Penrith Town Council

Unit 1, Church House, 19-24 Friargate, Penrith, Cumbria, CA11 7XR
Tel: 01768 899 773 Email: office@penrithtowncouncil.co.uk

INFORMATION SECURITY

PRINCIPLE POLICY

KTD making sense of IT

Penrith Town Council
Policy Pack

SECURITY POLICY PACK

External Approval: W. Cockerill KTD
Effective Date: 9th April 2018

Version: v1.

Issued by: W. Cockerill Effective Date: 9th April 2018

Associated documentation:

1. Contract of Employment and other Council policy documents

2. Penrith Town Council's GDPR Documentation – in particular

    a. Record Management & Retention Policy
    b. Social Media and Electronic Communication Policy
    c. Information Protection Policy
    d. Information Security Incident Policy
    e. Removable Media Policy
    f. Data Protection Policy
    g. Privacy Policy
    h. Staff-Councilor Privacy Policy
    i. SARequests
    j. Password Policy
    k. Staff Handbook
    l. Councillors Code of Conduct

1 Introduction

a. This Security Policy Pack sets out the requirements and responsibilities for maintaining the security of information within Penrith Town Council, preserving the confidentiality, integrity and availability of Penrith Town Council information and ensuring an overall approach to security in which all members of staff and Councillors fully understand. These Policies are a formal set of rules by which those people who are given access to Council technology and information assets must abide.

b. These Policies describe the technology and information assets that must be protected and identifies many of the threats to those assets and inform Council users, employees, contractors and other authorised users of their responsibilities and privileges along with their obligatory requirements for protecting the technology and information assets of the Council. It makes users aware that any breach of this policy and associated policies will be dealt with under Penrith Town Council Disciplinary Procedures.

c. This Security Policy Pack aims to create and maintain a level of security awareness within Penrith Town Council.

d. These policies are supported by related policies and documents to ensure statutory compliance.

e. These Policies shall be reviewed at least annually.

2 Responsibilities

a. Overall responsibility for security sits with the V. Tunnadine, Town Clerk of Penrith Town Council and on a day-to-day basis the Town Clerk shall be responsible for managing and implementing the policies and connected processes and procedures.

b. The Town Clerk is responsible for ensuring that permanent staff, temporary staff and contractors are aware of these Security Policies and how they are applicable in their work areas.

c. The Town Clerk will ensure staff and councilors understand their personal responsibilities for security and how to gain advice on security matters.

d. All staff and councillors shall be responsible for the operational security of the information systems they use, comply with these Security Policies and must understand their responsibilities to protect the Council's data. Failure to do so may result in disciplinary action.

e. Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with these information security policies is in place. Such contracts shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

3 Compliance with Legal Requirements

a. Penrith Town Council must comply with certain UK, European Union and international laws as well as other external guidelines, industry rules and regulations, such as (but not limited to):

- The Health and Safety at Work Act (1974)
- The Data Protection Act (1998)
- The Copyright, Designs and Patents Act (1988)
- Human Rights Act (1998)
- The Computer Misuse Act (1990)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- And the General Data Protection Regulation – GDPR - from 25th May 2018

b. Staff, Councillors and third parties of the Penrith Town Council, may be held personally accountable for any breaches of information security for which they are responsible.

c. It is essential that everyone is aware of their responsibilities and actions required to protect the security of the business and the data we the Council holds

4 Principles for Information Security

a. Penrith Town Council's approach to security shall be based on risk assessments. An overall risk assessment of the information systems is performed annually. Risk assessments will identify, quantify and prioritise the risks according to relevant criteria for acceptable risks.

b. Risk assessments are to be carried out when implementing changes that impact information security. Recognised methods of assessing risks should be employed, such as Cyber Essentials Accreditation and processes and the Information Assurance for Small and Medium Enterprises.

c. Risk assessments must be approved by the Council. If a risk assessment reveals unacceptable risks, measures must be implemented to reduce the risk to an acceptable level.

