## 1.1 Role of Information and Information Systems

The Council is critically dependent on information and information systems. If important information were to be disclosed to inappropriate persons, the Council could suffer serious losses. The good reputation that the Council enjoys is also directly linked with the way that it manages both information and information systems. For example, if a citizen's information were to be publicly disclosed, the council's reputation would be harmed. For these and other important business reasons, the management working in conjunction with Members have initiated and continue to support an information security effort. One part of that effort is definition of this information security policy.

## 1.2 Team Effort

To be effective, information security must be a team effort involving the participation and support of every Council worker who deals with information and information systems. In recognition of the need for teamwork, this policy statement clarifies the responsibilities of users and the steps they must take to help protect Council information and information systems. This document describes ways to prevent and respond to a variety of threats to information and information systems including unauthorised access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use.

## 1.3 Involved Persons

Every employee and members of the Council must comply with the information security policies found in this and related information security documents. Workers or Members who deliberately violate this and other information security policy statements will be subject to disciplinary action up to and including dismissal.

## 1.4 Involved Systems

This policy applies to all computer and network systems owned by or administered by Copeland Borough Council. The policy covers all operating systems, computers, and application systems. The policy not only covers information handled by computers and networks, but the spoken and written word. For information about the protection of information in paper form, see the Asset Classification Section of this document.

## 2 Objectives and Scope

This policy contains the security requirements for the Council Infrastructure including HR, Finance, Internal IT (systems and networks), Development, Security and Facilities. All Council employees and Members must read, sign and adhere to this policy.

Definitions:

**Must** – read as mandatory.

**Should** – read as recommended.

**Confidentiality** – Ensuring that information is accessible only to those authorised to have access.

**Integrity** – Safeguarding the accuracy and completeness of information and processing methods.

**Availability** – Ensuring that authorised users have access to information and associated assets when required.

Exceptions to the policy must be documented and authorised by the Chief Executive.

# 3 Infrastructure

## 3.1 Electronic Communications Systems

### 3.1.1 Who is covered by the policy

All Members, employees, consultants, contractors, temporary agency staff and visitors using the Council's electronic communications systems, including Internet, e-mail, IT storage, mobile and fixed telephones are covered by this policy.

### 3.1.2 Aim of the policy

The aim of this policy is to protect individuals and the Council from the effects of misuse of electronic communications systems and to clarify our policy in this area.

### 3.1.3 Background

The Council is ultimately responsible for all communications conducted via its various communications systems (regardless of whether the individual intends the communication to be personal or business related). As such it may be necessary to monitor use of these systems to ensure that the Council does not break the law, (for example that relating to libel, harassment and criminal acts) or cause harmful effects on the Council's business, its suppliers, customers or associates.

### 3.1.4 Monitoring of communications

The Council reserves the right to monitor Internet access, Intranet access, e-mail use, and the use of mobile and fixed telephones and electronically stored information by using software or other method's dedicated for this purpose to ensure:

(a) Compliance with legislation.

(b) To investigate or detect crime.

(c) If the Council considers in its reasonable opinion, that there is a business risk which requires the use of monitoring.

(d) for the investigation or detection of unauthorised use of the Council's electronic communications system.

(e) For checking compliance with the Council's practices and procedures.

Employees and Members should be aware that security systems to carry out this monitoring are available within Council. *In addition, to protect you, the Council will hold suspect files in quarantine, and may advise you of this. After checking, they will be released to you or sent on to a 3rd party recipient if there is no further problem.*

### 3.1.5 Guidelines for use of communications systems

All employees are expected to use the electronic communications systems in a professional manner and in a manner that does not compromise the Council, its Members or its employees in any way. In respect of use of mobile telephones, we may monitor usage using data provided by telecommunications providers to ensure mobile phones and equipment are being used for business purposes.

#### 3.1.6 Trade Union Representative Access

Trade Union representatives are authorised to use the Council's electronic communication systems for legitimate industrial relations purposes, and in connection with official trade union business.

