Causeway
Coast & Glens
Borough Council

Draft ICT Policies and Procedures	**19 June 2018**
Corporate Policy and Resources Committee **FOR DECISION**	

Linkage to Council Strategy (2015-19)	
Strategic Theme	Leader and Champion
Outcome	Establish key relationships with strategic partners to deliver our vision for this Council area
Lead Officer	Head of ICT
Cost: (If applicable)	

1.0 Introduction

1.1 The General Data Protection Regulation (GDPR) has been enforced from 25th May 2018 and organisations in non-compliance face heavy fines. Appendix 1 lays out draft ICT policies and procedures that reflect adherence to this legislation.

2.0 Detail

2.1 GDPR is designed to harmonize data privacy laws across Europe, to protect and empower the data privacy of all EU citizens and to reshape the way organizations across the region approach data privacy. The United Kingdom is scheduled to depart the European Union (EU) on Friday 29 March, 2019. Irrespective of the specific detail on the final agreement on the UK's withdrawal from the EU, it is widely anticipated that, in the new environment, that we are likely to be governed by similar legislation to GDPR.

2.2 GDPR's impact across our use of technology in Causeway Coast and Glens Borough Council (Council) impacts across a plethora of areas, and specifically in 3 particular areas:

1 How we physically secure our ICT hardware (servers, PCs, laptops, smartphones, etc);

2 What data is stored on those devices and can we justify the storage of said information;

3 Adherence to relevant policies and procedures in relation to the use of this data;

Area 1 is being currently addressed by the ICT Service to ensure that we have the relevant security technology on place. Area 2 is being considered by our Heads of Services in conjunction with our Information Governance Team and our ICT Section. Area 3 is being addressed by us prioritising the adoption of a significant portion of the more substantive policies and procedures that are likely to be under most scrutiny from relevant authorities upon implementation of GDPR.

2.3 The particular Policies and Procedures under scrutiny are:

- Encryption;
- Attempted Intrusion Detection and Monitoring;
- Bring Your Own Device;
- Email Communications;
- Account Privilege;
- Removable Media;
- Patch Management.

3.0 Recommendation

3.1 **It is recommended** that the Corporate Policy and Resources Committee recommend to Council the approval of the draft Policies and Procedures as set out in **Appendix 1**.

Appendix 1

ICT Policy – Encryption Policy No: ICT-101

1. Purpose

This Policy defines standards for the use of Encryption Software on all computers and servers operating in Council. These standards are designed to minimise the risk of loss or exposure of sensitive information, and to reduce the risk of acquiring malicious software such as viruses.

2. Scope

This Policy applies to all users of information assets to include Council employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as “electronic and non-electronic assets owned by Council or entrusted to Council (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software”.

3. Incident Reporting

Users with permission to use encryption software on the Council Network are responsible to secure their devices and information. If you encounter any security issues with Encryption Software you **must** report this as a security incident to the ICT Security Officer.

4. Enforcement

It is the responsibility of the ICT Security Officer to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

ICT Procedure – Encryption Procedure No: ICT-101

1. Requirements

Council recognises that encryption software is a major tool in protecting sensitive data. However, encryption used outside of tightly defined protocols is a threat ICT security.

- Only ICT-provided encryption solutions should be used and controls implemented to insure this.

- Password protection is a form of encryption. Data encrypted in this way cannot be recovered if the password is forgotten.

- It is important that encryption is used when sensitive or personal data is to be sent off the corporate network. Encryption solutions should be provided for email, universal serial bus (usb) flash drives, laptops and portable devices.

- To protect against encryption attempts by users, hackers or malware, all practical steps should be taken, including comprehensive anti-malware, application white-listing and behavioural analysis to detect unusual behaviour.

- Encryption should be used where practical for other valuable/sensitive data within the network eg. databases and backups.

ICT Policy – Attempted Intrusion Detection and Monitoring: No: ICT-204

1. Purpose

This Policy defines standards for proactive intrusion detection and monitoring on all computers, servers and network devices operating in Council. These standards are designed to minimise the risk of loss or exposure of sensitive information, and to reduce the risk of acquiring malicious software such as viruses.

2. Scope

This Policy applies to all users of information assets to include Council employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by Council or entrusted to Council (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

Any ICT staff member who notices an intrusion attempt must log the incident in the Security Incident Log and notify the ICT Security Officer immediately.

4. Enforcement

It is the responsibility of the ICT Security Officer to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

ICT Procedure – Attempted Intrusion Detection and Monitoring: No: ICT-204

1. Requirements

The ICT Security Officer will implement an intrusion detection and monitoring scheme within Council. Intrusion to the corporate network is any unauthorised access and/or action by a human (hacker) or software (malware). Measures should be implemented to:

- Monitor internal and boundary network traffic.
- Identify unusual or malicious activity.
- Block threats to the network at the boundary.
- Implement anti-malware protection throughout the network to detect and nullify any breach.
- Detect and minimise the impact of a successful intrusion.

1. Purpose

This policy is intended to protect the security and integrity of Council data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Council grants its employees the facility to use personal smartphones and tablets of their choosing at work for their convenience. Council reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

Council employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the Council's network.

2. Scope

This Policy applies to all users of information assets to include Council employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by Council or entrusted to Council (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

Users are responsible for their device and **must** report any misuse, loss, or theft as a security incident immediately to the ICT Security Officer.

4. Enforcement

It is the responsibility of the ICT Security Officer to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Requirements

- Personal devices should not be connected to the Council network directly or via a Council client device.