5 Main Threats

5.1 Employees

a. One of the biggest security threats are employees, who may cause accidental damage to business systems either through lack of awareness of the risk/s or on occasions may be on purpose and cause deliberate purposeful damage.

b. To mitigate the risk of accidental or deliberate damage, security shall be layered to compensate, and Penrith Town Council will:

- Only give out appropriate rights to systems. Limiting access to only business hours, unless required for their role.
- Not share accounts to access systems.
- Not share login information with co-workers.
- Remove or limit access to systems if an employee is disciplined.
- Physically secure computer assets, so that only staff with appropriate need can access them.

6 Security in Connection to Users

6.1 Prior to Employment

a. Security responsibility and roles for employees and contractors shall be described.

b. Information security expectations of staff shall be included within appropriate job descriptions.

c. References shall be verified and a passport, driving license or other document shall be provided to confirm identity.

6.2 During Employment

a. All contracts of employment shall contain a security and confidentiality clause.

b. The IT regulations should be reviewed regularly with all users.

c. A confidentiality agreement should be signed by contractors or others who may gain access to sensitive and/or internal information.

d. IT regulations should be accepted for all employment contracts and for system access for third parties

e. All employees and third-party users should receive adequate awareness, training and updating regarding the Information security policy and procedures.

f. Whenever a staff member leaves the Council their user accounts will be disabled the same day they leave.

g. Whenever a councillor leaves the Council their email account will be disabled the same day they leave.

6.3 Disciplinary for Security Policy Violation

a. Penrith Town Council takes the issue of security seriously. Those people who use the technology and information resources of Penrith Town Council must be aware that they can be disciplined through the Council's procedures should they violate this policy.

b. Upon violation of this policy, an employee of Council may be subject to discipline up to and including discharge. The specific discipline imposed will be determined by a case-by-case basis, taking into consideration the nature and severity of the violation of the Security Policy, prior violations of the policy committed by the individual, country laws and all other relevant information.

c. Discipline which may be taken against an employee shall be administrated in accordance with any appropriate rules or policies within the Penrith Town Council Staff Handbook and relevant policies and procedures.

7 Policy 1 - Access Management, Control & Authorisation

7.1 User Responsibilities and Access

a. This section establishes usage and access rights for the Penrith Town Council computer systems, networks, devices used to access or process any Council information and the information resources themselves.

b. It pertains to all employees and contractors who use the computer systems, networks, and information resources as business partners, and individuals who are granted access to the network for the business purposes of the Council.

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

7.2 Acceptable Use

a. User accounts on Council computer systems are to be used only for business of the Council and not to be used for personal activities. Unauthorised use of the system may be in violation of the law may constitute theft and can be punishable by law. Therefore, unauthorised use of the Council computing system and facilities may constitute grounds disciplinary procedures and either civil or criminal prosecution.

b. Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Furthermore, they are prohibited from making unauthorised copies of such confidential information and/or distributing it to unauthorised persons outside of the Council.

c. Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to Council systems for which they do not have authorisation.

d. Users shall not attach unauthorised devices on their PCs or workstations, unless they have received specific authorisation from the Town Clerk and the Council's IT designee.

e. Users shall not download or install unauthorised software from the Internet onto their PCs or workstations.

f. Users are required to report any weaknesses in the Council computer security, any incidents of misuse or violation of this policy to the Council's IT designee.

Further information:
Social Media and Electronic Communication Policy
Information Protection Policy
Staff Handbook

7.3 User Classification

a. All users are expected to have knowledge of these security policies and are required to report violations to the Town Clerk, Data Protection Officer and the Council's IT designee. Furthermore, all users must conform to the Acceptable Use Section defined in this document at 7.2

b. The Council has established the following user groups and defined the access privileges and responsibilities:

User Category	**Privileges & Responsibilities**
Employees	Access to information, application and databases as required for job function.
The Council's IT designee	Access to computer systems, routers, switches, Wireless Access Systems, and other infrastructure technology required for job function. Access to confidential information on a "need to know" basis only.
The Council's IT designee	Highest level of security clearance. Allowed access to all computer systems, databases, firewalls, and network devices as required for job function.
The Council's IT designee	Access to applications and databases as required for specific job functions. Access to routers and firewall only if required for job function. Knowledge of security policies. Access to Council information and systems must be approved in writing by the Town Clerk
Other Agencies and Business Partners	Access allowed to selected applications only when contract or inter-agency access agreement is in place or required by applicable laws.
General Public	Access is limited to applications running on public Web servers. The general public will not be allowed to access confidential information.

