EXEC 280709
ITEM 7

EXECUTIVE MEMBER:	Cllr Elaine Woodburn, Leader
LEAD OFFICER:	Julie Crellin, Head of Finance and Management Information Systems
REPORT OFFICER:	Martin Stroud, ICT Manager
DATE OF REPORT:	06 July 2009

GCSX AMENDED INFORMATION SECURITY POLICY & ACCEPTABLE USE POLICY

Summary and Recommendation:

The report seeks to advise the Council on the draft updated Information Security and Acceptable Use policies required to support the GCSx Code of Connection.

Executive is recommended to agree the updated Information Security Policy and GCSx Acceptable Usage Policy and Personal Commitment Statement and recommend these policies to Council for adoption to ensure they in place before 30th September 2009.

1. INTRODUCTION

1.1 Executive agreed a report at the May meeting which detailed the progress and the steps to be taken to achieve COCO compliance, to enable connection to the GCSX Network by the deadline of 30th September 2009.

1.2 The purpose of this report is to advise Members of the amendments to the Council's existing Security Policy and separate Acceptable Use Policy to ensure compliance with COCO security requirements. These policies will need to be in place and the GCSX Acceptable Use Policy and Personal Commitment Statement will need to be wet signed by current council employees, elected Members, contractors, and 3rd parties by 30th September 2009 and be maintained in the future.

1.3 The Council is required by Central Government to comply with COCO to have access to the GCSx Network, allowing DWP and Customer services to securely share information used in the processing of benefits, this is essential to allow the authority to carry on processing benefits and share information with the DWP.

2. RECOMMENDATION

2.1 Executive is recommended to agree the updated Information Security Policy and the GCSX Acceptable Usage Policy and Personal Commitment Statement and recommend these policies to Council for adoption, preferably at its next meeting (4th August) or the following meeting (8th September).

3. DETAIL

3.1 The current IT security and acceptable use policies are outdated and do not clearly define acceptable use or provide guidance on all aspects of information security.

3.2 Copeland's ICT team have developed, working in conjunction with Sefton Metropolitan Borough Council and other lead authorities, a policy framework to address the gaps in our policies and has liaised with in particular HR and the Head of Legal Services to develop a revised Information Security Policy and Acceptable Use Policy to meet COCO requirements. These are set out in Appendix A 'Information Security Policy' and Appendix B 'GCSX Acceptable Usage Policy and Personal Commitment Statement'.

3.3 The aims of the updated security and acceptable use policies are to :-

- More clearly define the requirements for information security.
- More clearly define the acceptable use of the internet, email, and communication systems.
- Minimise and interruption caused by security incidents.
- All legislative and regulatory requirements are met.
- Meet the requirements for COCO & GCSX acceptable use.
- Ensure the council's information technology is used responsibly, securely and with integrity at all times.

3.4 These documents are lengthy, but there are essential to ensuring the protection of information and the users of our information systems, in their broadest sense. COCO is not solely concerned with ICT technical issues. ICT solutions can be used to make the policing and implementation of ICT security easier, but there are implications for how we do business to ensure the protection of data and information. The policy requires for example, more stringent security checks in relation to staff employed by the organisation, an enhancement to asset management security, (clean desk policy etc) and ICT business continuity arrangements will be refreshed to reflect the updated policy as it now defines those security requirements and more clearly defines what is acceptable use of ICT services and systems.

3.5 The main changes to the current information security and acceptable use policy are summarised below :-

- Provides guidance and information for the Data Protection and the Freedom of Information Act (chapter 2 Compliance)
- Defines the policy on data protection, identifies information types and principles to protect such data.
- More clearly defines the acceptable use policy and supporting policy framework. (Chapters 4/5).
- More clearly defines access control and user access management and responsibilities for access control (Chapter 6 access control).
- Provides further guidance on password policy (Chapter 7).
- New section added for physical security (chapter 8).
- New section added Communications and operations management aimed at ICT staff (Chapter 9).
- New section added providing guidance for information security incident management (chapter 10).
- New section added providing guidance for business continuity (chapter 11).
- New section added to provide guidance for asset management (chapter 12).
- New section added to provide guidance on the procurement and maintenance of information systems, software and hardware (chapter 13).
- Appendix A added to provide clear guidance for the acceptable and safe use of mobile devices (Appendix A).
- Appendix B added to provide clear guidance for the acceptable and secure transfer of data (Appendix B).

