following risks:

- Data Leakage.
- Illegal activities.
- Potential legal action against the Council or individuals as a result of information loss or misuse.

5.3 Non-compliance with this policy could have a significant effect on the efficient operation of Council business and may result in breach of confidentiality, financial loss, reputation damage and an inability to provide essential services to our customers.

6. Applying the Policy

6.1 Email as a Form of Communication

6.1.1 Email is designed to be an open and transparent method of communicating. It cannot however be guaranteed that the message will be received or read, nor that the content will be understood in the way that the sender of the email intended. It is therefore **the responsibility** of the person sending an email to decide whether email is the most appropriately secure method to use.

6.1.2 Email must not be considered to be any less formal than memos or letters that are sent out from a particular service or the Council. When sending external email, care should be taken to ensure that the email does not contain any non-public information identified as PROTECT or RESTRICTED which would reflect poorly on the Council's reputation or its relationship with customers, clients or business partners. Such information must be sent securely, using encryption (Sec 6 process) or via GCSx mail. For further advice please contact the ICT Service Help Desk Tel 01422 393423. Also refer to Appendix B for further guidance on email usage.

6.2 Use of Email Facilities

6.2.1 All emails sent to conduct or support official Calderdale Council business must comply with relevant Council policies and the law.

6.2.2 Emails held on Council equipment are considered to be corporate records as well as providing a record of staff activity with regard to email.

6.2.3 Emails that evidence an action undertaken by the Council are subject to the respective retention period. Emails to be retained as records should be transferred to the approved record keeping system for that information e.g. EDRMS or structured network folders etc.

6.2.4 Non-work email accounts **must not** be used to conduct or support official Calderdale Council business.

6.2.5 Users should be aware that deletion of email from individual accounts does not necessarily result in permanent deletion from the Council's ICT systems

6.2.6 Under no circumstances should users communicate material (either internally or externally), which does not comply with the Council's Equality and Diversity Policy, or which could reasonably be anticipated to be considered inappropriate or in breach of the Council's Code of Conduct. Any user, who is unclear about the appropriateness of any material, should consult their Line Manager prior to commencing any associated activity or process.

6.2.7 The legal status of an email message is similar to any other form of written communication. Consequently, any email message sent from a facility provided to conduct or support official Calderdale Council business should be considered to be an official communication from the Council. In order to ensure that Calderdale Council is protected adequately from misuse of email, the following controls must be followed:

6.2.8 **Acceptable Use**

Where 'work time' is stated this means the time you are working for the Council – **not just core hours.**

You may:

- ✓ **Use Council email facilities for personal purposes outside work time.**
- ✓ **Open personal emails received in your Council email account in work time.**
- ✓ **Use the facilities, with the prior approval of your manager, for personal purposes in work time.**

6.2.9 Unacceptable Use

Where 'work time' is stated this means the time you are working for the Council – **not just core hours.**

The list below gives examples of "inappropriate" usage but is neither exclusive nor exhaustive. "Inappropriate" material would include data, images, audio files or video files the transmission of which is illegal under British law, and material that is against the rules, essence and spirit of this and other Council policies.

Do Not Allow:

- × **Anyone else to use your email account or provide any other person with the means to access your email account e.g. by disclosing your user ID and password etc.**
- ×

Do Not Carry out:

- × **Unauthorised transmissions to a third party of non-public information identified as PROTECT or RESTRICTED information concerning the activities of the Council.**
- ×

Do Not Create or Transmit:

- × **Any material that includes false claims of a deceptive nature.**
- × **Any material or anonymous messages - i.e. without clear identification of the sender which could bring the Council into disrepute.**
- × **Unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.**
- × **Any so-called 'flame–mail' - i.e. the use of impolite terms or language, including offensive or condescending terms.**

Do Not Knowingly:

- **View, send or receive any offensive abusive, obscene or indecent images, data, or other material, or any data capable of producing obscene or indecent images or material which is likely to cause annoyance, inconvenience or needless anxiety.**
- **View, send or receive material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, and disability, political or religious beliefs.**
- **Engage in any activity that corrupts or destroys other users' data or disrupts the work of other users.**
- **Engage in any activity that unreasonably wastes staff effort or use networked resources, or activities that unreasonably serve to deny the service to other users.**
- **Infringe copyright or intellectual property rights.**
- **Use the facilities for any activity, which is illegal or fraudulent.**
- **Make statements or derogatory remarks purporting to represent the Council when they are personal views.**
- **Use an automatic forwarding rule that sends any received emails from your Council email account (@calderdale.gov.uk) to an external email address.**
- **Set emails to auto-forward to your Council email account from a non-council email account.**
- **Use the email facility to receive or save any personal files such as programs/applications, music or animations or images etc.**