7.4 Access Control

a. A fundamental objective of the Council's Security Policies is controlling access to the critical information resources that require protection from unauthorised disclosure or modification.

b. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorised to access specific resources. Access controls exist at various layers of the system, including the network.

c. Access control is implemented by logon ID and password. Access to information shall be based on the principle of "least privilege" and restricted to authorised users who have a business need to access the information.

7.5 User Access – Normal User (System & Network)

All users will be required to have a unique logon ID and password for access to systems.

7.5.1 Identity and Passwords

a. Passwords must be used to secure access to data kept on IT systems and equipment to ensure that confidential data is protected in the event of loss or theft.

b. Passwords are unique to each user, must be kept confidential and must not be made available to anyone else unless authorised by the Town Clerk.

c. On termination of employment (for any reason) staff must provide details of their passwords to the Town Clerk.

7.5.2 Group Policy

The Council password policy must be configured and enforced by group policy:

Enforce password history	13 passwords remembered
Maximum password age	60 days
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled

7.5.3 Lockout Policy

An account lockout policy should also be group enforced:

Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 mins

7.5.4 Password Complexity

Passwords must meet complexity requirements as set out in the Council's Password Policy document

By following the Council's Policy, Passwords will not be easily guessable. The following list suggests easily guessable passwords as an example but is not limited to:

Usernames	Passwords	admin	administrator	cisco	guest
manager	monitor	operator	public	recovery	security
superuser	support	sysadmin	system	tech	test
User	1234	12345678	Admin	Administrator	Changeme
Changeme2	Cisco	Letmein	Manager	Operator	Password
Password	Password1	Password123	PASSWORD	Passw0rd	recovery

7.5.5 Password Protocol

a. Users are not allowed to access password files on any network infrastructure component.

b. Password files on servers will be monitored for access by unauthorised users.

c. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

d. Users will not be allowed to logon with an Administrator password for their normal activity on the network.

e. The Administrator Password is secured by the Council's IT designee.

f. Employee Logon IDs and passwords will be deactivated as soon as possible if the employee leaves the employment of the Council by the Council's IT designee.

g. The Town Clerk will report change in employee and councillor status that requires terminating or modifying ~~employee~~ logon access privileges.

h. Employees who forget their password must call the IT Company Designee to get a new password assigned to their account. The employee must identify himself/herself and this request must be verified by the Town Clerk.

i. Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee's password and ID.

j. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems, without prior permission from the Town Clerk.

Further information:

Password Policy

7.6 User Access - Administrator-level access

a. Administrator level access and System Administrator access permissions are awarded only to the Council's IT designee.

b. The Council's IT designee will have access to host systems, routers, switches and firewalls.

c. Administrator-level accounts shall not be used for day-to-day activity. Such accounts shall only be used for specific tasks requiring administrator privileges and must not be used to access email or for general web browsing to ensure the minimum exposure to external threats.

7.7 Special Access

a. Special access accounts may be provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are monitored by the Council and require the permission of the Town Clerk.

b. Monitoring of the special access accounts is done by entering the users into a specific area and periodically generating reports to management. The reports will show who currently has a special access account, for what reason, and when it will expire.

c. Special accounts will expire in 90 days and will not be automatically renewed without permission.