3.6 Upon adoption all staff, elected Members, partners and remote support providers will be required to wet sign the GCSX Acceptable Usage Policy and Personal Commitment Statement. ICT will work with HR to ensure that the existing users sign the policy. ICT will record and are required to audit compliance and evidence this compliance to external inspectors. It is the intention (subject to the date of Council approval) for the deadline for the first round of completion of signatures to be 31st August, in readiness for the 30th September deadline.

3.7 COCO requires the designation of an officer within the Authority to be the Information Security Officer and this has been assigned to the ICT Manager and the postholder will provide ongoing guidance and support for both ICT and all Copeland staff, working closely with HR and Legal Services to ensure support for both departments (Data protection/Staff security).

3.8 Successful adoption of the updated security and acceptable use policy will provide all staff with clearer guidance for all aspects of information security and be a further step to achieving COCO compliance and strengthen the authority's Information Security, provide the tools to ensure compliance with

the Data Protection Act and prove to our citizens we act responsibly in respect of the information and data we hold about them.

4.0 Financial and Human Resources Implications (Including Sources of Finance):

4.1 Officer time has been expended in updating and modernising the current IT security and acceptable use policies. The estimated direct costs of adopting the updated information security and acceptable use policy are associated with staff time and printing costs associated with printing and distributing updated policies. Wherever possible, ICT will deliver the Information Security and Acceptable Use Policy electronically.

4.3 There will be the need, however, to identify staffing resources from other departments to work with ICT to deliver the updated information Security & Acceptable Use Policies -

- HR – to help ICT identify all user required to sign acceptance.
- Legal & Democratic Services (support for FOI and DPA sections)

4.4 These updated policies require clear communication and understanding by the Council and in particular, ICT users. Training in the form of briefing sessions will be provided during the August and September by ICT. The training materials have been drawn from recommended training materials from the Cabinet Office. ICT will produce an accompanying ‘rough guide’ to information security to help all users understand the need for stronger information security and what their role is. It will also be available on the intranet. Executive will receive a presentation at the meeting setting out the key implications of the Security Policy for users in relation to their day-day experience.

5. IMPACT ON CORPORATE PLAN AND BUSINESS RISKS:

5.1 Failure to adopt the updated Security and acceptable use policy will mean that we fail a number of the requirements for COCO and would result in failure to succeed in gaining permission to connect to the GCSx network. This would have a major detrimental effect upon the Customer Services department who require access to DWP information. It would also represent a failure to operate to industry standards and increases the risks of data loss and impairment of data security.

5.2 Gaining permission to connect to the GCSx connection will enhance the aims for T-enabling and provide smarter more secure way of working for all departments. Therefore, the Impact on the Corporate Plan is high.

5.3 The Corporate Plan 2009/10 has a specific target related to COCO compliance. i.e. Information Security Project (1.3), part of Transformational Leadership.

Appendices

Appendix A – (Updated) Information Security Policy
Appendix B – GSCx Acceptable Usage Policy and Personal Commitment Statement

List of Background Documents:

COCO supporting documents and references.

- NISCC Technical Note 10/04 Revised 23 February 2005 (Understanding Firewalls)
- GCSX Operational Support Guide Version 1.0
- GCSX Pre Connection Take on Guide Version 1.7
- National Security Agency (NSA) Recommended 802.11 Wireless Local Area Network Architecture
- National Security Agency (NSA) Systems and Network Attack Centre (SNAC) Security Guidance for Deploying IP Telephone Systems
- National Institute of Standards and Technology (NIST) Security Considerations for Voice over IP.
- Cabinet Office HMG Baseline Personnel Security Standard Version 1 July 2006
- CESG INFOSEC Memorandum No35 Remote Access to Public Sector IT Systems
- CESG Security Procedures For Blackberry Enterprise Solution Administrators
- CESG Security Procedures for Blackberry Enterprise Solution users
- Sefton MBC Security Policy for GSX Connected Authorities
- Copeland Borough Council Draft Information Security Policy Version 1.0 November 2008 (Draft ICTSECPOL1.1)
- Manual for Protective Security
- Report to CMT – COCO Compliance (Jan 2009)
- HMG Security Policy Framework
- HMG 1A Standard No.6 – Protecting Personal Data and Managing Information Risk

