Appendix 4

West Dunbartonshire Council

(Information Security Policy Framework)
Privacy and Monitoring

Contents Listing

1 Introduction 2
2 Scope of Guidelines 2
3 Awareness 3
4 Clarification of Policy Contents 3
5 General 4
6 Automatically Logged Data Examples 7

1 Introduction

These **Privacy and Monitoring** guidelines provide information related to the monitoring of IT communications and use of IT technology and specifies:

- The definition of electronic communications;
- The approach to monitoring and interception of communications;
- What information is recorded by usage logging;
- How content inspection is controlled; and
- How users of electronic communication facilities are made aware of this procedure.

Electronic communications covered by these guidelines include:

- Telephones including, land lines, mobile phones, smartphones and IP/Internet Telephony also referred to as VoIP (Voice over Internet Protocol);
- Verbal recordings such as dictation, voice-mail and systems that record telephone calls from, for example clients and citizens;
- Internet access including social media and file sharing access;
- Cloud hosted system use including O365 content such as email, connectivity to the Council tenancy, processing and sharing of content;
- Instant messaging use;
- Voice, web and video conferencing facilities;
- Email use;
- Fax communications;
- ICT Systems and facilities;
- Computing Networks and attached equipment including non-wired connections and equipment such as wireless; and
- Remote connections to the Council.

2 Scope of Guidelines

These guidelines apply to all Council employees whether permanent, contract or temporary, Elected Members or any other party accessing any computer systems owned, leased or operated by West Dunbartonshire Council and are part of the Acceptable use Policy framework.

“ICT Systems and facilities” refers to physical hardware, software applications, peripherals and components of the Councils network infrastructure that support the transmission of electronic data.

These guidelines extend to the use of all such equipment or systems. This applies regardless of where those equipment or systems are located. This also applies regardless of the physical location where user access or connections originate.

3 Awareness

Employees will be made aware of the Acceptable Use Policy and associated framework as follows:

- New starts will be informed at their Service induction;
- Updates to the policy will be distributed via electronic means such as MetaCompliance[1], email or future tools used by the Council;
- Services will be responsible for manually distributing updates to the policy where anomalies exist such as multiple users sharing a login account;
- The policy and associated procedures will be available on the Councils Intranet or online by other means; and
- Updates will be communicated via Information Security Forum representatives.

Elected members will be made aware of the Acceptable Use Policy and associated procedures as follows:

- Informed of the policy at initial briefing and induction;
- Updates to the policy will be highlighted by Members Services; and
- The policy and associated procedures will be available on the Councils Intranet or online by other means.

4 Clarification of Policy Contents

In the event of an issue arising from an interpretation of the AUP or these guidelines clarification should be sought from the Manager of ICT.

For further advice or assistance please contact the ICT Security Officer in the first instance either by email or by telephoning 01389 737568.

[1] MetaCompliance automates the dissemination and acceptance of policies

5 General

1) Access to Council information processing systems and facilities is provided for business use. Any circumstances that permit personal use will be publicised on the Intranet; misuse or prohibited use shall be dealt with under the Council's disciplinary procedures.

2) A range of monitoring is undertaken to ensure information processing facilities are operating efficiently and effectively. Information entering, leaving, accessed or stored on information processing facilities, including Internet access, Instant Messaging and Council email is monitored. The monitoring undertaken is not generally focused on specific individuals; however personal data may be accessed as part of the process.

3) By logging in to any Council information processing system or facility a user is deemed to consent to the Council's monitoring procedures.

4) Monitoring is undertaken principally to:

- Comply with regulatory and statutory obligations;
- Monitor standards of performance;
- Ensure the effective operation of Council systems and information processing;
- Prevent or detect unauthorised use or other threats to information processing systems;
- Investigate allegations of misconduct, breach of contract, a criminal or civil offence or fraud by the user or any third party;
- Ensure compliance with Council policies and procedures;
- Review usage; and
- Ensure business operates during employee absence and other business requirements.

5) To ensure information processing systems are not open to abuse, the Council reserves the right to monitor individual employee's usage. This level of monitoring must be fair and proportionate and will be appropriately authorised.

Privacy

6) The Council aims to strike a balance between respect for an individual's privacy while enabling the monitoring and scanning necessary to fulfil legal obligations and business needs.

7) Individual's privacy will be respected in accordance with the Human Rights Act 1998 and data protection law such as the Data Protection Act 2018 and GDPR. The Council will act in accordance with its obligations under the

- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000;
- Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA);
- Privacy and Electronic Communications (EC Directive) Regulations 2003; and
- And any other relevant legislation as may be enacted from time to time.