7.8 Connecting to Third-Party Networks

a. Third-party refers to vendors, consultants and business partners doing business with Penrith Town Council, and other partners that have a need to exchange information with Penrith Town Council.

b. Third-party network connections are to be used only by the employees of the third-party, only for the business purposes of the Penrith Town Council. There will be a documented business case for this access requirement.

c. Secure Connectivity will be provided between Penrith Town Council and all third-party companies and other entities required to electronically exchange information with the Council.

d. The third-party company will ensure that only authorised users will be allowed to access information on the Penrith Town Council network.

e. The third-party will not allow Internet traffic or other private network traffic to flow into the network.

f. A network connection will terminate on completion of the task and the third-party will be subject to standard Council authentication rules.

g. This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re-designed as needed.

h. All requests for third-party connections must be made by submitting a written request and be approved by the Town Clerk.

7.9 Connecting Devices to the Network

a. Only authorised devices may be connected to the Penrith Town Council network. Authorised devices include Servers, PC's, Laptops or other types of workstations and mobile devices owned by Penrith Town Council that comply with the configuration guidelines of the Council. Other authorised devices include network infrastructure devices used for network management and monitoring.

b. Users shall not attach to the network or to access any Council information any non-Council devices that are not authorised, owned and/or controlled by the Council.

c. Users are specifically prohibited from attaching any personal devices to the Council network or data.

d. NOTE: Users are not authorised to attach any device that would alter the topology characteristics of the Network or any unauthorised storage devices, e.g. USB drives and writable CD's, DVD's. For more information – please refer to the council's Removable Media Policy.

7.10 Remote Access

a. Only authorised persons may remotely access the Penrith Town Council network. Remote access is provided to those employees, contractors and business partners of the Council that have a legitimate business need to exchange information, copy files or programs, or access computer applications.

b. Authorised connection can be remote PC to the network or a remote network to Penrith Town Council network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID / VPN.

Further information:

Removable Media Policy

7.11 Unauthorised Remote Access

a. The attachment of (e.g. switches or hubs) to a user's PC or workstation that is connected to the Council LAN is not allowed without the written permission of the Council's IT Designee.

b. Users may not install personal software designed to provide remote control of the PC or workstation.

c. This type of remote access will try and bypass the authorised highly secure methods of remote access and poses a threat to the security of the entire network.

7.12 Application Access

a. Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.

b. Authorisation to use an application shall depend on a current license from the supplier.

7.13 Hardware Access and System Perimeter access (firewalls)

a. Access beyond the application access level is restricted solely to the Council's IT designee who will ensure that:

- Access to the network shall be restricted to authorised devices only.
- Autorun and auto display must be disabled on any device. An approved business case is required to enable and must be documented and reviewed every 6 months as a minimum.

7.14 System Perimeter access (firewalls)

- The boundary between business systems and the Internet shall be protected by firewalls, which shall be configured to meet the threat and continuously monitored.
- All servers, computers, laptops, mobile phones and tablets have a firewall enabled, if such a firewall is available and accessible to the device's operating system.
- The default password on all firewalls shall be changed to a new password that complies to the password requirements set by the council's Password Policy document and shall be changed every 60 days.
- All firewalls shall be configured to block all incoming connections.
- That if a port is required to be opened for a valid business reason, this must be documented and reviewed quarterly. The change shall be authorised following the system change control process. The port shall be closed when there is no longer a business reason for it to remain open.
- Changes shall be authorised following the system change control process

7.15 Monitoring System Access and Use

a. The Council reserves the right to monitor systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

b. The Council has the capability to monitor electronic information created and/or communicated by persons using Council computer systems and networks, including e-mail messages and usage of the Internet.

c. It is not the Council policy or intent to continuously monitor all computer usage by employees or other users of the Council computer systems and network.

d. Users of the systems should be aware that the Council may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with Council policy.

An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis

8 Policy 2 - Asset Management, Control and Classification

8.1 The Assets we are protecting.

a. It is the obligation of all users of the Penrith Town Council systems to protect the technology and information assets of the Council. This information must be protected from unauthorised access, theft and destruction.

b. The technology and information assets of the Council are made up of the following components:

- Council information or data.
- Physical Computer hardware, devices, email, web, application servers, PC systems, application software, system software, etc.
- System Software including: operating systems, database management systems, and backup and restore software, communications protocols, and so forth.
- Application Software: This includes custom written software applications, and commercial off the shelf software packages.
- Communications Network hardware and software including: routers, routing tables, switches, hubs, modems, firewalls, private lines, and associated network management software and tools.

