CCTV Policy

Document Control			
Policy Owner	Barry O'Hagan		
Policy Author	Barry O'Hagan		
Version	2.0		
Consultation	Senior Management Team Yes Trade Unions Yes		
Equality Screened by	screening in progress	**Date**	28/03/2023
Equality Impact Assessment	Not Applicable	**Date**	N/A
Rural Screened	Screening completed	**Date**	29/03/2023
Approved By	Previously Policy & Resources (PR 159/17)	**Date**	
Adopted By		**Date**	
Review Date	October 2022	**By Whom**	BOH
Circulation	Councillors, Staff, External CCTV companies		
Document Linkages	Data Protection Policy. ICO Data Privacy Impact Assessment Disciplinary Policy Code of Conduct for Local Government Employees		

CONTENTS PAGE

Paragraph	Description	Page Number
1.0	Introduction	3
2.0	Policy Aim & Objectives	3
3.0	Policy Scope	4
4.0	Linkage to Corporate Plan	4
5.0	Operational Considerations and implementation	4
6.0	Roles & Responsibilities	12
7.0	Impact Assessment • Equality Screening • Staff & Financial Resources	13
8.0	Support & Advice	13
9.0	Communication	13
10.0	Monitoring & Review Arrangements	13

1.0 INTRODUCTION

This policy sets out how Mid Ulster District Council uses closed-circuit television (CCTV) in the operation of its functions. It is designed to ensure that personal data consisting of the images of people captured by CCTV systems (data subjects) is processed fairly in terms of the Council's obligations as a data controller under the Data Protection Act 2018, the Local Government Act (Northern Ireland) 2014, the Regulation of Investigatory Powers Act 2000 and in terms of article 8 of the European Convention on Human Rights. The policy is also designed to comply with the CCTV Code of practice issued by the Information Commissioner's Office in 2014 and should be read alongside Mid Ulster District Council's Data Protection Policy.

Mid Ulster District Council uses CCTV cameras in Council premises including offices, leisure and community centres, amenity sites, other outdoor venues and public spaces including some town centres .

The cameras are used to record, store and process images of staff and service users. The CCTV system consists of:

- Fixed exterior and interior cameras situated on Council property and vehicles, which continually record activities;
- Public space cameras including Town centre Camera's
- Temporary public space cameras, which are used from time to time to monitor indiscriminate littering and dog fouling occurrences;
- Body worn video cameras, which are activated from time to time by Council enforcement staff operating in public areas;

2.0 POLICY AIM & OBJECTIVES

2.1 **Policy Aim**: To ensure Council manages our CCTV systems in accordance with all relevant regulations and Council policies. The policy governs the use of the systems, including the storage, disposal and access to images and the storage of information.

2.2 **Policy Objectives:**

The policy aims through the use and deployment of CCTV to achieve the following:

- To prevent, detect, investigate, and report crime and to assist with the apprehension and prosecution of offenders;
- To discourage anti-social behaviour including dog fouling and littering;
- To enhance the safety and well-being of staff and the public using Council premises, services, and town centres;
- To assist with investigation and processing of insurance claims, investigations and the overall management and supervision of Council buildings, premises, and events;
- To assist with the preparation for and conduct of disciplinary investigations and hearings including those involving alleged or suspected criminal activity and/or breaches of Council policies in relation to the health, safety or wellbeing of employees, subcontractors, and the public generally;

3.0 POLICY SCOPE

This policy applies to all Council departments and to the services they provide.

Definitions

CCTV or closed-circuit television is the use of video cameras to transmit a video and/or audio signal to a specific place on a limited set of monitors. CCTV may or may not be recorded.

Data controller is the person who (either alone or jointly or in common with other persons) determines the purposes for which and the way any personal data (including CCTV images) is to be processed.

CCTV manager is the person who is responsible to the relevant Service Officer (e.g., facility manager) for the day-to-day management and use of CCTV systems in their service.

4.0 LINKAGE TO CORPORATE PLAN

4.1 Referring to Mid Ulster District Council's Corporate Plan 2020-24, this policy contributes toward the delivery of Corporate Theme 4: Environment.

5.0 OPERATIONAL CONSIDERATIONS & IMPLEMENTATION

Privacy Notice and System Usage

Images obtained from CCTV systems are normally automatically overwritten at intervals ranging from 14 to 31 days, dependent on the type

of equipment and capacity in use at each location, unless they are needed for investigation purposes and subsequent disciplinary hearing /appeals. It is necessary to hold images for this duration due to the time lapse between an incident/accident taking place and notification of this being received by the Council. Where recorded images are needed for investigation purposes, they will be held for the minimum period necessary to carry out the investigation/disciplinary/appeal processes and will be destroyed following this (see Retention of Images below).

Viewing of live images on monitors should be restricted to designated individuals who are authorised to view them, for example to monitor congestion for health and safety purposes. Control units for the display of CCTV images should therefore be situated in restricted areas where they are not visible to members of the public unless the monitors display scenes which are in plain sight of the public.

All processing of CCTV images shall be conducted in accordance with this policy and, in particular, processing of personal information shall be in compliance with the requirements of the Data Protection Act 2018, the Data Sharing Code of Practice and Video surveillance (including guidance for organisations using CCTV) issued by the Information Commissioner's Office. Where images are obtained of persons committing acts of an illegal nature and/or acts which breach any Council byelaws, rules or regulations, these images may be used as evidence in the prosecution of the offence.

Images collected by CCTV systems may, subject to the requirements of this policy and the Data Protection Act 2018 and the Data Sharing Code of Practice, may be shared with other organisations or individuals for the purposes of law enforcement, investigation of incidents/civil claims, or to comply with subject access requests.

The Data Protection Act 2018 provides individuals with the right of access to personal data that the Council holds about them, including CCTV images. This right can be exercised by making a subject access request (see section on Access and Disclosure below) to the Data Controller for the service.

Signs must be displayed to identify all areas subject to CCTV surveillance and the signs should be clearly visible and legible. The signs must indicate the purpose for which cameras are installed and the contact details for Mid Ulster District Council as the organisation responsible for the CCTV system.

Cameras must be sited in such a way that they only monitor locations intended to be covered. They will not be used to look into private property.

Concealed cameras may be deployed where the organisation suspect the law is being broken or in strict accordance with the provisions of or the Regulation of Investigatory Powers Act 2000 (RIPA 2000). In exceptional circumstances where it is not practicable to secure the appropriate authorisation as required by RIPA 2000 prior to deployment such as where there is reasonable cause to suspect that illegal activities, or serious breaches of Council policy pertaining to health and safety are taking place or about to take place, deployment may occur but on the strict provision that the appropriate authorisation is obtained and recorded without delay.

The authorised officer for the purposes of RIPA 2000 is the Chief Executive or, in his absence, the Deputy Chief Executive. The authorised officer now has to make a RIPA application to a District Judge, via the Magistrate Court, before covert techniques can be used.

5.2 Approval and Documentation

All CCTV installations require mandatory screening to ensure that the processing of personal data in this way is justified. The Information Commissioner's Office Guidance on screening is contained in Appendix 1: DPIA Screen Checklist ICO Oct 2022.

Screening will be signed off by Assistant Director/ Heads of Service/Lead Officers (e.g., facility manager). Where screening identifies the need for a Privacy Impact Assessment to be undertaken, it will be the responsibility of the appropriate Assistant Director/ Heads of Service/Lead Officers to ensure that this is completed using the template and guidance issued by the Information Commissioner's Office contained in Appendix 2.

Notwithstanding the use of concealed cameras, Privacy Impact Screening / Assessments are required to be in place and documented for all CCTV installations throughout the Council. Where no existing Privacy Impact Screening/ Assessments are in place, these must be carried out using the questions / template issued by the Information Commissioners Office contained in Appendices 1 & 2.