List of Consultees to Document: CMT

Check list For Dealing With Key Issues:

Please confirm against the issue if the key issues below have been addressed. This can be by either a short narrative or quoting the paragraph number in the report in which it has been covered.

Impact on Crime and Disorder	Improves data security of the organisation
Impact on Sustainability	None
Impact on Rural Proofing	None

Health and Safety Implications	Improved rigour in relation to building security and HR policies requiring documented checks on employee status should positively contribute to H&S.
Impact on Equality and Diversity Issues	None
Children and Young Persons Implications	None
Human Rights Act Implications	No infringement would result from implementation the updated Security and Acceptable use policy.
Monitoring Officer comments	Has been kept involved during the process.
S. 151 Officer comments	Nothing further to add

Copeland Borough Council

Information Security & Acceptable Use Policy

Chapter 1

Introduction

Author: Martin Stroud Finance and MIS
Version: 1.0

Document Control Information	
Document ID	ICTSPOL1.1
Document title	Information Security Policy - Introduction
Version	1.0
Status	Draft
Author	Martin Stroud
Job title	ICT Manager
Department	Finance and MIS
Publication date	7 July 2009
Approved by	
Next review date	
Distribution	All

Contents

1. Introduction

The increasing use of Information and Communication Technology and the development of information strategies to support the process of providing effective services make it necessary to take appropriate action to ensure that these systems are developed, operated and maintained in a safe and secure manner.

Whilst the aim is to provide facilities for employees to use freely in pursuit of their job there are, however, management and legal issues, which should be borne in mind to ensure the effective and appropriate use of information technology.

Information Security is an asset that, like other important business assets, has value to an organisation and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

1.1. Importance of Security

Copeland Borough Council has a significant investment in computer systems and networks. **In** common with other organisations, to a large and continually increasing extent the Council is dependent upon the data, which is stored and processed, on its computers and the management information that is generated from the data.

The loss of data and computer processing facilities or breaches of data access security could incur significant costs, loss of revenue and damage to the Councils reputation as a result of:

- Business activities being fully or partially suspended.
- Having to restore the data, computer programmes and/or equipment.
- Unauthorised disclosure of confidential information relating to individuals and/or other confidential business information being made available to 'interested parties'.
- Fraudulent manipulation of cash or goods.

The preservation of the confidentiality, integrity and availability of information held not only electronically within systems but also on paper, microfiche, floppy discs or CDROM is therefore essential to the Council.

1.2. Objectives

The objectives of this Corporate Information Security Policy are to protect the Council's information through clear direction and guidance to ensure that:

- The public and all users of the Council's systems are confident of the accuracy and integrity of the information used and produced.
- Business damage and interruption caused by security incidents are minimised.
- Confidentiality of personal and other sensitive information is assured.
- All legislative and regulatory requirements are met.
- The Council's Information Technology is used responsibly, securely and with integrity at all times.

1.3. Scope

All users granted access to the Councils information, computer facilities and their associated information networks.

1.4. Principles

The principles of Information Security applied by Copeland Borough Council are based on ISO27001 and include:

- Asset management.

- Risk assessment and business impact analysis.
- Human resources security.
- Physical and environmental security.
- Communications and operations management.
- Access control.
- Information systems acquisition, development and maintenance.
- Information security incident management.
- Business continuity management.
- Compliance.

1.5. Compliance

Some aspects of the Council's security will be governed by statutory legislation including:

- The Freedom of Information Act 2002.
- The Human Rights Act 2000.
- The Electronic Communications Act 2000.
- Regulation of Investigatory Powers Act 2000.
- The Data Protection Act 1998.
- The Copyright Designs and Patents Act 1998.
- The Computer Misuse Act 1990.