Do Not Publish:

- **To others the text of messages written on a one-to-one basis, without the prior express consent of the author.**

Do Not Use or Attempt to Use email:

- **For personal purposes in works time, UNLESS it is in compliance with the Green – Acceptable Use section above.**
- **To make Libellous statements about individuals or other organisations or use email to engage in gossip.**
- **To violate the privacy of other users or to unfairly criticise individuals.**

6.2.10 Filtering

In order to enforce the Policy and to protect staff from receiving inappropriate material and/or breaching the **Council's Software Installation Policy** the following activities are filtered using automated email scanning software cover:

- SPAM
- Pornographic images
- Offensive language

- Attachments that breach the Software Installation Policy e.g. Executable programs, etc.

6.3 Categorisation of Messages

6.3.1 When creating an email, the information and associated attachments contained within must be assessed in order to determine if the data is non-public information (identified as PROTECT OR RESTRICTED). Such data should be classified by the owner, when appropriate, in accordance with the Council's Information Protection Marking Policy and Guide to Using the Government Protective Marking Scheme. **NB: Only emails on the GCSx network require a protective mark to be applied under current Council Policy.**

6.4 Legal Consequences of Misuse of Email Facilities.

6.4.1. In a growing number of cases involving the civil or criminal law, email messages (deleted or otherwise) are produced as evidence in a permanent written form.

6.4.2 There are a number of areas of law which apply to the use of email and which could involve the liability of users or the Council. These include the following.

- **Intellectual property** – anyone who uses email to send or receive any material that may infringe the intellectual property rights of a third party.

- **Obscenity** – A criminal offence is committed if a person publishes any material which is pornographic, excessively violent or which comes under the provision of the Obscene Publications Act 1959 and/or the Protection of Children Act 1978, which makes it a offence to publish or distribute obscene material of a child.

- **Defamation** - Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredits an identifiable individual rests with the sender of the email and may lead to substantial financial penalties being imposed.

- **Data Protection** – processing information which contains personal data about individuals requires the express written consent of those individuals. Any use of personal data beyond that registered with the Information Commissioners will be illegal.

  Email and attachments may be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000. Further information regarding this can be obtained from the Council's Corporate Information Manager Tel 01422 392298 or email tracie.robinson@calderdale.gov.uk.

- **Discrimination** – any material disseminated which is discriminatory or encourages discrimination may be unlawful under the Equality Act 2010, where it involves discrimination on the grounds of sex, race or disability.

6.5 SPAM/Junk Mail

6.5.1 There may be instances where a user will receive unsolicited mass junk email or spam. It is advised that users delete such messages without reading them. **Do not reply to the email.** Even attempting to remove the email address from the distribution list, using the link on the email, can confirm the existence of a 'live' email address and result in receipt of further SPAM emails.

6.5.2 Before giving your email address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the benefits outweigh the potential problems.

6.5.3 Chain letter emails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) **must not** be forwarded using Calderdale Council's systems or facilities.

6.6 Mail Box Size

6.6.1 In order to ensure that the systems enabling email are available and perform to their optimum, users should endeavour to avoid sending unnecessary messages.

6.6.2 Users are provided with a limited mail box size of **256 MB** to reduce problems associated with server capacity. Email users should manage their email accounts to remain within the limit, ensuring that items are filed or deleted as appropriate to avoid any deterioration in systems.

6.6.3 Email messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists should be sent rather than a copy of the file. This is to avoid excessive use of the system and avoids filling to capacity another person's mailbox.

6.7 Access to another User's email account

6.7.1 Line managers are responsible for ensuring that they have **read-only** access to the email accounts of users under their supervision.

6.7.2 Access to another user's email account by another colleague is also allowed, providing there are legitimate business purposes and the access has been authorised by the line manager.

6.7.3 Accessing another user's email account must only be done **where absolutely necessary** and must be carried out with due regard to the rights and freedoms of the employee. Managers/authorised colleagues must only open emails which are relevant to the Council's business i.e.:

Managers/authorised colleagues are permitted to:

- Open emails that are clearly business related.
- Open emails where it is not possible to identify whether they are business related or personal. This must, however, only be for the purpose of ascertaining whether they are business related or not.

Managers/authorised colleagues **MUST NOT**:

- Open any emails that are clearly of a personal nature. If in doubt, advice should be obtained from the Council's Corporate Information Manager Tel 01422 392298 or email tracie.robinson@calderdale.gov.uk **prior** to opening the email.

6.7.4 The access permitted to the user's email account must be **read-only** unless additional access has been specifically authorised by the relevant Director/Head of Service.