Following this, existing Privacy Impact Assessments will be reviewed every 2 years (or sooner if there is a material change in circumstances) to establish whether the continued use of CCTV is justified.

Privacy Impact Screenings and where necessary Assessments must be carried out for all proposed new installations of CCTV.

When a Privacy Impact Assessment has been signed off by the Assistant Director/ Heads of Service/Lead Officers(e.g., facility manager), reviewed by the Director and approved by the relevant Council Committee, the Head of Service/Lead Officer should forward it to the officer with responsibility for ensuring that Council complies with its responsibility as a Data Controller, along with details of the relevant CCTV scheme.

A central register Appendix 3 will be maintained listing the locations where CCTV cameras are sited and the purposes for which the systems have been installed. Any new installations of CCTV or revised locations, including body worn or temporary cameras, should be notified to the officer with responsibility for ensuring that Council complies with its responsibility as a Data Controller so that the appropriate records can be updated. Each part of the CCTV system must fully comply with the provisions of this policy.

Requests from individuals and statutory bodies such as law enforcement agencies to view CCTV images should be considered in accordance with the provisions of this policy, the Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000, article 8 of the European Convention on Human Rights, the CCTV Code of practice issued by the Information Commissioner's Office in 2014 and Mid Ulster District Council's Data Protection Policy.

Both the requests for access and the decisions in relation to the requests must be recorded. Individuals authorised to view images must formally confirm by personal signature that they undertake to abide by the requirements of this policy.

Formal records must also be kept of CCTV images released (see Processing Images below).

5.3 Maintenance of Cameras and Equipment

Each Head of Service/facility manager, in conjunction with Council's Property Services department, is responsible for ensuring that adequate maintenance arrangements are in place for the CCTV equipment deployed in their service area.

Each manager should ensure that the equipment is protected against vandalism, remains in good working order, and is repaired promptly when damaged. This is essential to ensure that images required for evidential purposes are of sufficient quality.

Maintenance/repair logs should be kept and completed when maintenance work is carried out on any Council CCTV equipment. All maintenance contractors' visits will be by prior arrangement.

5.4 Processing Images

It is important that access to and disclosure of images is restricted and carefully controlled, not only to safeguard the rights of individuals but also to ensure that evidence is not compromised should the images be required for evidential purposes.

Directors, Heads of Service and Lead Officers must ensure that:

- access is restricted to those staff who need to have access to recorded images for the purpose(s) for which the system was installed and where appropriate, external statutory agencies;
- images are viewed by authorised staff in a secure and confidential location;
- downloaded and saved images from body worn video or temporary cameras are only viewed in the event of an incident having taken place which needs to be investigated - if no such incidents have taken place the images should be deleted after 31 days;
- those authorised to view images are issued with a copy of this policy and required to personally sign a declaration that they fully understand their obligations to adhere to its conditions;
- the Duty Officer in charge of Council premises may authorise requests by PSNI officers to view CCTV images at monitoring stations;
- if recorded images are released, a record will be maintained at each location to record this by the facility manager. The logs should include a description of the images, the purpose for which they were released and the secure location where they are stored. Two copies of each incident should be made, one for retention by the Council and one for the requesting person/organisation.

5.5 Access and Disclosure

Mid Ulster District Council's Data Protection Policy includes arrangements for access to CCTV images. As the operator of the CCTV system, Mid Ulster District Council may provide access and disclosure in accordance with the provisions of the Data Protection Act under a Subject Access request, an overriding legal obligation such as a court order, and in certain situations, in response to a Freedom of Information requests.

5.6 Requests from Individuals for Disclosure of CCTV Images

Under the Data Protection Act 2018 an individual has the right of access to personal data held in relation to them which includes CCTV images. In this case they can make a subject access request to view the data and to be provided with a copy of the images. This must be provided within 1 month of the Council receiving a request. In these circumstances a judgment must be made as to whether disclosure of the images will impede crime prevention and detection. If this is the case, the information held about the requester is exempt from disclosure.

If information requested also contains images of any third party, a judgment should be made as to whether providing these images would involve an unfair intrusion into the third party's privacy or cause unwarranted harm or distress. If this is not the case, the images may be released; however, where this is not the case, it may be necessary to disguise or blur images of the third party to protect their privacy. If it is considered necessary to anonymise footage of third parties, this will be carried out on behalf of the Council by a sub-contracted processor who will guarantee security of images and compliance with Council's policy. Subject access requests from individuals should be made using the standard form :Appendix 5.

Where an individual requests CCTV images of themselves under the Freedom of Information Act 2000 (FOI), this information is exempt from the Act and the request should be treated as a data protection subject access request. If the images requested under the FOI are those of other people, they can only be disclosed if this does not breach the data protection principles. If individuals could be identified from the CCTV images, the images are personal information about them and it is unlikely that this information can be disclosed, as it may be unfair processing in contravention of the Data Protection Act.

5.7 Requests from Outside Bodies for Disclosure of CCTV Images

Requests for the disclosure of images may come from the Police Service of Northern Ireland (or other agencies such as the Department for Work and Pensions - Benefit Fraud Section). If not disclosing the information requested would be likely to prejudice any attempt by the police to prevent crime or catch a suspect, the information may be released. Requests for disclosure of images from the PSNI should be made using Appendix 4:PSNI Form .

Where the Council decides to disclose personal data to external agencies, this will be done in compliance with the Data Protection Act 2018 and the Data Sharing Code of Practice issued by the Information Commissioner's Office. Where a request for recorded images is received from solicitors, they must sign an undertaking that they will adhere to the Code of Practice and destroy the images/footages once no longer required in any legal proceedings.

5.8 Disclosure Records

Records of each decision made about the disclosure or non-disclosure of personal information and the reasons for the decision must be maintained by the Data Controller named under the council's data protection registration.

All staff queries or issues concerning CCTV should be directed to the Data Controller. Staff who receive subject access requests from the public should provide the person making the request with the relevant form (appendix 5) and direct them to the Data Controller for the Council.

All subject access requests will be dealt with by the Data Controller in consultation with the appropriate Director, Head of Service and local CCTV manager.

5.9 Duties of Staff Who Have Access to CCTV Systems

All staff with access to the Council's CCTV systems must keep personal data secure and not disclose it to anyone without the approval of the Council. Under S170 of the Data Protection Act 2018 there is an offence, which is defined as:

It is an offence for a person knowingly or recklessly—

(a)to obtain or disclose personal data without the consent of the controller,

It is essential Staff operating the Council's CCTV systems have read and understand both the CCTV and the Data protection policy.

5.10 Retention of Images

The CCTV system operates in such a way that information recorded is automatically overwritten after intervals ranging from 14 to 31 days (dependent on the type of equipment in use at each location).

If images need to be retained for any of the other reasons set out above they will be retained on a secure suitable media device and this will be recorded and kept only for as long as required.

Recorded images for use by Mid Ulster District Council will be kept for the minimum period necessary, i.e., until closure in the event of an investigation/disciplinary/appeal processes, in accordance with the Council's Retention and Disposal Schedule and then destroyed or erased.

6.0 ROLES AND RESPONSIBILITIES

The overall responsibility for implementing Council's Data Protection Code of Practice as it relates to CCTV rests with the Chief Executive.

Each Director is responsible for managing the Council's CCTV network within their own facilities/areas. Heads of Service/lead officer (e.g. facility managers) act as the Data Controller for their service and are responsible for carrying out Privacy Impact Assessments on the use of CCTV in their services.

The Council’s Data Controller is responsible for the management of centralised CCTV records, for providing advice and support as required and for liaising with the Information Commissioner’s Office when required.