Data protection and privacy must be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. Key records must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

1.6. Implementation

The ICT Team has been appointed to create the policy and monitor Information Security.

The ICT Manager is responsible for ensuring that the networks and communications, the operating systems and support software and computer centers are secure and meet Policy requirements.

Internal Audit will evaluate security controls while undertaking audit reviews in addition to undertaking specific Information Security audits on a regular basis.

All breaches of Information Security, actual or suspected will be reported and investigated by Information Services and Audit.

1.7. Individual Responsibilities

All Elected members must accept responsibility for maintaining Information Security standards within the organisation.

All managers must accept responsibility for initiating, implementing and maintaining security standards within the organisation.

All non-managerial employees must accept responsibility for maintaining standards by conforming to those controls, which are applicable to them.

ICT will be responsible for implementation of the controls marked for IT specialists.

Local managers must undertake yearly assessments of security risks within their own areas to ensure that the cost of implementation of controls is proportionate to both the value of the information and the business harm likely to result from any security breach whilst complying with ISO27001.

1.8. Supporting Documentation

This Policy must be read in conjunction with any specific instructions issued for each

information facility, and the following supporting documentation.

- Copeland Borough Council Freedom of Information Policy and Guidelines
- Copeland Borough Council Information Management Policy
- Copeland Borough Council Retention and Disposal Guidelines
- Copeland Borough Council Codes of Practice
- Copeland Borough Council Information Management Policy

Copeland Borough Council

Information Security & Acceptable Use Policy

Chapter 2

Compliance

Contents

1. Compliance

1.1. Legislation

All relevant statutory, regulatory and contractual requirements and the organisation's approach to meeting these requirements must be explicitly defined, documented, and kept up to date for each information system. The key laws associated with Information and their uses are included in the following table:

Law	Main issues covered.
The Freedom of Information Act 2002.	Public access to Council information.
The Human Rights Act 2000.	Right to privacy and confidentiality.
The Electronic Communications Act 2000.	Cryptography, electronic signatures.
The Regulation of Investigatory Powers Act 2000.	Hidden surveillance of staff.
The Data Protection Act 1998.	Protection and use of personal information.
The Copyright Designs and Patents Act 1998.	Software piracy, music downloads theft of Council data.
The Computer Misuse Act 1990.	Hacking and unauthorized access.
The Environmental Information Regulations 2004.	Public access to Council information related to the environment.
The Re-use of Public Sector Information Regulations 2005.	The Council's ability to sell certain of its data for commercial gain.

1.1.1. Data Protection

The Data Protection Act controls the processing of personal data about living people. Processing covers any use of the data including its storage and retrieval. In order to process data legally the processing must be in accordance with the eight data protection principles:

- Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
- Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
- Shall be accurate and where necessary, kept up to date;
- Shall not be kept for longer than is necessary for that purpose or those purposes;
- Shall be processed in accordance with the rights of data subjects under the Act;
- Shall be kept secure i.e. protected by an appropriate degree of security;
- Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Copeland Council's Data Protection policy is reproduced in full in Chapter 3.

1.1.2. Freedom of Information Act

The Freedom of Information Act came into force in January 2005. By granting a general right of access to records held by public Authorities it encourages an attitude of openness and will enable the public to scrutinise their decisions and working practises. The key features of the Act are:

- Every Council employee has a duty to provide advice and assistance to requesters requesting information.
- The public has a general right of access to all recorded information held by the Council and some Independent Contractors ('the Council'). Subject to exemptions set out in the Act a requester has the right to know whether a record exists, and the right to a copy of that record supplied in a format of their choice.
- Every Council must adopt and maintain a Publication Scheme, listing what kinds of records it chooses to publish, how to obtain them, and whether there is a charge involved.
- The Information Commissioner's Office will oversee the implementation and compliance with this Act and the Data Protection Act 1998.

Further information can be obtained from the Copeland Council Policy and Guidelines on Freedom of Information available on the Intranet.