6.7.5 Access should be to the Inbox, Sent Items and any folders that the user has created.

6.7.6 The Manager/Colleague must ensure the preview pane and auto preview is turned off when accessing other user's folders to prevent inadvertent automatic opening of potentially personal emails.

6.7.7 Technical advice on setting read-only access can be obtained from Business Change & Performance Management - ICT Service Help Desk Tel 01422 393423. Or email icthelpdesk@calderdale.gov.uk

6.7.8 Access in Respect of Leavers

(a) Where a member of staff leaves, the line manager is responsible for ensuring the user deletes any personal emails from their email account and forwards any relevant work emails where necessary to an appropriate nominated employee before they leave. The manager must make it clear to the employee that any remaining emails will be available to any new owner of the LID (username).

(b) In exceptional circumstances (e.g. instant dismissal, death in service, retirement on health grounds etc.), and on specific request by the Head of Service to Business Change and Performance Management – ICT Service, an email account may be left 'live' for an agreed period of time in order that the line manager can identify and extract any required business emails from the users account. The restrictions at 6.7.3 must still be observed.

6.8 Logging, Monitoring and Investigations

6.8.1 All users must be made aware that email activity is logged and monitored.

6.8.2 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 - *SI 2000/2699* permit the Council, without further authorisation, to lawfully intercept its employees' email or telephone communications and monitor their internet access for the following purposes:

- The prevention or detection of crime
- The detection of unauthorised use of these systems (e.g. hacking)
- To check whether a communication relates to the Council
- To check compliance with internal/external rules or procedures
- To establish the existence of facts
- To check for viruses

6.8.3 Authorised users are personally responsible for the security provided by their network account logon-id and password. Users must not divulge their logon-id and password to any other person or allow another person to use their account.

6.8.4 Where a line manager suspects misuse of the email facility, further advice must be obtained from the officer designated as the Directorate Responsible Officer (for Anti-Fraud and Corruption). **If any serious abuse or criminal activity is suspected the Management Auditor (Investigations) must be informed immediately (01422 393593).**

Under no circumstance should a line manager attempt an investigation without obtaining advice.

6.8.5 Interrogation of email activity logs and/or email contents will **only** be carried out where proper considerations of the merits of an investigation have been assessed. This will include a full and proper assessment of necessity and proportionality and consideration by the Head of the Forensics Team. Investigations will only be carried out where the actions are fully documented and have been authorised by the Head of the Forensics Team.

6.9 Security

6.9.1 Emails sent between calderdale.gov.uk addresses are held within the same network and are deemed to be secure along with the use of GCSx email accounts. However, emails that are sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system. See section 6.1.2 of this document for further guidance on how to address this risk.

6.10 Confidentiality

6.10.1 The law, the Code of Conduct for Council Employees and Council Policies requires that information which, is non-public is **not** to be disclosed to third parties. If any member of staff is unsure as to whether to pass information on or not, they should consult the Council's Corporate Information Manager (Tel 01422 392298) for further guidance

6.10.2 Staff must make every effort to ensure that the confidentiality of email is appropriately maintained. Staff should be aware that a message is not deleted from the system until all recipients of the message, and of any forwarded or attached copies, have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent via outside networks, such as the Internet, because of the insecure nature of such networks and the number of people to whom the messages can be freely circulated without the knowledge of the sender.

6.10.3 All emails must be properly addressed, especially when it contains non-public information. Authorised users must check addresses carefully before clicking "Send".

6.10.4 All official external emails carry the official Council disclaimer (see Appendix A).

6.11 Negligent Virus Transmission

6.11.1 Computer viruses are easily transmitted via email. If any user has concerns about possible virus transmission, they must report the concern to the ICT Service Help Desk Tel 01422 393423.

6.11.2 In particular, users:

MUST:-

- Ensure that ICT mobile equipment such as laptops are connected to the ICT network on a two weekly basis in order for regular anti-virus updates to be installed.
- Report any suspected files to the ICT Service Desk

MUST NOT:-

- Transmit by email any file attachments which they know to be infected with a virus.
- Download data or programs of any nature.

6.11.3 The Council will ensure that email is virus checked at the network boundary and at the host, and where appropriate will use two functionally independent virus checkers.

6.11.4 If a computer virus is transmitted to another organisation, the Council could be held liable if there has been negligence in allowing the virus to be transmitted. For further guidance please refer to the Council's Protection against Malicious and Mobile Code Policy and Protection against Malicious & Mobile Code – Staff Guide.

6.12 Acceptable Usage Policy

6.12.1 Calderdale Council email users must read, understand and verify that they have read and accepted this policy.

6.12.2 Each workstation displays a 'Conditions of Use' message that requires positive confirmation that the user will comply with this and other associated policies. Users **must only press the OK button and continue** to sign on to their Council computer where they agree to comply with the conditions of use. See **Appendix C** for the 'Conditions of Use' Message.