Responsibility for the day-to-day management and use of authorised CCTV systems is delegated to appropriately designated local facility managers in conjunction with the responsible Director, Assistant Director, Head of Service or Lead Officer.

Staff who are authorised to have access to the CCTV system are required at all times to comply with the Council policy and procedures governing its use.

Staff who are not authorised to use the CCTV system must not attempt to access or view images or system records.

7.0 IMPACT ASSESSMENTS

7.1 Equality Screening

7.1.1 The policy shall be subjected to equality screening in accordance with the council's screening process.

7.1.2 Rural Needs Impact Assessment

The Policy shall be subjected to rural equality screening in accordance with Councils procedures and Rural Needs Act (NI) 2016.

7.2 Staff & Financial Resources

7.2.1 No issues have been identified which would significantly impact on the council's resources and delivery of its business as a result of this policy being implemented.

8.0 SUPPORT AND ADVICE

8.1 Advice and guidance on the implementation of this should be sought from the Head of IT or the Councillor Solicitor.

9.0 COMMUNICATION

9.1 All staff will have access to this policy published on the intranet and a hard copy on request from their manager.

10.0 MONITORING & REVIEW ARRANGEMENTS

10.1 Implementation of this policy will be monitored and a formal review undertaken 48 months from its effective date or earlier in the event of legislative changes.

Privacy impact assessments will be reviewed in conjunction with the policy review to establish whether the continued use of CCTV is still justified and proportionate.

1 Appendix one

DPIA screening checklist

☐ We consider carrying out a DPIA in any major project involving the use of personal data.

☐ We consider whether to do a DPIA if we plan to carry out any other:

☐ evaluation or scoring;

☐ automated decision-making with significant effects;

☐ systematic monitoring;

☐ processing of sensitive data or data of a highly personal nature;

☐ processing on a large scale;

☐ processing of data concerning vulnerable data subjects;

☐ innovative technological or organisational solutions;

☐ processing that involves preventing data subjects from exercising a right or using a service or contract.

☐ We always carry out a DPIA if we plan to:

☐ use systematic and extensive profiling or automated decision-making to make significant decisions about people;

☐ process special-category data or criminal-offence data on a large scale;

☐ systematically monitor a publicly accessible place on a large scale;

☐ use innovative technology in combination with any of the criteria in the European guidelines;

☐ use profiling, automated decision-making, or special category data to help make decisions on someone's access to a service, opportunity, or benefit;

☐ carry out profiling on a large scale;

☐ process biometric or genetic data in combination with any of the criteria in the European guidelines;

☐ combine, compare, or match data from multiple sources;

☐ **process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;**

☐ **process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;**

☐ **process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;**

☐ **process personal data that could result in a risk of physical harm in the event of a security breach.**

☐ **We carry out a new DPIA if there is a change to the nature, scope, context, or purposes of our processing.**

☐ **If we decide not to carry out a DPIA, we document our reasons.**

Appendix two

ICO_DPIA_Template_V4_ (1).docx

ICO_DPIA_guidance_V3_FINAL_PDF.pdf

Appendix 3

Current list of All premises with Camera Installed (as Oct 2022)

Location	Purpose
Cookstown Council Office (15 cameras)	See Section 2.2 Policy
Magheraglass LFS (7 cameras)	See Section 2.2 Policy
Moneymore Recreation Centre and Moneymore Recycling Centre (14 cameras)	See Section 2.2 Policy
Cookstown Leisure Centre (47 cameras)	See Section 2.2 Policy
Ballyronan Marina (14 cameras)	See Section 2.2 Policy
Burnavon Theatre (11 cameras)	See Section 2.2 Policy
Cookstown Recycling Centre (16 cameras)	See Section 2.2 Policy
Tullyvar Landfill site (10 cameras)	See Section 2.2 Policy
Technical Service Depot Dungannon (12cameras)	See Section 2.2 Policy
Dungannon Leisure Centre (16 cameras)	See Section 2.2 Policy
Coalisland Civil Amenities (8 cameras)	See Section 2.2 Policy
Drumcoo Civil Amenities (15 cameras)	See Section 2.2 Policy
Ranfurly House (12 cameras)	See Section 2.2 Policy
Dungannon Council Offices (16 cameras)	See Section 2.2 Policy
Maghera Leisure Centre (18 cameras)	See Section 2.2 Policy
Killymeal Road (6 Cameras)	See Section 2.2 Policy
Bridewell (7 cameras)	See Section 2.2 Policy
Magherafelt Council Office (2 cameras)	See Section 2.2 Policy
Seamus Heaney Home Place (21 cameras)	See Section 2.2 Policy
Meadowbank (24 cameras)	See Section 2.2 Policy
Greenvale Leisure Centre (51 cameras)	See Section 2.2 Policy
Tobermore Civil Amenity (2 cameras)	See Section 2.2 Policy
Draperstown Civil Amenity (2 cameras)	See Section 2.2 Policy
Magherafelt Civil Amenity (4 cameras)	See Section 2.2 Policy
Maghera Civil Amenity (2 cameras)	See Section 2.2 Policy
Castledawson Civil Amenity (2 cameras)	See Section 2.2 Policy
Ballymacomb Landfill (4 cameras) currently out action)	See Section 2.2 Policy
Magherafelt Council Depot (17 cameras)	See Section 2.2 Policy
Mid Ulster Sports Arena (16 cameras)	See Section 2.2 Policy
Fairhill Bowling Green and Toilet (2 cameras)	See Section 2.2 Policy
Cookstown Town centre	See Section 2.2 Policy
Dungannon Town centre	To enhance the safety and well-being of staff and the public using Council premises, services, and town centres;
Magherafelt Town centre	
Draperstown	

Appendix 4:

PSNI CCTV Request Form

Mid Ulster District Council
CCTV System

PSNI CCTV Request for Data from Mid Ulster District Council

THIS FORM IS TO BE USED WHEN PSNI OFFICERS OR OTHER STATUTORY AGENCIES ARE APPLYING FOR DATA FROM THE CCTV SYSTEM

The completed form should be forwarded to:
Public CCTV :PCSP Manager Mr Michael McCrory, (michael.mcrory@midulstercouncil.org)
Internal CCTV: Barry O'Hagan, the Data Controller for Mid Ulster District Council)at the Dungannon Office, 15 Circular Road, Dungannon, BT71 6DT. Tel: 03000 132 132, **Email: ict@midulstercouncil.org**

DETAILS OF THE OFFICER INVESTIGATING:

Name -	Organisation - PSNI
Rank & Number (if applicable) -	Station/Office -
Tel -	Signature - Date -

Applications made under Section 29 of the Data Protection Act 1998

What information are you requesting? (Please specify date, time, and location)

Details of the person(s)/incident(s) you are investigating Name(s) (if known), description(s), vehicle(s) etc.

INTERNAL USE ONLY

Request Approved/Denied by:

Name: _____ Position: _____

Date: _____ **PRIVATE AND CONFIDENTIAL**

Appendix 5
Standard CCTV Request Form

THIS FORM IS TO BE USED WHEN INDIVIDUALS ARE APPLYING FOR DATA FROM MID ULSTER DISTRICT COUNCIL'S CCTV SYSTEM

Section 1 About Yourself The information requested below is to help the Council (a) satisfy itself as to your identity and (b) find any data held about you. PLEASE USE BLOCK LETTERS		
Title:	First Name(s):	Surname/Family name:

Your Current Home Address (to which we Will reply)	
	Post Code
Day Time telephone number~: (In case we need to contact you)	Mobile
	Landline
Email (preferred method of contact)	

Section 2 Proof of Identity

To help establish your identity you must show us **one** official document showing your name and current address and provide a recent, full-face photograph of yourself e.g. Passport, Driving License.
Failure to provide this proof of identity may delay your application

Section 3 To Help Us Find the Information

If the information you have requested refers to a specific incident or offence, please complete this section.