8.2 Asset Handling and Classification

a. User information found in computer system files and databases shall be classified. The Council shall classify the information controlled by them and shall identify particularly valuable or sensitive information assets.

b. All staff are responsible for handling information assets in accordance with this security policy. Where possible the data classification shall be marked upon the asset itself.

c. The Council is required to review and approve the classification of the information and determine the appropriate level of security to best protect it.

d. Local Area Network (LAN) Classifications. A LAN will be classified by the systems directly connected to it. For example, if a LAN contains just one key information system all network users will be subject to the same restrictions required by that information system. A LAN will assume the Security Classification of the highest-level systems attached to it.

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

f. Records and Management: An accurate record of business information assets, including source, ownership, modification and disposal shall be maintained.

g. Destruction: All data shall be securely wiped from all hardware before disposal.

8.3 Removable media

For more information – please refer to the Council's Removable Media Policy document.

8.4 Mobile working

a. Where necessary, staff may use Council-supplied mobile devices such as phones, tablets and laptops to meet their job role requirements.

b. All devices will be supplied by the Councils IT designee who will ensure that all devices have the appropriate level of Antivirus and separate specific Malware protection enabled, in license and updated within 14 days of security releases and 7 days of any engine updates.

c. Use of mobile devices for business purposes (whether business-owned or personal devices) requires the approval of the Town Clerk. Such devices must have anti-malware software installed (if available for the device), must have PIN, password or other authentication configured, must be encrypted (if available for the device) and be capable of being remotely wiped. They must also comply with the software management requirements within this policy.

d. Users must inform the Town Clerk immediately if the device is lost or stolen and business information must then be remotely wiped from the device.

e. Personal devices / Bring Your Own Device (BYOD) are not allowed to access any information on the network in particular email.

f. No personal devices are to be used to access business information

8.5 Social Media

a. For more information – please refer to the Council's Social Media and Electronic Communications Policy document.

b. Business social media accounts shall be protected by strong passwords in-line with the password requirements for administrator accounts.

9 Policy 3 - Physical and Environmental Management

a. IT equipment and information that require protection should be placed in secure physical areas. Secure areas should have suitable access control to ensure that only authorised personnel have access.

b. In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. IT equipment classified as 'key' must be protected against environmental threats (fires, flooding, temperature variations, etc.). Classification of equipment should be based on risk assessments.

c. Information classified as "sensitive" must not be stored on portable computer equipment (e.g. laptops, cell phones, memory sticks, etc.). If it is necessary to store this information on portable equipment, the information must be password protected and encrypted in compliance with guidelines from the Council.

d. Systems shall be protected from power loss by UPS if indicated by the risk assessment. Systems requiring particular environmental operating conditions shall be maintained within optimum requirements.

10 Policy 4 - Computer and Network Management

10.1 Operations Management

a. Purchase and installation of IT equipment must be approved by the Council.

b. Changes to IT systems should only be implemented if well-founded from a business and security standpoint and approved by the Council.

c. Penrith Town Council shall ensure that all software is properly licensed.

d. Individual and Penrith Town Council intellectual property rights shall be protected at all times. Staff breaching this requirement may be subject to disciplinary action.

10.2 System Change Control

a. Changes to information systems, applications or networks shall be reviewed in conjunction with the Council's IT designee and approved by Counsel.

b. The Councils IT designee will ensure that:
   - Requirements for information security are taken into consideration when designing, testing, implementing and upgrading IT systems, as well as during system changes.
   - Routines are developed for change management and system development/maintenance.
   - IT systems are dimensioned according to capacity requirements. The load should be monitored in order to apply upgrades and adjustments in a timely manner. This is especially important for business-critical systems.
   - All new and modified information systems, applications and networks include security provisions ensuring that they are correctly sized, with appropriate security requirements, be compatible with existing systems according to an established systems architecture (as required) and be approved by Town Clerk before they commence operation.

10.3 Software Management

Users shall not install software or other active code on the devices containing business information.