7. Policy Compliance

7.1 All users who hold Council email accounts have a duty of care to maintain the confidentiality of personal details that are processed by them.

7.2 Failure to comply with this Policy and Procedure document may constitute gross misconduct and could lead to dismissal. Suspected illegal activities may also be reported to the Police.

7.3 If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager.

8 Review

8.1 The Corporate Lead for HR is the owner of this document and is responsible for ensuring that this document is reviewed on an annual basis.

8.2 A current version of this document and related documents will be available to all members of staff on the corporate intranet.

8.3 This document has been approved by the Information Governance Board on 12th May 2011 and the Governance and Business Committee on the 24 October 2011 and is issued on a version controlled basis.

8.5 The Governance and Business Committee agreed on the 24 October 2011 that the Corporate Lead for HR be authorised to agree any future minor/housekeeping changes required to the Internet and e-mail usage policies, with any proposed major/fundamental changes being referred to the Government and Business Committee for approval.

9. Associated References

The following Calderdale documents are directly relevant to this policy:

- Internet Acceptable Usage Policy
- Government Connect (GCSx) – Guide to Obtaining Government Connect Secure Extranet Email Account
- Information Protective Marking Policy
- Guide to using the Government Protective Marking Scheme
- Protection against Malicious & Mobile Code Policy
- Protection against Malicious & Mobile Code – Staff Guide
- ICT Code of Practice for Employees
- Software Installation Policy

- Remote and Mobile Working Device Policy
- Physical & Environmental Security Policy
- ICT Information Security Incident Reporting Procedure.
- ICT Information Security Incident Management Procedures
- Information Governance Incident Reporting - Breach of Non-Technical Data
- Anti Fraud & Corruption Strategy.
- Whistle Blowing Policy
- Data Protection Policy
- Records Management - Retention and Disposal Policy
- Records Management - Retention and Disposal Schedule

10. List of Appendices

Appendix A – Disclaimer Text

Appendix B – Email Usage Guidance

Appendix C – Conditions of Use Message

11. Change History

Rev	*Rev Date*	*Rev By*	*Issue Date*	*Description*
1.1				*Policy on Email and Internet Usage*
1.0			*22/8/04*	*Email Filtering & Monitoring Measures*
1.0	*Dec 2010*	*S Westbrook/ A Metcalfe*	*Dec 2009*	*Guidance to employees on the use of council provided Email Facilities*
1.2	*Feb 2011*	*A Metcalfe/J Pashley*	*Feb 2011*	*Review the current policy/standards documentation to produce one document within a standard format.*
1.3	*Feb 2011*	*B Wright/I Bowie/S Milner/T Robinson/C Yates*	*Feb 2011*	*Reviewed by BW and suggested amendments incorporated by AM.*
1.3	*12th May 2011*	*Information Governance Board*	*May 2011*	*Approved for Submission to Members for Approval.*
1.3	*24 November 2011*	*A Metcalfe*	*Nov 2011*	*Amended to reflect approval at the Council's Governance and Business Committee.*
1.3	*Jan 2012*	*A Metcalfe*	*Jan 2012*	*Slight amendments to grammar per recommendations from Communications Section. Minor addition new second bullet in key messages reminding of need to consider protective marking.*
1.3	*Jan 2015*	*A Metcalfe*	*Jan 2015*	*Minor revisions in respect of auto forwarding email and connection period for laptops.*

DISCLAIMER TEXT

Appendix A

Warning

Please note that whilst this email and any attachments originate from Calderdale MBC, the views expressed may not necessarily represent the views of Calderdale MBC.

This email and any attachments may contain information that is privileged, confidential or otherwise protected from disclosure. They must not be used by, or copied or disclosed to persons other than the intended recipient. Any liability (in negligence or otherwise) arising from any third party acting, or refraining from acting, on any information contained in this email is excluded. If you have received this email in error please inform the sender and delete the email.

Email can never be 100% secure. Please bear this in mind and carry out such virus and other checks, as you consider appropriate. Calderdale MBC accepts no responsibility in this regard.

Copyright of this email and any attachments belongs to Calderdale MBC.

Should you communicate with anyone at Calderdale MBC by email, you consent to the Council monitoring and reading any such correspondence.

This email message has been scanned for viruses and its content cleared.

Email Usage Guidance — Appendix B

Avoid:-

- Using email to avoid face-to-face communications on difficult matters.
- Using email as a substitute for normal face-to-face discussions, particularly for managing staff.
- Sending emails to "All mailboxes" unless there is a specific business need to do so.
- Sending attachments (particularly large documents) if you can provide a link to a shared folder or web page.
- Setting up automatically delete e-call email they may contain important information.