Please complete a separate box in respect of different categories/incidents/involvement. Continue on a separate sheet if necessary.

Were you?: Please tick box(s) ✓

A person reporting an offence or incident	
A witness to an offence or incident	
A victim of an offence	
A person accused or convicted of an offence.	

Other - please explain briefly

Date(s) of Incident (s)	**time(s) of incident(s)**

Place where incident Happened	

Brief details of Incident

Declaration (to be signed by the applicant)

The information that I have supplied in this application is correct and I am the person to whom it relates

Signed by ..... Date .....

Warning - a person who impersonates or attempts to impersonate another may be guilty of an offence

Before returning this form please check:

- **Have you completed ALL sections of this form?**
- **Have you brought/enclosed ONE official document showing your name and current address and provided ONE recent photograph?**
- **Have you signed and dated the form?**

OFFICIAL USE ONLY

Please complete ALL of this section

Application checked and legible ? Date Application Received

Identification documents checked? Fee Paid

Details of documents (see page 2) Method of Payment

Receipt No

Documents Returned

Member of Staff completing this Section:

Signature Date

ICT Security Policy

Document Control			
Policy Owner	Head of IT		
Policy Authors	Barry O'Hagan		
Version	V2.0		
Consultation	Senior Management Team Heads of Service Trade Unions	December 2022 Yes yes	
Equality Screened by	Yes	**Date**	30/03/2023
Equality Impact Assessment	No	**Date**	
Approved By	Previously Policy & Resources Committee Pr158/17	**Date**	
Adopted By	Previously Council sept 2017	**Date**	
Rural Needs Assessment	Yes	**Date**	30/03/2023
Review Date	36 months from date of adoption	**By Whom**	Head of ICT
Circulation	Councillors, Staff, Intranet		
Document Linkages	Information Security &IT Governance Policy Data Protection Policy Mobile Phone Policy Email and Instant Messaging Policy Internet Usage Policy Removable Media Policy Disciplinary policy Code of Conduct for Local Government Employees		

CONTENTS PAGE

Paragraph	Description	Page Number
1.0	INTRODUCTION	3
2.0	POLICY AIM & OBJECTIVES	3
3.0	POLICY SCOPE	4
4.0	LINKAGE TO CORPORATE PLAN	4
5.0	PROCEDURE & IMPLEMENTATION	5
5.1	Security of Assets	6
5.2	User Account Management	8
5.3	Reporting of Security Incidents	9
5.4	Laptops & Portable Devices	9
5.5	Internet Access	11
5.6	Disposal of Equipment	12
5.7	Desktop Computer Systems	12
5.8	Asset Management	13
5.9	Anti-Virus, Malware and Ransomware	13
6.0	POLICY COMPLIANCE	17
7.0	ROLES & RESPONSIBILITIES	17
8.0	IMPACT ASSESSMENT	17
8.1	Equality Screeing & Impact	17
8.2	Staff & Financial Resources	17
9.0	SUPPORT, ADVICE & COMMUNICATION	18
10.0	MONITORING & REVIEW ARRANGEMENTS	18
	Appendix1: Password Guidance	
	Appendix 2 Reporting of Security Incidents	
	Appendix 3:Incident reporting Form	

1.0 INTRODUCTION

This policy describes the controls and processes put in place to maintain the confidentiality, integrity and availability of the technological system and thereby the information stored and processed on Council IT infrastructure.
The information stored within Council systems are increasingly valuable corporate asset and it is therefore essential that it is protected against known and emerging threats.

The provision of services must not be jeopardised by any breach, loss or unavailability of our information systems.

Compliance is mandatory

2.0 POLICY AIM & OBJECTIVES

2.1 **Policy Aim**: This policy aims to preserve the confidentiality, integrity and availability of our information.

They can be defined as follows:

Confidentiality: access to data and information shall be confined to those authorised to have access to it.

Integrity: information shall be accurate and complete. All systems, assets and networks will operate correctly and to specification

Availability: information shall be available and delivered to the right person at the time it is required.

The objectives of this policy are:

- To protect the organisation's business technological assets and information and any client or customer information within its custody or safekeeping by safeguarding its confidentiality, integrity and availability.

- To establish safeguards to protect the organisation's information resources from theft, abuse, misuse and any form of damage.

- To establish responsibility and accountability for Information Security in the organisation.

- Maintain the integrity of the data.

- Prevent unintended or deliberate consequences to the stability of Council's computer network.

- Avoid contravention of any legislation, policies or good practice requirements.

- Build confidence and Council in the data that is being shared between systems.

- Maintain high standards of care in ensuring the security of sensitive information.

- Prohibit the disclosure of information as may be necessary by law.
- To encourage management and staff to maintain an appropriate level of awareness, knowledge and skill to allow them to minimise the occurrence and severity of Information Security incidents.
-
- To ensure that the organisation can continue to provide activities in the event of significant Information Security incidents.
-
- To provide suitable coverage of International Standards ISO 17799 and BS 7799.

3.0 POLICY SCOPE

This policy applies to all areas of information technology and information management including:

This list is not exhaustive and will continue to reflect emerging technologies as they become available.	
Personal computers, laptops and computer	Mobile phone devices, cameras and internet or network enabled devices
Server, printers and all network devices	Software systems hosted and provisioned locally
All telecommunications ,Telephones and data networks	All devices and media containing data including storage devices, cards and devices containing same

The policy applies to all Councillors, staff and volunteers of the Council, contractual third parties and agents of the Council who have access and are authorised to access Councils IT systems.

4.0 LINKAGE TO CORPORATE PLAN

4.1 Referring to Mid Ulster District Council's Corporate Plan 2020-24, this policy contributes toward the delivery of Corporate Theme 4: Environment..

Controls that underpin this policy

- **Technical Security Controls**
- **Culture and Awareness**
- **Risk Management**
- **Personnel Security**
- **Physical Security**
- **Security Incident Management**
- **Information Security Controls**
- **Governance Controls**
- **Personnel Security**

Legislation and Standards

Users of Council ICT systems must comply with current legislation regarding the use and retention of information and use of computer systems. These include, but are not limited to:

- The Data Protection Act 2018
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990
- Human rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2007
- ISO 27001:Information Security Management
- Criminal Justice Act 2008
- Common Law of Confidentiality
- Digital Economy Act 2010
- Malicious Communications Act 1988
- Human Rights Act 1998
- Regulation of Investigatory Powers Act (RIPA) 2000
- Privacy and Electronic Communications Regulations 2003

5.0 PROCEDURE & IMPLEMENTATION

The Council will use the series of control measures to reduce risk of information loss of confidentiality, availability or its integrity. Those controls include technical controls, staff awareness and training, rules, policies, standard operating procedures and practices in line with good practice and standards such as ISO 27001.

5.1 Security of Assets

Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

Application Access Control

Access to data, system and software shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators, ICT technical staff and third-party support companies and their representatives.

Authorisation to use an application shall depend on the availability of a licence from the supplier. The system owners of each system will regularly conduct access reviews.

Equipment Security

To minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Head of IT . No devices will be connected to the Council network without prior authorisation from IT.

Information Risk Assessment

ICT security risk assessments will be managed and reviewed in line with the corporate risk procedures.

Information security incident, events and weaknesses

All information security events and suspected weaknesses are to be reported to the Head of IT.

Council will monitor Security Incident and Event logs generated by systems through services and systems as resources allow.(typically through security information & event management (SIEM) systems.