All application software used must be approved and documented on an approved software list from the Council's IT designee. This software, operating systems and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities.

The Councils IT designee will ensure that:

a. All application software used must be approved and documented on a Council Approved Software List. Software, operating systems and firmware are updated on a regular basis to reduce the risk presented by security vulnerabilities.

b. All software security updates/patches are installed within 7 days of their release.

c. All workstations, servers, software, system components etc. owned by Penrith Town Council have up-to-date system security patches installed to protect the asset from known vulnerabilities.

d. Where ever possible all systems, software have automatic updates enabled for system patches released from their respective vendors. Any exceptions to this process must be documented and approved by the Councils IT designee.

e. Only software which has a valid business reason for its use shall be installed on devices used for business purposes.

f. Software that is not license compliant is brought into compliance promptly or uninstalled.

g. Users shall not install software or other active code on the devices containing business information without permission from Town Clerk and this software must be required to be added to the approved software list for the Council.

h. All unnecessary and unused application software is removed from any devices used for business purposes.

10.4 Local Data Storage

a. All sensitive data stored and handled by Penrith Town Council and its employees must be securely protected against unauthorised use at all times. Any sensitive data that is no longer required by Penrith Town Council for business reasons must be discarded in a secure and irrecoverable manner by the Councils IT designee.

b. Data stored on the business premises shall be backed up regularly and restores tested at appropriate intervals (at least quarterly), by the Councils IT designee.

c. A backup copy shall be held in a different physical location to the business premises. Where the backup resides off site this data should be encrypted. Backup copies of data shall be protected and comply with the requirements of this security policy and be afforded the same level of protection as live data.

10.5 External Cloud Services

The Councils IT designee will ensure that:

Where data storage, applications or other services are provided by another business (e.g. a 'cloud provider') these must be independently audited, and written confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.

10.6 Protection from Malicious Software

The Councils IT designee will ensure that:

a. The business shall use software countermeasures, including anti-malware, antivirus, and management procedures to protect itself against the threat of malicious software.

b. All computers, servers, laptops, mobile phones and tablets shall have anti-malware software installed, where such anti-malware is available for the device's operating system. The antivirus / malware software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits etc.)

c. All anti-malware software shall be set to:

- Retain any logs generated from the antivirus / malware solutions as per any legal / regulatory / contractual requirements
- scan files and data on the device daily
- scan files on-access
- automatically check for, and install, virus definitions and updates to the software itself daily
- block access to malicious websites
- all removable media should be scanned for viruses before being used
- not be able to be modified and any settings changed or altered by end users of the antivirus / malware software

10.7 Vulnerability scanning

The Councils IT designee will ensure that:

a. The business shall have as a minimum, a yearly vulnerability scan of all external IP addresses carried out by a suitable external company.

b. The business shall act on the recommendations of the external company following the vulnerability scan to reduce the security risk presented by any significant vulnerabilities.

c. The results of the scan and any changes made shall be reflected in the Council risk assessment and security policy as appropriate.

11 Policy 5 - Response

11.1 Information security incidents

a. The term "security incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the Council network. Some examples of security incidents are:

   - Illegal access of a Council computer system. For example, a hacker logs onto a production server and copies the password file.

   - Damage to a Council computer system or network caused by illegal access. Releasing a virus or worm would be an example.

   - Denial of service attack against a Council web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.

   - Malicious use of system resources to launch an attack against other computer outside of the Council network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

   - An exposure of Council data to an unauthorised person or company either through error or malicious activity.

b. Employees, who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to Town Clerk immediately.

c. An appropriate response must be initiated, and the exposure or data breach needs to be dealt with by those experienced in such incidents.

d. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.

For more information – please refer to the Council's Information Security Incident Policy document.

11.2 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.

11.3 Reporting

Town Clerk shall keep the business informed of the information security status of the organisation by means of regular reports to senior management.

Authorisation This policy has been authorised by:

Signature:

Date 21 MAY 2018

Name: Cllr. Jackson

Position: **CHAIRMAN OF THE COUNCIL**