8) Monitoring differentiates between:

- Usage logging – involves collecting data, generally from automated log files, showing information related to how and when a user accessed an information processing system with a specific user account (i.e. a login);

- Content inspection - viewing information held in business or personal files, email etc or viewing information on screen. Content inspection will take place only if properly authorised and if the usage record alone is not sufficient; and
- Covert monitoring – actively undertaking targeted monitoring of an individual in a way that would not be expected and without their knowledge. Covert monitoring could involve real time monitoring of events. The Council will not normally undertake covert monitoring under the scope of these guidelines.

Usage logging

9) Usage logging is undertaken to ensure and improve service performance, comply with legislative requirements and to help identify and investigate potential prohibited use or misuse. This can be undertaken by the Council or on its behalf by a 3rd party supplier / contractor.
   - Typical data logged is noted at the end of this document;
   - Content logging is minimal as the aim is to log information about the activity however some logs will retain minimum information as part of the standard logging process; and
   - Access to logging information is restricted and controlled.

Content Inspection

10) Content inspection will only be undertaken for legitimate business reasons which may include:
   - To ensure continued business operation during employee absence or when an employee leaves their post;
   - To comply with legislative requests for information such as Subject Access and Freedom of Information requests;
   - Where there is reason to believe that a breach of policy is or has occurred, including a breach of the Acceptable use Policy and its framework;
   - To comply with the request of law enforcement officers;
   - To comply with legal obligations;
   - To prevent or detect contravention of criminal or civil law; and
   - Where there is reason to believe that a breach of an individual's employment contract is occurring or has occurred.

11) Council IT systems and facilities are provided for business use. The Acceptable Use Policy framework outlines where limited personal use is permitted. Monitoring systems cannot differentiate on types of use therefore any communications on Council facilities should not be regarded as private.

    Content inspection may involve viewing or accessing information held in:
   - Business and or personal files and documents;
   - Business and or personal email messages or any other ICT based communication;
   - Business and or personal information within instant messaging systems;
   - Business and or personal information within any information store, drive structure or repository provided by the Council;
   - Business and or personal information displayed on a screen;
   - Emails that have not yet been opened or received by the intended recipient;
   - Detailed access logs such as those detailing Internet use; and
   - Telecoms and voice recording systems.

12) Requests to inspect content must be formally requested by a Senior Manager using the appropriate process.

13) Where the process requires it, managers will normally seek authorisation from a Strategic Lead. Where the request involves a Strategic Lead authorisation should be sought from the relevant Strategic Director or from the Chief Executive (if appropriate). If the request involves a Strategic Director or Elected Member, authorisation should be sought from the Chief Executive.

14) Where authorisation is granted, the authorising officer must ascertain if it is appropriate to advise the individual concerned.

15) The individual concerned should normally be informed of any inspection in advance and again on completion. However, in certain circumstances it may be necessary to obtain access without informing the individual, such as where there is reason to believe that to do so would prejudice an investigation, the employee is on long term absence or the individual is no longer an employee.

16) The authorisation should be passed to the Information Security Officer for action or other member of IT Services if appropriate.

17) IT Services team managing the request will ensure approval has been given and demonstrate when access was provided and to whom. This information will be held by the Information Security Officer or the IT Service Desk where appropriate and may involve HR.

Covert Monitoring

18) Circumstances for covert monitoring are very rare and as such will not normally be undertaken by the Council. Such requests would be authorised by the Strategic Lead, Legal & Regulatory Services and the Chief Executive without notification being provided to individuals as doing so could prejudice the prevention or detection of suspected criminal activity or malpractice.

Authorisation would include a permitted timeframe for the monitoring with all activity ceasing after any investigation is complete.

Circumstances where covert monitoring may be authorised include:

- To comply with the request of law enforcement officers;
- To comply with legal obligations;
- To prevent or detect contravention of criminal or civil law; and
- To prevent or detect malpractice.

6 Automatically Logged Data Examples

Examples of data which may be automatically logged includes, but is not limited to:

Source	Information
Network and application access	User Id date and time of login, Location of access device File(s) accessed, modifications and deletions Print activity Data copying Processes initiated and terminated
Cloud hosted applications (by the Council and on its behalf)	User Id date and time of login, Location of access device File(s) accessed, shared, modifications and deletions Invitations to other parties Print activity Data copying Processes initiated and terminated Where available record based activity
Email	Sender email address, Recipient(s), Date, time Size Subject Content Attachment size and type Routing Filtering undertaken and results
Email Journaling	As above Content
Instant Messaging	Sender and Recipient name Date, time Content Files transferred
Conferencing facilities (Inc. webinars, skype etc.)	User Id date and time of use Location of access device File(s) accessed, modifications and deletions Print activity Data sharing undertaken Processes initiated and terminated
Internet	User Id date and time of login Location of access device Sites accessed and access time Blocking undertaken
Telephone	Date and time of call Duration Number making the call Number called Ring time if unsuccessful Cost (if appropriate)