As far as resources allow all information security events shall be investigated to establish their cause and impacts with a view to detecting indicators of compromise, breaches and security incident and avoiding similar events in the future, taking automatic controlling actions and playbooks to prevent spread and employ Security Operation Centre (soc) specialists and services to manage same.

Protection from Malicious Software

The organisation shall use technical countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with these measures. Users shall not install software on the organisation's equipment by ICT. Users breaching this requirement may be subject to disciplinary action.

Removable Media and USB Storage Devices

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, must follow the policy and guidance as laid out in the USB and Removable media policy before they may be used on the Council's systems. Such media must be fully encrypted and virus checked before being used on the organisation's equipment by ICT. Users breaching this requirement may be subject to disciplinary action.

Monitoring System Access and Use

An audit trail of system access and data use by staff (where available) shall be maintained and reviewed on a regular basis. Council reserves the right to monitor activity and investigate potential breaches of policy, security incident and alerts. Council may monitor and record communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

Accreditation of Information Systems

The Council shall ensure that all new information systems, applications and networks include a disaster and recovery plan and are approved by the Head of IT before they commence operation.

System Change Control

Changes to information systems, applications or networks shall be reviewed and approved through internal ICT procedures.

Intellectual Property Rights & Licensing

The organisation shall ensure that all information products are properly licensed and approved by the IT service. Users shall not install software on the organisation's property without permission from the IT Service. Users breaching this requirement may be subject to disciplinary action.

Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

Reporting
The Head of IT shall keep the Council informed of the information security status of the organisation by means of regular reports and updates.

5.2 User Account Management

Role of IT Services

The creation, suspension and deletion of user accounts are the responsibility of the Head of Service after approval by Human Resources.

User accounts must not be requested by the individual user but can be requested their supervisor. A copy of these requests will be retained for audit purposes.

All user accounts should be clearly identifiable by the user's roles and responsibilities.

Accounts will be allocated the least privilege access required for the job/Function.

IT service will maintain a list of all staff that have been granted access rights and permission to the system it manages.

Suppliers and support companies must have their own user accounts setup, the Councils password management policy will apply to all accounts.

System-level Passwords

All system-level passwords (e.g., root enabled, Administrator, application administration accounts, etc.) must be changed in line with policy whenever a change in Administrators occurs and for protected stored with the encrypted secured platform where necessary.

User-accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

IT must maintain a list of all staff that has been granted Administrator rights to systems.

Account Housekeeping

Authorised System Manager and Heads of Service should periodically check that all user accounts are still in use. If an account has not been accessed for 28 days then the account may be suspended until either HR or the user's departmental head has been contacted.

Password / Pin Resets

Where a user forget their passwords, a password reset requests will be submitted to IT and issued a new then the Application System Manager may issue a new password but should record the event upon the IT Helpdesk system.

Compromised Accounts
If an account or password is suspected to have been compromised, report the incident to the ICT Service Desk who will in turn suspend and disable the account and report to the Head of Service.

Password / Pin Security

The login password must meet the complexity requirements as specified. These will adjust as per NCSC recommendations and best practice security recommendations.

Passwords must not be written down or inserted into email messages or other forms of electronic communication.

All passwords must be changed after the initial login.

On systems that support this feature Password changes should be unique from previous passwords and be configured to lock out after four unsuccessful attempts.

Role of Supervisor / Manager / Heads of Service

All supervisors / managers are responsible for informing the IT Service Desk and the relevant Application System Manager(s) of the following:-

New Starters – start date and role.
Leavers – leaving date.
Long term sickness – date off work
Maternity leave – date leave commences.
Movements – whereby doing so the user needs differing system access

All such dates should be known before (they occur) due and the supervisor / manager should make every effort to advise the ICT Service Desk / Application System Manager in advance of the date.

Role of IT Service Desk

The IT Service Desk manages user accounts for Active Directory services.

The creation, suspension and deletion of these user accounts is the responsibility of the IT Service.

User accounts must not be requested by the individual user but can be requested via their supervisor, manager or human resources.

The IT Service will retain these requests for audit purposes.
All user accounts should be clearly identifiable by the user's roles and responsibilities.

Role of Human Resources

This department will notify IT of all leavers/changers/new starts including employment agency staff within the Council.

5.3 Reporting of Security Incidents

All suspected or confirmed incidents, breaches or compromises of ICT systems must be reported to a member of the ICT team as soon as possible by any means.

Full details of the incident will be captured on the incident form and notes in Appendix 2 &3.

Please use the mobile numbers available on the helpdesk intranet to contact the ICT Team outside of normal hours.

5.4 Laptops and Portable Devices

Hardware and Software

The IT Service provides all hardware and software which is compatible with Councils systems.

All appropriate hardware and software is procured and installed by the IT Service and users must not install additional hardware or software.

Staff with non-Council IT service provided portable devices are not allowed to connect them to the Councils data Network without prior approval by the ICT service helpdesk.

Unauthorised software downloaded from the Internet must not be loaded onto systems managed and supported by the ICT Service.

Software obtained illegally must not be loaded on a portable device.

Upon termination of employment or contract, the user is required to return all Council owned properties before leaving the Council.

The user will exercise care in using and housing Council owned equipment.

The IT Service may recall laptops and portables devices at any time to audit and update them.

Protection of Portable Hardware

The user is responsible for safeguarding of the portable device hardware. In this case, it means:

- When not in use, portable devices should be kept in a secure location.
- While in transit, portable devices should be in a suitable carrying case and should be kept out of view.
- Portable device security is **always your responsibility**.
- Do **not** leave the portable device unattended in a public place e.g. car park.
- Do **not** keep password details in the same location as the portable device.
- Avoid leaving the portable device within sight of ground floor windows/inside cars/within easy access.

Virus Control

The portable device has an Anti-Virus and other security software package installed by Council's IT Service.

These systems are installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files on the relevant devices. Any users must not alter the configuration of this package.

The anti-virus system's database of virus definitions **must** be updated on a regular basis, each day if possible. This means connecting the portable device to the network/internet for the virus updates to be applied.

Losses and Confidentiality/Security Breaches

Incidents that constitute a loss of hardware or data, which could potentially lead to a breach of confidentiality, are to be reported as soon as possible directly to the IT Service Desk (using the Councils Incident Reporting form to complete the detail).

Where there is a potential for breach in staff or personal data confidentiality, a copy of the Incident Form (see appendix 2) should also be sent to the Director of Corporate & Finance.

Security of Data

Confidential data must only be held on portable devices supplied by the Council where possible which have an appropriate level of encryption implemented.

Each portable device must be suitable encrypted to minimise the loss of any Council Data.

If work is being conducted in public places, meeting rooms and other unprotected areas care should be taken to avoid the unauthorised access to or disclosure of the information stored and processed by the portable device.

Care should be taken by the staff using the portable device to minimise the risk of unauthorised persons overlooking the screen.

Confidentiality Policies apply equally to information whether in the office or at home. Failure to maintain confidentiality may result in a disciplinary action.

Data backup solution is provided centrally on the Councils data network and not on each portable device. **It is the user's responsibility to ensure that their data is stored to the data network, for backup purposes.**

The use of the portable device and the data on it must not be shared with family members.

Accounting/Audit and Legislation

The software and information held on portable devices are subject to the same audit procedures as the Council's desktop computer systems. This also covers information and data stored on removable media e.g. memory sticks, CDs, DVDs.

Users of portable devices must comply with current legislation regarding the use and retention of information and use of computer systems. These include, but are not limited to:

- The Data Protection Act 1998
- Access to Health Records Act 1990
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990

5.5 Internet Access

Internet access is covered by a separate policy within Council published on the Intranet covering the various aspects of internet usage including.