1.2. Software Licensing

The Council uses software in all aspects of its business to support the work carried out by its employees. In all instances every piece of software is required to have a licence and the Council will not condone the use of any software that does not have a licence.

Computer software must be purchased through CPU and installed by a member of Information Services or appropriate arrangements can be made for a relevant member of the department to install the software.

Shareware, Freeware and Public Domain Software are bound be the same policies and procedures as all other software. No user may install any free or evaluation software onto the Council's systems without prior approval from ICT.

Employees must not make copies of computer software owned by the Council for private use. Misuse of the Council's software in this manner will result in disciplinary action.

Managers must ensure that all policies and procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

Copeland Borough Council

Information Security & Acceptable Use Policy

Chapter 3

Data Protection Policy

Contents

Data Protection Policy

1.1. Introduction and Scope

Copeland Council collects and uses personal data about people with whom it deals in order to operate. This data covers current, past and prospective employees, suppliers, clients/customers, including school pupils and students, and others with whom it communicates. In addition, it may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of government departments. Any personal information must be dealt with properly however it is collected, recorded and used, whether on paper, in a computer, or recorded in other media, and there are safeguards to ensure this in the Data Protection Act 1998.

This policy relates to all personal data held by Copeland Council, in any form for which Copeland Council is the Data Controller. It applies to all employees of the Authority and any other person or external data processor that has access to Copeland Council personal information.

1.2. Policy statement

Copeland Council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998. The council will therefore aim to ensure that all employees, elected members, contractors, agents, consultants, partners, external agencies or other servants of the council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under the Act.

1.3. What is personal data?

Personal data is defined as, data relating to a living individual who can be identified from that data, or from that data combined with other information that is in the possession of, or is likely to come into the possession of the data controller.

Personal data includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

1.4. What are the principles of data protection?

The Data Protection Act 1998 stipulates that anyone processing personal data must comply with **Eight Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;

7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and sensitive personal data. Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

The data subject also has rights under the act. These consist:

- The right to be informed that processing is being undertaken;
- The right of access to one's personal information within the statutory 40 days;
- The right to prevent processing in certain circumstances;

The right to correct, rectify, block or erase information regarded as wrong information.

1.5. How will Copeland Council ensure compliance?

In order to ensure it meets its obligations under the Data Protection Act, Copeland Council will ensure that:

- There is an individual with specific responsibility for data protection in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;

Copeland Council will, through appropriate management and the use of strict criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;

- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of Data Subjects can be fully exercised under the Act.

1.6. What roles and responsibilities have been assigned?

Proper definitions of roles and responsibilities are essential to assure compliance with this Policy. In summary these are:

1.6.1. Data Protection Officer and the Legal Department

The Data Protection Officer and the Legal department will promote this policy and provide detailed advice training and resources to departments to facilitate the correct processing of Requests for Access and other Data Protection related issues. They will also monitor departments to ensure compliance with statutory and regulatory obligations.

1.6.2. Senior Management

Senior management will provide support and approval for this Data Protection Policy and any related initiatives across the Authority. It will also ensure that adequate funding is made available.

1.6.3. Departmental Managers

Departmental managers are responsible for ensuring that Sefton Data Protection Policy is communicated and implemented within their area of responsibility, and for ensuring that any issues such as resourcing or funding are communicated back to their strategic directors in a timely manner.

1.6.4. Individual employees

Individual employees will be responsible for understanding this Policy and ensuring that Requests for Access and other Data Protection related issues in their own department are handled in compliance with this policy.

1.6.5. Departmental information management specialists

Departmental information management specialists will provide first line advice to departments on Requests for Access and other Data Protection related issues.

1.7. Policy Compliance

If you are found to have breached this policy, you may be subject to the Council's disciplinary procedure. If you have broken the law, you may be subject to prosecution.

If you do not understand the implications of this policy or how it may apply to you, seek advice from Information Services via the Helpdesk.