Ensure:-

- You complete the "Subject" box with a meaningful description, and should the data or attachment be of a "Protect" or "Restricted" nature, the email and subject box should be marked as such.
- You always think before you send an email. Never email rashly or in anger.
- You keep your mailboxes tidy.
- You contact the ICT Service Desk if you need to send an encrypted email.
- Global emails are sent out under the e-Call scheme.
- An "Out of Office" message is activated to advise when the recipient of an email is away from work, and provide alternative contact details.

Care should be taken:-

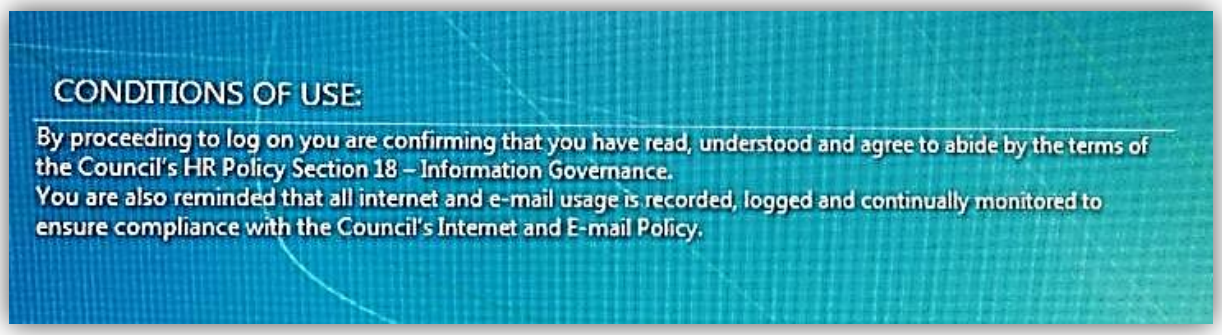
- To ensure the correct address is applied to an email message e.g. mis-spelling email addresses or selecting the wrong address from a list.
- To ensure that all email messages are clear and easily understood (avoid any jargon or 'local terms').
- When using distribution lists, especially if forwarding an email. Check the recipients list to make sure you are not sending it on to someone who has already received it.

Email is a powerful tool and if this policy and its procedures are observed then email will be used wisely as an effective communication.

Appendix C

Conditions of Use Message

The following Conditions of Use message will be displayed at each log-on to a Council PC or Laptop



Email Usage Policy and Procedures (2015)
Quick Reference Guide

The following is a quick reference guide to the key points and details of appropriate and inappropriate usage. Further information can be found in the full version of the Email Usage Policy and Procedures document available on the Council's Intranet.

Key Messages:

> All emails that are used to conduct or support official Calderdale Council business must be sent using a Council provided email account in the format of "@calderdale.gov.uk" or for GCSx "@calderdale.gcsx.gov.uk". **Non-Council** provided email accounts **must never** be used to conduct or support official Calderdale Council business.

> Emails and attachments should be protectively marked where appropriate in compliance with the Guide to using the Government Protective Marking Scheme.

> Users must never allow anyone else to use their Council provided email account.

> Care must be taken by users to ensure that all emails are correctly addressed.

> All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual user. Emails held on Council equipment are considered to be corporate records as well as providing a record of staff activity with regard to email.

> Emails that evidence an action undertaken by the Council are subject to the respective retention period. Emails to be retained as records should be transferred to the approved record keeping system for that information e.g. a record keeping system such as EDRMS or structured network folders etc.

> Users are permitted to use their Council email account for personal purposes **in their own time** (Any personal use in works time requires line manager authorisation).

> Users must **never** use their Council email account for inappropriate purposes.

> All users must ensure that any emails sent or received externally containing non-public information (identified as PROTECT or RESTRICTED) must be sent securely, using encryption or via GCSx. For further advice please contact the ICT Service Desk on 01422 393423.

> Council email addresses must not be set to automatically forward email to non-Council email addresses. In addition, automatic forwarding to internal email addresses must be considered carefully, to prevent sensitive information being forwarded inappropriately.

> Line managers must ensure that they have read only access to their employees email accounts.

> Auto forward received emails from any non-Council email account to your Council email account.

> All email activity is recorded and monitored to ensure compliance with this policy.

> **Failure to comply with this Policy and Procedure document may constitute gross misconduct and could lead to dismissal. Suspected illegal activities may also be reported to the Police.**

Appropriate Usage

You may:

✓ Use Council email facilities for personal purposes outside work time.

✓ Open personal emails received in your Council email account in work time.