- Personal Use of the Internet
- Acceptable Use of the Internet
- Online Data storage and transfer Websites
- Internet Content Filtering
- Internet Monitoring

Staff should refer to this policy for more information on the proper use of the internet.

5.6 Disposal of Equipment

Due to the increasing dependence on electronic storage systems and the use of disposable media, data disclosure has become a major risk in the operation and decommissioning of media.

Hard Disk Destruction

IT will physically destroy disk drives using a specialist secure disposal service or wipe using NCSC accredited solutions.

CD-ROM/DVD/Solid State Devices (SSD) Destruction

IT will dispose of redundant or damaged CD-ROM /DVD/SSD through the waste service within the Council.

Data Removal and Destruction Management

IT will maintain a secure method of managing the process of data destruction ensuring that all media requiring cleaning or destruction is correctly organised and properly audited.

5.7 Desktop Computer Systems

Hardware and Software

The Council's IT Service provides hardware and software which is compatible with other Council systems.

All appropriate hardware and software is procured and installed by Council IT services. Users must not install additional hardware or software.

Staff with systems that are not provided by IT Service, are not permitted to connect them to the Council data networks.

Software downloaded from the Internet must not be loaded onto systems unless prior authorisation has been given by IT Service.

Software obtained illegally must not be loaded onto any desktop systems within the Council.
Upon termination of employment or contract, the user is required to return all Council owned properties as soon as possible.

The user is required to exercise care in using and housing Council owned equipment.

The IT Service may recall desktop systems at any time to audit their use.

Security of Data

Confidential data must only be installed on desktop systems which have been supplied by the IT Service and have an appropriate level of access security and/or encryption implemented.

If work is being carried out in public places, meeting rooms and other unprotected areas, care should be taken to avoid unauthorised access to or disclosure of the information stored and processed by Council systems.

Care should be taken by the staff using the desktop system to minimise the risk of unauthorised persons overlooking the PC Monitor.

The desktop system has an Anti-Virus software package installed by Council ICT Service.

Losses and Confidentiality/Security Breaches

Incidents that constitute a loss of hardware or data, which could potentially lead to a breach of personal or sensitive data. A suspected loss or breach must be reported directly to the ICT Service using the Councils Helpdesk.

Where there is a potential for breach in staff confidentiality, a copy of the Incident Form Appendix 3 (should also be sent to the Director of Finance.

Accounting/Audit

Users will make their systems available at any time for any audit by the Council.

5.8 Asset Management

Assets Recorded – Hardware

The following hardware items are recorded within the Council ICT Service:

- File Servers
- Network Devices
- Desktop PCs
- Laptops & Tablets
- Monitors (be it part of a Desktop PC Package or separately issued monitor)
- Printers
- Peripherals
- External CD / DVD Burners
- Docking Stations

Assets Recorded - Desktop Software

Software products generally require a license purchased before installation on to the user’s desktop system.

All purchased software must be recorded and their usage monitored.

System Software

A System Asset Register is maintained by the IT service.

Asset Tags

All hardware assets must retain an asset tag as a means of identification within the IT asset database(s).

5.9 Anti-Virus, Malware and Ransomware

All desktop or portable systems which connect to Council's infrastructure or with access to the Internet must have anti-virus software installed where possible.

Desktop Systems

Due to the increasing capabilities of desktop machines and their growing exposure to the Internet, host based anti-virus software must be deployed as a bare minimum.

Typical features will include logging and scan various systems that will be centrally logged and reviewed for indicators of compromise to systems. include:

- **Ransomware ,Malware and Spyware**

  Due to the many possible methods of infection by ransomware, malware and spyware, an effective anti-malware strategy requires equally varied levels of protection. Many of the most popular malware applications collect information which may be valuable to retailers, such as browsing habits or the popularity of certain products. These more minor behaviours can often mask more sinister activities such as password collection or sensitive document disclosure.

Users must not attempt to disable or circumvent any of the features within the anti-virus software
Any virus detection must be reported to ICT via the helpdesk and incident report form in Appendix 3.

Remote Access and Virtual Private network (VPN) gateway Systems

VPN and remote access system includes technologies and hardware that allow remote access to the Council network for remote working.

Due to their exposure, they are particularly vulnerable to attack and, if not correctly protected, can act as the initial infection point of a network.

The software installed on theses will requires Multi Factor Authentication (MFA) to secure access.

The gateway system must use different software to that used elsewhere within the Council's infrastructure. Due to the complex nature of attacks, which may spread through the use of email or network vulnerabilities, the gateway must be able to automatically protect the network when it recognises malicious activity.

This heuristic, or behaviour-based defence, allows the software to automatically block suspected traffic through automatic detection of new viruses or outbreaks.

File Servers and Anti-Virus Exceptions

Apart from dedicated servers (e.g. gateway and email systems), there are often cases in which an anti-virus solution is desirable but due to possible impacts to availability and performance prior consideration is necessary.

On Access scanning or memory resident detection mechanisms may adversely affect high volume servers that demand high availability.

While enterprise class anti-virus solutions can go some way to alleviating these concerns there will always be areas unable to support anti-virus, either through incompatibility with appropriate class software or performance impacts.

In such cases it is often useful to run scheduled scans as frequently as possible during time periods when resource demand is low. If the system will not support this, scheduled maintenance periods will be necessary to perform comprehensive and complete systems scans.

6.0 POLICY COMPLIANCE

Potential breaches of this policy will be investigated and the user may be subject to Mid Ulster District Council's or other relevant disciplinary procedure.

If it is believed that a criminal offence has been committed Council will contact the police and provide the relevant information to assist in the investigation/prosecution of the alleged offender(s).

7.0 ROLES AND RESPONSIBILITIES

7.1 **Council and Chief Executive:** will assume executive authority regarding the implementation of the Policy and delegation through the Director of Finance and the Senior Management Team.

Assistant Directors, Heads of Service and SMT

- Ensure that all staff receive information about this Policy and be part of any local induction where appropriate.
- Ensure that all staff affected understand their responsibility in relation to complying with this policy.

7.3 **Heads of IT** must ensure:

- The implementation of this policy, procedures and controls underpinning it.
- **IT Service** will maintain controls and processes to enforce and monitor within the policy definitions and scope

7.4 **All staff and authorised third parties** are obliged to adhere to this policy

8.0 IMPACT ASSESSMENTS

8.1 Rural Impact Assessment, Equality & Good relations Screening

The policy has been Equality Screened and has been 'screen out' for an EQIA. A Rural Needs Impact Assessment has also been completed.

8.2 Staff & Financial Resources

No issues have been identified which will impact on the delivery of Council business as a result of this policy being implemented.

9.0 SUPPORT, ADVICE AND COMMUNICATION

9.1 Advice and guidance on the implementation of this policy should be sought from the IT Service.

9.2 Information Awareness relating to Information security and IT policies shall be included in the staff induction process. An ongoing awareness programme shall be established and maintained in order to ensure that staff as appropriate receive refresher and update training.

9.3 This policy will be communicated internally using a range of appropriate internal communication methods including intranet, inductions, and team meetings.

9.4 All Elected Members and Directors shall be provided with a copy of this policy. Senior Management Team will make arrangements to ensure it is communicated with their relevant staff.

10.0 MONITORING & REVIEW ARRANGEMENTS

10.1 Implementation of this policy will be routinely monitored and a formal review undertaken 36 months from its effective date.

Appendix 1: Password Guidance

Password Protection Standards

Do not use the same password for Council accounts and for other non-community access (e.g. home internet and email account passwords should not be the same as the one you use at work).