Appendix 1 - Related resources and links

Internal guidance on implementation of the Act, and key DPA related documents are available to staff via the Copeland Council Intranet at:

http://cbc-stag/CopelandIntranet/default.aspx?page=3

Copeland Councils record retention guidelines:

http://ntintranet/main.asp?page=1628

General guidance and a free helpdesk dealing with DPA related issues are available to staff and the public via the Internet on the Information Commissioners website at:

http://www.ico.gov.uk/

The Data Protection Act can be accessed on the Internet via the UK Statute Law Database at:

http://www.statutelaw.gov.uk/Home.aspx

Copeland Borough Council

Information Security & Acceptable Use Policy

Chapter 4

Internet Acceptable Use Policy

Contents

1. Internet Acceptable Use Policy

1.1. What Information is contained in this Document?

This policy document tells you how you should use your Council Internet facility, which you have accessed on any Council owned equipment. It outlines your personal responsibilities and tells you what you must and must not do.

This policy updates the Council's Internet and Email Acceptable Use Policy (April 2008) and replaces all locally agreed Internet usage policies.

1.2. What approach has the Council taken to Internet usage?

The Council recognises that it is not practical to define precise rules that cover the full range of Internet activities available and in general, it is adherence to the spirit and essence of the policy that will allow the Council as a whole, and employees in person, to productively benefit from access to this powerful technology.

1.3. Who audits compliance with this policy?

Policy compliance is audited by the Council's ICT Section.

1.4. What are the related Copeland Borough Council codes, policies and guidance?

- Internet Guidance
- Email Policy
- Data Protection Policy
- Freedom of Information Act Guidance
- Employee Code of Conduct
- Members Code of Conduct
- Working from Home Policy

1.5. To whom does the policy apply?

The Copeland Borough Council Internet Policy applies to all users of the Councils Internet service and computer equipment.

1.6. When does the policy apply?

At all times.

1.7. What is the purpose of providing the Internet service?

The Internet service is primarily provided to give Council employees and Elected Members:

- Access to information that is pertinent to fulfilling the Council's business obligations.
- The capability to post updates to Council owned and/or maintained Web sites.
- An electronic commerce facility.

1.8. What you should use your Council Internet account for

Your Council Internet account should be used in accordance with this policy to access anything in pursuance of your work including:

- Access to and/or provision of information.
- Research.
- Electronic commerce (e.g. purchasing equipment for the Council)

1.9. Personal use of the Council's Internet service

At the discretion of your line manager, and provided it does not interfere with your work, the Council permits personal use of the Internet in your own time (for example during your lunch-break).

The Council is not however responsible for any personal transactions you enter into, for example in respect of the quality, delivery or loss of items ordered. You must accept responsibility for, and keep the Council protected against, any claims, damages, losses or the like which might arise from your transaction for example in relation to payment for the items or any personal injury or damage to property they might cause.

If you purchase personal goods or services via the Council's Internet service you are responsible for ensuring that the information you provide shows that the transaction is being entered into by you personally and not on behalf of the Council.

You should ensure that personal goods and services purchased are not delivered to Council property, rather, they should be delivered to your home or other personal address.

If you are in any doubt about how you may make personal use of the system you are advised not to do so.

All personal usage must be in accordance with this policy. Your computer and any data held on it are the property of Copeland Borough Council and may be accessed at any time by the Council to ensure compliance with all its statutory, regulatory and internal policy requirements.

1.10. Internet account management, security and monitoring

The Council will provide a secure logon-id and password facility for your Network account. The Council's ICT Department is responsible for the technical management of this account.

You are responsible for the security provided by your Network account logon-id and password. Only you should know your log-on password and you should be the only person who uses your Internet account.

The provision of Internet access is owned by the Council and all access is recorded, logged and interrogated for the purposes of:

- Information Services monitoring total usage to ensure business use is not impacted by lack of capacity.
- The filtering system monitors and records all access for reports that are produced for line managers and auditors.

1.11. Things you must not do

Access to the following categories of websites is currently blocked using a URL filtering system:

- Illegal
- Pornographic
- Violence
- Hate and discrimination
- Offensive
- Weapons
- Hacking
- Web chat
- Gambling
- Dating
- Radio Stations
- Games
- Web Mail

Except where it is strictly and necessarily required for your work, for example IT audit activity or other investigation, you must **not** use your Internet account to:

- X Create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
  "Unsuitable" material would include data or images the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of this and other Council policies.
- X Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- X Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs.
- X Subscribe to, enter or use online gaming or betting sites.
- X Subscribe to or enter "money making" sites or enter or use "money making" programs.
- X Run a private business.