✓ Use the facilities, with the prior approval of your manager, for personal purposes in work time.

Where 'work time' is stated this means the time you are working for the Council – **not just core hours.**

Inappropriate Usage

The list below gives examples of "inappropriate" usage but is neither exclusive nor exhaustive. "Inappropriate" material would include data, images, audio files or video files the transmission of which is illegal under British law, and material that is against the rules, essence and spirit of this and other Council policies.

Do Not Allow:

× Anyone else to use your email account or provide any other person with the means to access your email account e.g. by disclosing your user ID and password etc.

Do Not Carry out:

× Unauthorised transmissions to a third party of non-public information identified as PROTECT or RESTRICTED information concerning the activities of the Council.

Do Not Create or Transmit:

× Any material that includes false claims of a deceptive nature.

× Any material or anonymous messages - i.e. without clear identification of the sender which could bring the Council into disrepute.

× Unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.

× Any so-called 'flame–mail' - i.e. the use of impolite terms or language, including offensive or condescending terms.

Do Not Knowingly:

× View, send or receive any offensive abusive, obscene or indecent images, data, or other material, or any data capable of producing obscene or indecent images or material which is likely to cause annoyance, inconvenience or needless anxiety.

× View, send or receive material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, and disability, political or religious beliefs.

× Engage in any activity that corrupts or destroys other users' data or disrupts the work of other users.

× Engage in any activity that unreasonably wastes staff effort or use networked resources, or activities that unreasonably serve to deny the service to other users.

× Infringe copyright or intellectual property rights.

× Use the facilities for any activity, which is illegal or fraudulent.

× Make statements or derogatory remarks purporting to represent the Council when they are personal views.

× Use an automatic forwarding rule that sends all received emails from your Council email account (@calderdale.gov.uk) to an external email address.

× Set emails to auto-forward to your Council email account from a non-council email account.

× Use the email facility to receive or save any personal files such as programs/applications, music or animations or images etc.

Do Not Publish:

× To others the text of messages written on a one-to-one basis, without the prior express consent of the author.

Do Not Use or Attempt to Use email:

× For personal purposes in works time, **UNLESS it is in compliance with the Green – Acceptable Use section above.**

× To make libellous statements about individuals or other organisations or use email to engage in gossip.

× To violate the privacy of other users or to unfairly criticise individuals.

Where 'work time' is stated this means the time you are working for the Council – **not just core hours.**

Document Control Information	
Issue No	Version 1.3
Issue Date	November 2011
Status	FINAL
Approved By	Information Governance Board – 12 May 2011 Governance and Business Committee – 24 October 2011
Next Review Date	January 2013
Authors	Andrew Metcalfe & Janette Pashley
Service	Internal Audit & Business Change and Performance Management
Distribution	Information Governance Board ICT Control Environment Corporate Support Group Corporate Information Manger – Tracie Robinson Business Change & Performance Management – ICT Service – Iain Bowie, Pam Plant, Jon Smith Forensics Team Management Auditor (Computers) – Andrew Metcalfe

DATA PROTECTION ACT 1998

Access to Records

Employers must give staff access to the majority of their personal records including assessments, complaints, interview notes, sickness records and with some exceptions references. Employment records include those held by Line Managers or a training section.

Further Assistance

The Corporate Information Manager (Tracie Robinson) can be contacted on 07872 100567 regarding all Information Governance matters. There are also representatives within the Information Governance team who may also be able to assist you. Part of their remit is to advise on Data Protection matters. If you do receive a request for subject access, please pass the request onto them so that it can be dealt with on the correct system and in accordance with statutory guidelines.

Please contact:

John.giddings@calderdale.gov.uk
Information_management@calderdale.gov.uk

Please click on the Information Governance pages on the Intranet where a lot of additional policies and guides can be found.

What should I do if I receive a request for personal information?

If you receive a request then it must be passed to your Access to Information Liaison Officer. Any legitimate request must be made in writing, and a form for such requests is available on the Council's website.
There is also a fee and identification required. The Corporate Information Manager who will determine the response to the request with the Liaison Officer will then examine the request, and provide guidance on an individual request basis. Generally the Council must respond to requests within 40 Days.

Do we have to comply with the Request?

Not everything that is personal information is subject to the full force of the legislation. There are a number of exemptions that limit the requirements of the Act in certain cases. The application of exemptions is a complex legal procedure and advice should be sought from your Liaison Officer.
Exemptions exist in the 1998 Act for Information related to the following areas. It should be noted that this does not necessarily mean that all information related to the categories listed below is exempt. Each case must be examined on it's own merit? The exemptions relate to:

- National security;
- Crime and taxation;
- Some areas of health, education and social work;
- Regulatory activity;
- Journalism, literature and art;
- Some areas of research, history and statistics;
- Information made available to the public under other legislation;
- Disclosures required by law or made in connection with proceedings;
- Domestic use - e.g. home computing;
- Confidential references;
- Corporate finance and management forecasts;
- Exam marks and scripts;
- Legal professional privilege and self-incrimination.