All passwords are to be treated as confidential information.
Below is a list of “don’ts”:

- Do not reveal a password over the phone to ANYONE
- Do not reveal a password in an email message
- Do not talk about details of your passwords in front of others
- Use multifactor Authentication
- Do not hint at the format of a password (e.g. “my family name”)
- Do not reveal a password on questionnaires or security forms
- Do not share a password used at the Council with family members
- Do not reveal a password to co-workers while on holiday
- Do not use the “Remember password” feature of applications
- Do not write passwords down and store them anywhere in the office

If anyone demands your password, refer them to this document or have them call the ICT Service desk.

Compromised Accounts & Passwords:

If an account or password is suspected to have been compromised, **report the incident to the ICT Service Desk straightaway**. The incident will be recorded by the ICT Security Service. Such passwords must be changed immediately.

The ICT Service can at any time suspend a user’s access if it is believed they are sharing account details with others.

Unattended Equipment and Clear Screen:

Users must ensure that they protect the network from unauthorised access. Users must log off the network when they have finished working.

Users must ensure that any equipment logged on to the network be protected if they leave it unattended, even for a brief time.

If a PC is left unattended for a brief time the user will be required to re-input their password to reactivate the session in line best practice.

Appendix 2 Reporting of Security Incidents

What is an Information Security incident?

An information security incident is an event which may compromise the confidentiality, existence, accuracy or availability of stored information. Normally, these incidents violate the Council's policy or Government Laws and involve data or a computer resource owned or operated by the Council. Computer resources owned by the Council include, but are not limited to the following:

- Email accounts, User IDs and passwords issued by the Council for use on the Council applications/systems.
- Hardware and software licensed or leased by the Council.
- Network resources, including network devices and IP addresses owned by the Council.

- In general, an Information Security Incident is any event that results in or could have resulted in:
- Disclosure of confidential information to an unauthorised person.
- The integrity of the system or data being compromised
- Financial loss as a result of using IT system to perpetuate the incident.
- Disruption of information processing systems.
- Inappropriate use of the Councils ICT systems such as email and Internet activity.

What should I do if I encounter a computer security incident?

Gather as much information as you can and make sure you include the collected details on the Incident Reporting Form or via the ICT Helpdesk.

Details should include:

- Date, time and type of incident
- Names of known persons involved in the incident
- IDs or identifying information of persons/machines involved in the incident
- Print outs/copies of any supporting documentation regarding the incident, including headers and logs.

NOTE: Do not delete or destroy any supporting documentation that may be needed as evidence, for example, an email containing harassing content.

To whom should I report computer security incidents?

The ICT Service is the crucial point of contact for all computer security incidents at the Council. All computer and network security incidents should be reported to one of the following, as appropriate:

- Head of ICT and in their absence a member of the ICT team.
- The ICT Service Desk or .ict.helpdesk@midulstercouncil.org
- You must also fill in the Councils Incident form available on the helpdesk
- Your immediate Supervisor

Some examples of information security incidents

Examples of activities which constitute information security incidents include, but are not limited to:

Password is compromised	You discover that someone else has access to your account using your password, or others are misusing passwords. Obtaining, possessing, using, or attempting to use someone else's password regardless of how the password was obtained (e.g. password sharing).
Unauthorised Access	Accessing, or attempting to access, another individual's data or information without proper authorization Unauthorised access to data or files
Computer Virus infection /Virus Infection on a device	You find your computer running unwanted ransomware, strange warning pop-ups, software, behaving uncharacteristically and the computer
Hacking attempt	Usually, systems disable accounts where the wrong password was entered many times. If your account was disabled because someone else was attempting to access it then a security incident has occurred.
Misuse of Email and Internet	Inappropriate use on the Councils Email and Internet services, this may include: Accessing inappropriate or unauthorised inappropriate) than web sites Excessive personal use Using Email to harass staff or to disclose information. Transmitting of sensitive or person identifiable information in unencrypted form
Unauthorised People Using or Attempting to Use IT Equipment	This particularly applies to areas where sensitive data is processed. Only authorised and appropriately trained individuals should have access to ICT systems containing sensitive data of the Council. Also this could involve using the Council's resources for unauthorised purposes (e.g. using personal computers connected to the Council network to set up web servers for illegal, commercial or profit-making purposes).
Computer Files Missing	Self-explanatory
Theft/Loss of IT Equipment	A theft or loss is an information security incident if it means that information is lost or made available to others.
Unexplained Changes to System Data / Configuration	Any unexplained change to system data

Appendix 3

IT Security Incident Reporting Form

Instructions: This form is to be completed as soon as possible following the detection or reporting of an Information Technology (IT) security incident. All items completed should be based on information that is currently available. This form may be updated and modified if necessary.

1. Contact Information for this Incident	
Name:	
Title:	
Work Phone:	
Mobile Phone:	
Email address:	

2. Incident Description.

Provide a brief description:

3. Impact / Potential Impact Check all of the following that apply to this incident.

☐ Loss / Compromise of Data	☐ Other Organisations' Systems Affected
☐ Damage to Systems	☐ Damage to the Integrity or Delivery of Critical Goods, Services or Information
☐ System Downtime	☐ Violation of legislation / regulation
☐ Financial Loss	☐ Unknown at this time

Provide a brief description of the impact:

Provide a brief description of data that was compromised:
5. Who Else Has Been Notified?
Provide Person and Title:
6. What Steps Have Been Taken So Far? Check all of the following that apply to this incident.

☐ No action taken ☐ System Disconnected from network ☐ Updated virus definitions & scanned system	☐ Restored backup from tape ☐ Log files examined (saved & secured) ☐ Other – please describe:

Provide a brief description:
7. Incident Details

Date and Time the Incident was discovered:	
Has the incident been resolved?	
Physical location of affected system(s):	
Number of sites affected by the incident:	
Approximate number of systems affected by the incident:	
Approximate number of users affected by the incident:	
Please provide any additional information that you feel is important but has not been provided elsewhere on this form.	

Please submit this completed form to: Head of ICT

Barry.ohagan@midulstercouncil.org

&

mailto:ict@midulstercouncil.org

Internet Use Policy

Document Control			
Policy Owner	Head of IT, Barry O'Hagan		
Policy Author	Head of IT, Barry O'Hagan		
Version	2.0		
Consultation	Senior Management Team Yes Trade Unions Yes		
Equality Screened by	Yes	**Date**	
Equality Impact Assessment	N/A	**Date**	
Good Relations	Yes		
Approved By	(Policy & Resources)	**Date**	
Adopted By	Council	**Date**	
Review Date		**By Whom**	
Circulation	Councillors, Staff, Intranet		
Document & legislation Linkages and	Mobile Phone Policy Email and Instant Messaging Policy The Privacy and Electronic Communications Regulations (PECR) Data Protection Policy ICT Security Policy Social Media Policy CCTV Policy Disciplinary Policy Code of Conduct for Local Government Employees		

CONTENTS PAGE

Paragraph	Description	Page Number
1.0	Introduction	3
2.0	Policy Aim & Objectives	3
3.0	Policy Scope	3
4.0	Linkage to Corporate Plan	3
5.0 5.1 5.2 5.3 5.4 5.5 5.6	Procedure & Implementation Personal Use of the Internet Acceptable Use of the Internet Online Data storage and transfer Websites Internet Content Filtering Internet Monitoring Policy Compliance	4 4 4 5 5 5 6
6.0	Roles & Responsibilities	6
7.0	Impact Assessment • Equality Screening & Impact • Staff & Financial Resources	7
8.0	Support & Advice	7
9.0	Communication	7
10.0	Monitoring & Review Arrangements	7

1.0 INTRODUCTION

Mid Ulster District Council provides internet access for work related purposes including accessing applications, information, to facilitate research and to conduct business.