### 3.2 Unintentional misuse

#### 3.2.1 Unsolicited e-mails

If you receive unsolicited e-mails containing unacceptable content. You must not reply to the e-mail. You should open a IT helpdesk request so that they can take any appropriate action. The e-mail should be deleted from the system to avoid further distribution or access.

If the receipt of such e-mails is a regular occurrence then the sender may be blocked from our system.

#### 3.2.2 Internet access

If you inadvertently access an Internet site containing unacceptable content as indicated above, you should disconnect immediately and bring the matter to the attention of your line manager.

### 3.3 Viruses

No software should be introduced to the system without the specific authority of the Councils IT Section.

Un authorised software will be removed from any PC belonging to Copeland Borough Council

Any files or software downloaded from the Internet or brought from home must be virus checked before use. You should not rely on your own PC to virus check any such programmes but should refer directly to the IT Support Desk; a Helpdesk form must be completed.

#### 3.3.1 Breach of this policy

The Council considers this policy to be extremely important, particularly given the nature of our business and the associated trust our clients place in us. Should you be found to be in breach of the policy then you will be dealt with in accordance with the Disciplinary Procedure and you may be dismissed. In certain circumstances breach of this policy may be considered gross misconduct resulting in immediate termination of your employment.

### 3.3.2 Mobile and fixed telephone use

The Council will issue mobile telephones to staff when a valid business need has been identified and where it is deemed appropriate and necessary by line management. Itemised bills will be received from the nominated service provider on a monthly basis and will be scrutinised to ensure that the abuse or excessive personal use of the Council mobile telephones does not occur.

In the event of an employee abusing the Council mobile service, the mobile may be withdrawn and/or action be taken against the employee in accordance with the Council's disciplinary policy.

Users should be aware that mobile communications are inherently insecure and rendered even more insecure by the fact that the communications device is likely to be used in public places where conversations can be easily overheard. As with fixed line telephones, employee discretion is expected such that no confidential or sensitive information is divulged during the course of a conversation.

# 4 ASSET CLASSIFICATION & CONTROL

## 4.1 Asset Management

All computer hardware and software must be purchased through and delivered by the IT department. All requests for hardware and software will be checked and verified for use by the Council. IT will take delivery of all software and store it in a fire proof safe (where necessary) for future reference.

All software must be installed by the IT department. No other Council employee or Member may purchase software (through credit cards, expense accounts etc) or install software on any machine. All Desktop, laptop and associated hardware will be asset tagged and must be logged in the asset database against the inventory of the purchaser, or the project for which the assets have been purchased. Portable computer equipment must be kept secure.

All staff or department moves must involve the IT department so that the relevant asset databases are updated. Line management must also approve any Council assets that need to be taken off site, either temporarily or on a permanent basis.

All Desktop, laptops and associated hardware are allocated by department, line mangers must approve move of computer equipment between departments.

The IT department must carry out the disposal of all IT hardware and software belonging to Council. IT will manage this process so that information security is controlled.

All of the above needs to be recorded via the IT Support Desk using a Helpdesk form, which will log the request and allocate to the relevant employee.

Audits are conducted regularly to identify software loaded onto all computers and to ensure compliance of these policies and procedures.

### 4.1.1 Information Assets

Much of the Information the Council processes is confidential in nature and any sensitive personal, financial or Council confidential data should not be exposed to risk of loss or unauthorised modification. All Members, employees, consultants, contractors and temporary agency staff are required to sign the Confidentiality Statement.

### 4.1.2 Document Handling

Documentation should be protected using appropriate controls based on the sensitivity of the content. Council confidential documents should be clearly marked as such.

All employees should use their discretion when storing and transmitting sensitive information, distribution lists should be limited to individuals on a 'need to know' basis and any information, that could be damaging to the business if disclosed, should not be transmitted via e-mail.

*As a general rule of thumb, no Council data must be stored, or transmitted, via any form of insecure network transport* Where any doubt exists, the IT Department should be consulted and will advise as to the best method to proceed.

# 5 PHYSICAL SECURITY

## 5.1 Reception areas

As the first line of physical defence, reception areas must never be left unattended during normal business hours and should either be manned or monitored after hours. Reception areas should be considered one of the most important areas of physical security and should always be the first point of contact when visitors enter the Council premises.