If we do not have an exemption that can be relied upon, then the information should be provided. If we fail to do this, the Information Commissioner may serve a notice forcing the Council to comply with the request. A breach of the Act may lead to a personal fine or the Council could be fined.

What information will the enquirer receive?

Our response to a valid request for information should be to provide all the information held about the person in the Council's computer and manual records, with a description of the purposes for which we process the information, a list of services to whom the information is disclosed, and information about the source of the data.

Where automated decisions are made, for example about benefits or council tax, the enquirer is also entitled to information regarding the logic behind the automated decision.

What about my rights as a member of the public?

As a member of the public, the Act gives you access rights to data held by the council about you. These rights are explained on the Council website Data Protection pages.

So how do I find out more?

Resources are available on the Information Commissioner's website state above. You can also contact your Access to Information Liaison Officer. The Officers for each service are listed below.
For Freedom of Information Requests, Data Protection queries and Subject Access Requests please contact the relevant AILO for the service area or the Corporate Information Manager.

Corporate Information Manager -
Tracie Robinson (ext 2298)
Legal Services, Westgate House, Halifax. HX1 1PS
Telephone: 01422 392298
Tracie.Robinson@calderdale.gov.uk

Calderdale Council

www.calderdale.gov.uk

A Guide to Data Protection for Calderdale Council Employees

What is this guide for?

The purpose of this guide is to inform you of the key features of the Data Protection Act 1998, and how the legislation relates to your work as a Calderdale Council Employee. This is only an introductory guide and for further information you should contact your Access to Information Liaison Officer (AILO) for your Service. (You can find a list of AILOs on the back of this guide). You can also visit the Information Commissioner's website: www.informationcommissioner.gov.uk.
The Information Commissioner oversees the Legislation in the UK.

Introduction to the Data Protection Act:

Calderdale Council manages information about people in relation to most of the services it provides. There is personal information on application forms, benefit claim forms, council tax records, school records, housing records, planning applications and social services client files. These are just a few examples.
The Council has a duty under the Data Protection Act to manage personal information according to the principles set out in the legislation. This means that employees must always be careful when handling personal information about clients, particularly those who have who have responsibilities for the processing and protection of personal information.
The Act gives individuals a right of access to personal information held by the Council about them. The legislation calls this a Subject Access Request. This means that both Council Employees and members of the public have a right to see the information the Council holds about them.
The Act also provides a legal framework within which Date Controllers, of which the Council is one, must operate. It covers the information we hold about living people, which the Act describes as personal data. The data could be held in a multitude of formats, including email accounts, manual forms, card index systems, computer databases, CCTV footage and since January 1st 2005, even notebooks or post-it notes.
It includes both factual information and expressions of opinion. In essence all the information we hold should be treated as being subject to the legislation.

What are the implications for the Council?

The key requirement for the Council is to comply with the 8 principles of Data Protection when handling personal information. The principles are legally enforced and comprise the following:

Personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes and not in any manner incompatible with those purpose;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept any longer than is necessary;
- Processed in line with the data subject's rights;
- Secure;
- Not transferred to other countries without adequate protection.

To meet these requirements the Council will need to make sure all staff are adequately trained and instructed in the application of the Act. Additional guidance about Data Protection will need to be distributed to ensure all staff know how to apply the legislation in their Council role. The Council may need to examine how it handles information and examine ways of notifying data subjects (i.e. individuals) about how the Council handles their information, and where necessary, obtain their consent to process certain information.

How do I know if the Act affects me as an employee?

If your job involves handling information about living individuals then it is likely that you must comply with the requirements of the Act. Many jobs will involve using or manipulating personal information in some way.
The Act describes this as processing information. Processing is a broad term that covers the organisation, adaptation, alteration, retrieval, consultation, use, disclosure, transmission, dissemination, alignment, combination, blocking, erasure, destruction or archival of personal information. This is a broad definition that covers virtually all uses by the Council of personal information.
Under the legislation, if you process personal data then you must ensure that one or more of the following conditions for processing are met. Otherwise you should not process the information:

Conditions for Processing Personal Data:

- The individual has given his or her consent to the processing;
- The processing is necessary for the performance of a contract with the individual;
- The processing is required under a legal obligation;
- The processing is necessary to protect the vital interests of the individual;
- The processing is necessary to carry out public functions;
- The processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

It is likely that for Calderdale most of the processing we do is covered by the condition that the Council is carrying out public functions.
There are further conditions that need to be met for processing if you are processing what the Act describes as Sensitive Personal Date. This refers to personal information about the individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, sexual life. It also includes information on the commission or alleged commission of an offence and any proceedings for any offence or alleged offence. If you are dealing with this kind of information and require guidance then you should contact your Access to Information Liaison Officer.