However, it is recognised that the use of the internet does have associated risks so it is important that users do not misuse the internet facility and comply with the latest guidance, relevant legislation so to avoid the main risks which when used incorrectly could :

- Damage to reputation of Council as a result of misuse of the internet on Council provided devices.
- The interruption or contamination of Council information system's confidentiality, integrity and availability as a result of the introduction of viruses, ransomware and/or loss of personal data.

This policy outlines your responsibilities as a user and tells you how the internet facility provided by Council should be used.

2.0 POLICY AIM & OBJECTIVES

2.1 **Policy Aim**: This policy establishes a framework for the use of the Internet within the Council

2.2 **Policy Objectives:**

- To ensure that users understand how to conduct themselves legally, honestly and appropriately while using the internet safely.
- To protect Council and its users from legal action as a result of misuse of the internet
- To promote safe use of the internet for work related purposes.
- To establish the responsibilities of users whilst using the Council internet facility
- To help mitigate the informational security risks associated with internet use and establish good governance.

3.0 POLICY SCOPE

3.1 This policy applies to **all users** of Council provided internet-enabled devices and networks.

3.2 All users are expected to comply with this policy at all times when using the Council internet facility or when using any Council owned internet-enabled devices.

3.3 This policy does not include guidance on the acceptable use of Social Media, this can be found separately in Council's Social Media Policy which is available on the intranet.

4.0 LINKAGE TO CORPORATE PLAN

4.1 Referring to Mid Ulster District Council's Corporate Plan 2020-24, this policy contributes toward the delivery of Corporate Theme 4: Environment.

5.0 PROCEDURE & IMPLEMENTATION

This section outlines the framework for the use of the internet facility provided by Mid Ulster District Council

5.1 Personal Use of the Internet

5.1.1 The internet may be used for reasonable personal use outside of core hours i.e., when clocked out from time management , e.g., during breaks, before/after core hours provided that the use is in accordance with this policy, technical controls allow same and it does not interfere with your work, colleagues or Council.

5.1.2 Personal use of the internet is a privilege and not a right, this privilege may be modified or withdrawn at any time at the discretion of your line manager or by IT services to safeguard the Council.

5.1.3 Personal use of the internet is subject to the same conditions as for business use which includes restrictions to certain categories of website as well the monitoring and recording of activity.

5.1.4 No adjustments will be made to web filtering categories for personal use of the internet.

5.2 Acceptable Use of the Internet

5.2.1 The internet must be used in an acceptable manner to help mitigate risks associated with misuse, the internet must **not be used to do the following**:

- Create, download, upload, display or knowingly access any unsuitable material including anything that is obscene, libelous, offensive, discriminatory, defamatory, harassing, pornographic or illegal in nature.
- Access or attempt to access any unauthorized areas, also known as ‘hacking.’
- Access personal web-based email accounts(councillors may access their personal email on non-corporate networked devices such as iPads).
- Subscribe to or use any form of online gaming or gambling websites.
- Subscribe to or use any form of online chat facility including chatrooms and web-based messengers besides Council Cisco Jabber, Teams and Zoom services.
- Download, access or distribute copyright protected material where a license or permission from the copyright owner is not held to do so.
- Publish defamatory and/or false material about the Council, members, employees or anyone else associated with the Council anywhere online.
- Publish or distribute confidential information about the Council online including financial information, personal information or details of staff discussions.
- Download and introduce onto the Council network any software that is knowingly malicious, unlicensed or may damage Council’s systems or reputation.
- Carrying out any activities that will breach relevant legislation including, but not limited to, the Data Protection Act 1998 or the Computer Misuse Act 1990

- Express personal views which could be misinterpreted as being those of the Council anywhere online.
- Run a personal business or carry out any commercial activities.
- Access personal social media platforms profiles

5.2.2 The above list is an example of unacceptable use but it is not exhaustive.

5.3 Online Data Storage and Application access

5.3.1 **Data must not be stored on unapproved online storage websites.** Access to online storage websites including dropbox, WeTransfer etc. is not allowed as there are security risks with using such websites. ICT will provide a suitable secure arrangement to transfer and scan inbound large files using these services if necessary to recipients.

5.3.2 Council has approved the use of Microsoft OneDrive to share data that cannot be emailed including large files.

5.3.3 OneDrive can be accessed using your network login details.

5.3.4 A guide on using OneDrive is available on the intranet and Helpdesk knowledge base.

Multifactor controls are enabled to secure trysted access to hosted applications. Multifactor authentication details ,mobile devices and tokens must only be used by those they have been allocated to and setup for.

5.4 Internet Content Filtering

5.4.1 Internet access is subject to various technical controls based on Automate intelligence learning from Firewall to control safe access. Council makes use of a content filtering system to prevent access to content or sites considered to be unacceptable for use at work and prevent security breaches.

5.4.2 If you are prevented from accessing a business-related website you should create a ticket on the ICT helpdesk with details on the website in question.

5.4.3 The content filtering system uses a list of categories to determine whether access to a website will be granted or not.

5.4.4 Each user with internet access is assigned as a member of an access group depending on business requirements, each access group is configured to allow or deny access.

5.5 Internet Monitoring

5.5.1 All internet activity is logged by the security systems in accordance with current best practice and monitored.

5.5.2 Monitoring is facilitated to ensure that the internet is being accessed in accordance with this policy and you should have no expectation of privacy regarding your internet activity.

5.5.3 An internet access report that provides information on the internet usage of all users will be generated each month and emailed to your supervisor.

5.5.4 Supervisors can request more detailed individual user reports at their own discretion from the ICT Service.

5.6 Policy Compliance

5.6.1 Potential breaches of this policy will be investigated and the user may be subject to Mid Ulster District Council's disciplinary procedure.

5.6.2 If it is believed that a criminal offence has been committed as a result of internet misuse further action may be taken to assist in the prosecution of the offender(s)

6.0 ROLES AND RESPONSIBILITIES

6.1 **Council and Chief Executive:** will assume executive authority with regard to the implementation of the Internet Use Policy and delegation through the Director of Finance and the Senior Management Team.

6.2 **ICT Service** is responsible for the following:

- Management and maintenance of all Council owned internet-enabled devices, internet connections and content filtering system.
- Manage technical aspects of the content filtering system.
- Provide monthly internet activity reports to SMT and Heads of Service
- Provide individual user reports as requested.

6.3 **Heads of Service, Assistant Directors and SMT** must ensure:

- The implementation of this policy and procedures.
- Ensure that all staff receive information about this Policy and be part of any local induction where appropriate.

6.4 **Elected Members and staff:** All elected members and staff who use Council provided internet or internet-enabled devices are obliged to adhere to this policy, process the information and use the internet in accordance with all legislation including Data Protection and Human Rights legislation.

7.0 IMPACT ASSESSMENTS

7.1 Equality & Good relations Screening & Impact

The policy has been subjected to equality screening in accordance with the Council's screening process. The outcome of the screening has screened this policy out.

7.2 Rural Needs Impact

The policy has been subjected to a rural needs impact assessment and this policy has considered the assessment during the policy development.

7.2 Staff & Financial Resources

7.2.1 No issues have been identified which will impact on the delivery of Council business as a result of this policy being implemented.

8.0 SUPPORT AND ADVICE

8.1 Advice and guidance on the implementation of this policy should be sought from the ICT Service.

9.0 COMMUNICATION

9.1 This policy will be communicated internally using a range of appropriate internal communication methods including intranet, inductions and team meetings.

9.2 All Elected Members and Directors shall be provided with a copy of this policy. Senior Management Team are to make arrangements to ensure it is communicated with their relevant staff.

9.3 This policy will also form part of the induction process for all new staff.

10.0 MONITORING & REVIEW ARRANGEMENTS

10.1 Implementation of this policy will be routinely monitored and a formal review undertaken 36 months from its effective date.