### 5.1.1 Personal or Sensitive Data

Any personal or sensitive data must be protected, particularly in a public area, to ensure that it cannot be seen by unauthorised persons.

## 5.2 Visitors

Every visitor entering any Council, or client site at which Council has facilities, should be signed in and out of the building and must be issued with appropriate visitor or guest identification against a signature. This pass must be returned to the point of issue prior to the guest leaving the building.

Visitors must be accompanied throughout the duration of their visit and should be collected from reception areas by the person with whom they are visiting and not permitted to “find their own way”. Under no circumstances must visitors be allowed to wander around Council buildings unaccompanied.

Visitor badges must be clearly displayed at all times and must be returned to reception prior to leaving the building. It is the duty of the Council personnel to ensure that visitors return their visitor badges and that they are escorted from the premises.

All Members and employees have a role to play in keeping the Council secure. Members and employees are encouraged to challenge anyone that they don't recognise, or that is not wearing correct personnel or visitor identification. Where appropriate the visitor should be accompanied back to reception to be assigned a badge, and collected by the person they are visiting.

### 5.2.1 Office Security

Council have adopted a number of physical access control devices and security monitoring technologies in order to ensure that Members and employees are free to operate in a secure working environment. However, care must be taken when accessing personal or sensitive data so that it cannot be seen by unauthorised persons.

### 5.2.2 Access Control

Access to all Council offices is controlled via a centrally managed physical access control system maintained by the Facilities Management. People will be granted access to appropriate areas of the Council premises, at times agreed within the Facilities Management contract.

### 5.2.3 Photo ID Cards

All personnel will be issued with Photo ID cards that identify them as Council personnel and grant them access to the areas required during the normal course of business. If an employee requires access to areas other than those then a request from the appropriate line manager will be required and past to the relevant department for authorisation. All personnel are expected to carry their ID card at all times and any lost or stolen cards must be reported immediately such that access for the lost card can be revoked. A line manager can request temporary pass for and employee from the Customer Services Desk.

### 5.2.4 CCTV

Council offices are fully monitored through the use of CCTV and access control systems and these systems are configured to monitor key areas of the building in order to detect crime and in particular monitor any suspicious activity in order to maintain the highest levels of office security possible.

### 5.2.5 Clear Desk Policy

The Council operates a clear-desk policy throughout the organisation and this is designed to ensure that potentially sensitive documents are not exposed to unauthorised persons. This means that no documents other than those that are required during the course of the working day should be on display. At the end of each working day, desks should be cleared of all documents and papers.

# 6 PERSONNEL SECURITY

The primary objectives of personnel security are to reduce the risks of human error, theft, fraud or misuse of facilities through carrying out checks on potential employees.

## 6.1 Recruitment

As part of the HR process, all potential employees, including consultants, contractors and temporary staff, **must** undergo at least two of the following checks:

- Character references (ideally, at least one personal reference and one reference from a previous employer)
- A check of the completeness and accuracy of the applicant's curriculum vitae
- Confirmation of claimed academic and professional qualifications
- Independent identity checks (passport, utility bill, etc).

For particularly sensitive areas, there **must** also be a Criminal Records Bureau (CRB) check.

Confidentiality or non-disclosure agreements should be used to give notice that Council's information is confidential or secret. Employees should sign such an agreement as part of their initial terms and conditions of employment

### 6.1.1 Consultants, Contractors, Casual & Temporary Staff

Casual staff and consultants, contractors, or other staff from third party organisations, must also be made to sign a non-disclosure agreement and the Information Security Policy prior to being granted access to the Council' information processing facilities or systems.

### 6.1.2 Starters / Leavers Process

The Starters and Leavers Process is an essential part of system administration and general computer account management. It is designed to ensure that all new starters have access to the facilities and systems that they require in order to perform their task. Conversely, it is also used to ensure that any employees that leave the Council have their access levels revoked.