- Acceptable business use is defined as activities that directly or indirectly support the business of Council.

- Devices **must not** be used at any time to:

  - Store or transmit illicit materials
  - Store or transmit proprietary information belonging to another company
  - Harass others
  - Engage in outside business activities

1. Purpose

This Policy defines the requirements to ensure that Email, (including Instant Messaging), is used in an appropriate manner taking into account the confidentiality and sensitivity of information being transmitted.

2. Scope

This Policy applies to all users of information assets to include Council employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by Council or entrusted to Council (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

If you receive any inappropriate or offensive material via email, you **must** report this immediately to the ICT Security Officer.

4. Enforcement

It is the responsibility of the ICT Security Officer to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

ICT Procedure – Email Communications Procedure No: ICT-301

1. Requirements

- Email carries the same legal status as other written documents and should be used with the same care. You **must never** send or distribute abusive, threatening, offensive, profane, lewd vulgar or defamatory emails either internally or to external parties.

- Email should be used solely to communicate with colleagues, customers, suppliers and other interested parties in carrying out Council duties. Personal use may put Council at additional risk and is strongly discouraged.

- You must not send, post, or otherwise distribute chain letters or engage in spamming.

- Email is an inherently insecure method of communication and **must not** be used to send confidential or sensitive information without **appropriate security controls such as data encryption or digital certificates**. If in doubt as to what constitutes confidential or sensitive information, you should check with the ICT Security Officer.

- Ensure that you regularly delete unwanted email items and carry out regular housekeeping on your Inbox/Sent Items.

- Council maintains the right to monitor the content of all email being transported over its network. All email on Council systems remain the property of Council.

ICT Policy – Account Privilege Policy No: ICT-407

1. Purpose

This Policy dictates the various measures and limitations that are enforced on the User Accounts that are in use on Council ICT Systems.

2. Scope

This Policy applies to all users of information assets to include Council employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by Council or entrusted to Council (by internal and external customers) and includes, but not limited to, all documentation, electronic data, products, hardware and software".

3. Incident Reporting

User Accounts are an important aspect of computer security. Users with access to Council systems are responsible for securing their account details. If another user offers you an alternative Network Account, you **must** report this as a security incident to the ICT Security Officer.

4. Enforcement

It is the responsibility of the ICT Security Officer to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

ICT Procedure – Account Privilege Procedure No: ICT-407

1. Requirements

- Users shall only request/receive account privilege on systems they have a true business need to access.

- The relevant line manager will email user information and start date to the ICT Section. This information will specify the user's requirements. The ICT Section will set up the users account as required.

- Authorised groups using Council systems for training purposes will be given a special account limited to the duration of the event.

- Users must read and sign the Password Policy prior to requesting an Account.

- When a user leaves, their account will be locked and 60 days later their account and email will be deleted from the network in compliance with *Leavers Policy ICT-207.*

ICT Policy – Removable Media Policy No: ICT-409

5. Purpose

This Policy defines standards for the use of removable media on all computers and servers operating in Council. These standards are designed to minimise the risk of loss or exposure of sensitive information, and to reduce the risk of acquiring malicious software such as viruses.

6. Scope

This Policy applies to all users of information assets to include Council employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as "electronic and non-electronic assets owned by Council or entrusted to Council (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software".

7. Incident Reporting

Users with permission to use Removable Media on the Council Network are responsible to secure their devices and information. If you encounter any security issues with Removable Media you **must** report this as a security incident to the ICT Security Officer.

8. Enforcement

It is the responsibility of the ICT Security Officer to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

ICT Procedure – Removable Media Procedure No: ICT-409

2. Requirements

Removable Media is any device or media that is readable and/or writeable by the end user, i.e. flash memory devices such as pen drives, cameras, MP3 players; removable hard drives; optical disks such as CD and DVD disks; and any commercial music and software disks.

- Staff **must not** use personal removable media on Council computers or on equipment owned by customers or partners.
- Staff may **only** use removable media provided by the ICT Service which will be in the form of “Encrypted Memory Sticks”.
- Council removable media **must not** be connected to or used in computers that are not owned or leased by Council without explicit permission of the ICT Security Officer.
- Sensitive information should be stored on removable media **only** when required for legitimate business purposes with the approval of the relevant Head of Service.
- When sensitive information is stored on removable media, it must be encrypted in accordance with **Council** Encryption Standards.
- Removable media upon which sensitive information is stored **must** be labelled.

ICT Policy – Patch Management Policy No: ICT- 411

1. Purpose

This Policy defines standards for patch management on the Council network, ensuring all computer devices (including servers, desktops, printers, etc.) have secure virus protection software, current virus definition libraries, and the most recent operating system and security patches installed.

2. Scope

This Policy applies to all users of information assets to include Council employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, customers and functional units regardless of geographic location.

The term information asset is defined as “electronic and non-electronic assets owned by Council or entrusted to Council (by internal and external customers) and includes, but is not limited to, all documentation, electronic data, products, hardware and software”.

3. Incident Reporting

Any Patch security issues **must** be reported as a security incident immediately to the ICT Security Officer.

4. Enforcement

It is the responsibility of the ICT Security Officer to ensure that this policy is kept up to date. Any feedback or comments on this policy should be sent directly to him/her.

1. Requirements

Windows Updates:

- ICT staff **should** install and apply Windows and third party security updates as soon as they are approved by the ICT Infrastructure Team.

- Every effort should be made to test updates before widespread deployment.

- Particular care should be taken in patching server systems, and all changes recorded.