Telephone Policy and Procedure

1. Policy Statement

1.1 Council telephones are provided for business use, to facilitate the delivery of high quality services. However, it is noted that in some circumstances the private use of Council telephones is acceptable. This Policy is designed to ensure that employees are aware of the circumstances in which such usage is acceptable.

1.2 It is acknowledged that most employees have a personal mobile phone. This Policy will also include the appropriate use of personal mobile phones in the workplace.

1.3 Employees may be eligible to be Designated Mobile Phone Users in circumstances where for example they are expected to be on call and this Policy will outline the necessary criteria.

1.4 This Policy applies to all employees of the Council, including those in Community and Voluntary Controlled Schools.

2. Policy Objectives

2.1 This Policy aims to:

- ensure that all Council telephones are used in an appropriate manner to support service delivery;
- raise employee awareness of the appropriate usage of personal mobile phones in the workplace;
- outline a consistent framework of eligibility criteria for Designated Mobile Phone Users.

3. Employees Responsibilities

3.1 Employees are required to familiarise themselves with this Policy and act in accordance with it. Any breaches or abuse of this Policy will be dealt with under the Council's Disciplinary Procedure.

4. Personal use of Council Telephones

4.1 Limited personal use of Council telephones is permitted to make essential work-life balance calls such as calling home to let a partner or dependant know of your expected arrival time. Where possible these calls should be made during lunchtime.

4.2 Employees are not expected to pay for personal calls of this nature, this is a matter of trust between the Council and employees, and as such should not be abused. These calls should be as brief as possible, and they should not disturb other colleagues.

4.3 Other limited work-life balance calls are permitted, for example booking an appointment at the dentist or doctor. Personal calls of this nature must be paid for.

4.4 Employees should not use Council telephones at any time to make or receive social calls, or to further outside business interests or for personal financial.

4.5 Call records will be monitored.

5. The Use of Mobile Phones in the Workplace

5.1 All mobile phones must be kept on silent mode in the workplace.

5.2 As it is accepted that employees may need to deal with personal matters during working hours, calls may be made on **personal** mobiles to address work-life balance issues as outlined above in **Section 4**. Where possible these calls should be made during lunchtime and should be limited in terms of both their duration and their frequency.

5.3 Employees should not use **personal** mobile phones to make or receive social calls, or to further outside business interests or for personal financial gain during working hours.

5.4 Employees must not use either Council or personal mobile phones to make sound recordings or to take and/or transmit pictures of colleagues, clients or service users under any circumstances.

5.5 Employees must not use either Council or personal mobile phones to send/read personal text messages, forward or show texts or internet images to colleagues, clients or service users.

5.6 Employees must not use either Council or personal mobile phones to access the internet during working hours.

5.7 Employees must not charge **personal** mobile phones in the workplace.

6. Designated Mobile Phone Users

6.1 It is the responsibility of Chief Officers to designate mobile phone users in their Service areas, and to provide handsets and additional equipment such as mobile phone holder cradles where applicable.

6.2 The criteria below should be considered when designating staff as mobile phone users:

- they are lone workers, work in isolation or are deemed to be vulnerable or at risk;
- they work away from their administrative base for lengthy periods of time and at unsocial hours;

- the role involves out of hours support, eg on call;

- the individual needs to be contactable when away from their administrative base for operational or safety reasons, e.g. responding to emergency situations where there is a statutory requirement.

6.3 Employees who are issued with a mobile phone must follow the guidance listed in both **Section 4** and **Section 5** above during working hours.

6.4 The Council will reimburse the cost of business calls. Itemised bills should be produced to enable personal calls to be highlighted. The actual cost of the private call plus VAT must be paid.

6.5 It is illegal to use a hand-held mobile phone while driving, therefore authorised users must switch off their phones until they reach their destination. The use of an ear piece does not make a phone hands free. To be hands free a mobile phone must be fixed or in a cradle.

6.6 Managers must not attempt to contact mobile phone users if they know they are driving, it is an offence to 'cause or permit' a driver to use a hand-held mobile phone while driving. Further information about the safe use of mobile phones may be found on the Council intranet in the Health & Safety reference library - click here.

6.7 All Council issued mobile phones must be returned on the termination of employment and any outstanding balance for personal calls should be paid.