Managers must ensure that the IT Department is informed in at least 5 days in advance of any new starters, or leavers, so that the appropriate levels of system access, including email and internet access, can be established, or revoked, as needed.

### 6.1.3 Movers Process

Similar principles to those employed as part of the starters/leavers process should be employed with regard to individuals whose role within the Council changes to ensure

that levels of access to information systems is modified in line with the requirements of the new role.

### 6.1.4 Security Awareness and Education

All Members and employees and, where relevant, third party users, should receive appropriate training and regular updates relating to policies and procedures, including security requirements, legal responsibilities and business controls, as well as training in the proper use of information processing facilities, **before access to information or services is granted.**

# 7 COMMUNICATIONS & OPERATIONS SECURITY

In general, the Internet is neither more nor less secure than other means of communication, including mail, facsimile, and voice telephone service, all of which can be intercepted or otherwise compromised. As a matter of prudence, however, Council asks employees to assume that all of their communications are inherently insecure and to be aware of this fact during the normal course of their business.

## 7.1 LAN / WAN Network Security

Copeland Borough Council IT Section provides and maintains a secure network. Copeland IT will provide and maintain the necessary software and equipment to keep the network secure from any unauthorised connections or external threats. Copeland IT provides and maintains software and hardware systems to audit and manage the LAN / Wan network security.

## 7.2 Third Party Networks

By default, all third party networks are considered un-trusted and no links to third-party networks must be established without the express approval of the IT Department.

Additionally, on occasions where users are working at locations other than Council premises, laptops must not be connected to any other networks without first consulting the IT Department.

### 7.2.1 Servers

All servers must be built with the most current version of the required operating system and all required services and applications must have all appropriate security patches applied in a timely fashion.

All mission critical systems must undergo a full system security review, conducted by the IT section prior to going live. No systems must be deployed in an operational environment until it has been cleared by the IT Department. Where these are new financial systems, these must also be cleared by internal audit and the S.151 Officer.

### 7.2.2 Workstation & Desktop Security

Council IT personnel will build all workstations in line with the relevant guidelines for the operating system in question. Once deployed, all personnel are expected to ensure the security of their own workstations and should never leave systems logged on while unattended. Acceptable Screensavers must be set up with a password to prevent unauthorised access, when the system is left temporarily. This must be set to activate after a maximum time of 10 minutes. Users should also ensure that the password guidelines outlined in section 8 are followed and that general principles of 'least privilege' are used when using their system i.e. users' access must be restricted just to the functions they need to carry out their duties.

### 7.2.3 Wireless LANs

Wireless technologies are rapidly becoming the de facto choice for extending corporate services externally to employees using hand-held devices and to extending existing hard- wired networks quickly and without the need for cabling.

Unfortunately, most wireless deployments are not adequately secured and expose organisations to a range of unnecessary and unexpected risks that could lead to a significant security breach. The deployment of secure wireless networks requires the use of a range of security technologies to be deployed and wireless networks should not be connected to the Council network without the express approval of the of the IT section.

# 8 SYSTEMS ACCESS CONTROL

All staff must be adequately trained in the use of appropriate business systems before being granted access. Where employees change roles within the organisation, their access requirements should be reviewed and amended accordingly.

All personnel must be issued with a unique User ID and password that allows them to access the network resources. Users must ensure that they keep the passwords secure. Under no circumstances should any Council employee divulge their password to anyone else as processes are in place to resolve issues surrounding lost and/or forgotten passwords.

## 8.1 Passwords

You should not allow other employees access to your password. If you anticipate that someone may need access to your confidential files in your absence *then you should raise a helpdesk request clearly stating who you wish to give access to or arrange for your line manger to raise a helpdesk request.*

Passwords and systems access controls are vital to maintaining the security of data.

### 8.1.1 User IDs and Passwords

Copeland Borough Council requires that each worker accessing multi-user information systems have a unique user ID and a private password. These user IDs must be employed to restrict system privileges based on job duties, project responsibilities, and other business activities Request to change these privileges must be on a helpdesk request raised by an appropriate line manger . Each worker is personally responsible for the usage of his or her user ID and password. Passwords **Must Not** be shared. If a user believes that his or her user ID and password are being used by someone else, the user must immediately change the password and notify the IT section and their Line manager.

All passwords must be at least 5 characters long and must not contain easily guessed words. Passwords must be changed every 40 days.

Copeland IT section will monitor and audit access to systems and will revoke any account deemed not being used correctly as stated in this policy.

### 8.1.2 Password Storage

Passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorised persons might discover them. Passwords must not be written down in some readily-decipherable form and left in a place where unauthorised persons might discover them.

## 8.2 Token Based Authentication

Token-based authentication is an example of *two-factor authentication*. In contrast to password authentication, which relies solely on the use of a single password, two-factor authentication incorporates a personal identification number (PIN) in addition to a hardware or software token device. Because of the additional requirement of token generation, two-factor authentication is more secure than password authentication and is often referred to as *strong authentication*.

Where access is required to critical council infrastructure components, token-based authentication mechanisms should be deployed in order to restrict access to only those individuals that need access.

Additionally, token-based authentication systems should be used in the event that access to the Council network is required by any third-party or Remote Users. The IT Department must be consulted prior to the installation of any such network links and will advise on the appropriate course of action.

# 9 SYSTEMS DEVELOPMENT & MAINTENANCE

## 9.1 Logging Overview

Any attempted access to the network that is denied will be logged by a network security system. Each denied access is considered a security "event," but not necessarily a security 'violation'.

Copeland IT produce logs at predetermined intervals (e.g. weekly or monthly) covering events of the previous period. All collated log data will be reviewed to locate unusual security events. Any anomalous events will be investigated by the IT Department, by Audit, appropriate department or organisation.

A security 'violation' is any event which fails to comply with data security standards, or which represents an apparent or real effort to undermine, overrides, or otherwise circumvent security standards or controls. Depending on the severity of an incident, violations of security policy may result in prosecution of the offending individual.

### 9.1.1 Network Traffic Logs

All network traffic to and from third party networks and the Internet is blocked, unless specifically required and permitted by the firewall rule base. All blocked traffic is logged for both real-time intrusion attempts, and for historical analysis (e.g. in the event of an incident).

### 9.1.2 System Usage Logs

Users should be aware that most of Council systems routinely log user actions in order to facilitate recovery from system malfunctions and for other management purposes. Additionally, Council deploys systems monitoring software that will alert the IT Department of any abuse of the system and network resources provided.

User actions that are logged may include:

- Date and time users login and logout of the system
- Users' menu selections and queries
- Users' changes to data and fields
- Web and email usage

These logs are confidential and kept in secure locations to avoid violating privacy. Only system administrators have direct access to system logs.

## 9.2 Systems Testing and Approval

All business systems must be thoroughly tested prior to deployment in a live, production environment. Additionally, all systems should be reviewed by the IT department and will either receive security sign-off, or a series of recommendations as to how to improve the security of the systems in question.

Once System Administrators have implemented these recommendations, the systems will be reviewed again and the security sign-off process will continue until such time as the IT Department has determined the configuration to meet current security requirements.

# 10 COMPLIANCE

The IT Department Technical support team leader is responsible for ensuring compliance across the enterprise and will periodically review information security practices and procedures.

The IT Department will conduct regular system, application and network security reviews of the core infrastructure. The findings of these reviews will be used to suggest security enhancements to existing configurations and, where appropriate, amendments will be made to the relevant policy or standards document.

**Non-compliance will be reported to the relevant Head of Service, the S.151 Officer and the Audit Services Manager.**

## 10.1 Regulatory obligations

Council Information Policy is subject to the following legislative requirements:

- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Computer Misuse Act 1990
- Data Protection Act 1998
- Copyright, Designs & Patents Act 1988
- European Human Rights Act 1998
- Freedom of Information Act 2000

# 11 Appendices

## 11.1 User Acceptance

Insert the declaration that they have read and understood this policy.

## 11.2 The Confidentiality Statement

New employees, agency staff and contractors required to sign and adhere to the Confidentially Statement.