The above list gives examples of "*unsuitable*" usage but is neither exclusive nor exhaustive.

1.12. Our responsibilities

It is your responsibility to:

- ✓ Familiarise yourself with the detail, essence and spirit of this policy before using the Internet facility provided for your work.
- ✓ Assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.
- ✓ Know that you may only use the Council's Internet facility within the terms described herein.
- ✓ Read and abide by the related policies as described in paragraph 4 above.

1.13. Line Managers/Team Leaders responsibilities

It is the responsibility of Line Managers/Team Leaders to ensure that the use of the Internet facility is:

- ✓ Within an employees work time is relevant to and appropriate to the Council's business and within the context of the users responsibilities.
- ✓ Within employees own time and is subject to the rules contained within this document.

1.14. Whom should I ask if I have any questions?

In the first instance you should refer questions about this policy to your Line Manager who will refer you to HR, ICT or Audit as appropriate. Members should refer questions to the Members ICT Support Officer.

You should refer technical queries about the Council's Internet service to the ICT Helpdesk on extension 8323 or email at Icthelpdesk@copeland.gov.uk.

1.15. What will happen if I don't abide by this policy?

If you are found to have breached this policy, you will be subject to the Council's disciplinary procedure. If you have broken the law, you may be subject to prosecution.

Copeland Borough Council

Information Security & Acceptable Use Policy

Chapter 5

Email Acceptable Use Policy

Contents

1. Email Acceptable Use Policy

1.1. What information is contained within this document?

This policy document tells you how you should make use of the email facility that the Council has provided for your work. It outlines your personal responsibilities and tells you what you must not do.

This policy updates the Council's Internet and Email Acceptable Use Policy (April 2008) and replaces all locally agreed email usage policies.

1.2. Who audits compliance with this policy?

Policy compliance is audited by the Council's ICT section.

1.3. Related Copeland Council codes, policies and guidance

The Copeland Council:

- Internet Policy
- Data Protection Policy
- Guidance on the use of electronic communications systems
- Freedom of Information Act Guidance
- Internet Guidance Manual
- Employee Code of Conduct
- Member's Code of Conduct

1.4. To whom does the policy apply?

The Copeland Council Email Policy applies to all users of the Council's email system.

1.5. When does the Council's email policy apply?

At all times.

1.6. What is the purpose of providing the email system?

The email system is provided to allow electronic communication in pursuance of Council business between Elected Members, Council employees, individual Council service users and external organisations.

1.7. Email content ownership

The Council owns the email facility that you use. The emails that you produce, send and receive are the property of the Council.

1.8. Freedom of Information Act and your email

Be aware that Copeland Council may be required to disclose your emails or responses to them under the Freedom of Information Act.

1.9. Email account management, security and monitoring

The Council will provide a secure environment to host your email facility. This security framework includes a Network logon-id and password facility. The Council's ICT Department is responsible for the technical management of your account.

You are responsible for the security provided by your logon-id and password.

Only you should know your log-on id and password. You should not disclose your log-on id and password to anyone.

You may only use the email accounts that you are authorised to access.

Be aware that the Council will regularly monitor your email account usage and email content.

Emails sent from your account are deemed to have been sent by you.

1.10. What you should use the email system for

You should use the email system for sending business related

communications and associated attachments.

1.11. Personal use of the Council's email system

Provided it does not interfere with your work, the Council also permits ***"occasional and short"*** use of the email system for personal communications.

"Occasional and short" means infrequently and for seconds, rather than minutes. You are not allowed to use the system for personal "conversational" email (see paragraph 12 below).

In disciplinary situations, the Council will be the arbiter of whether or not the "***occasional and short***" test has been met.

Any Personal or Private e-mails sent must be marked as such in the Subject Field.

If you are in any doubt about how you may make personal use of the system you are advised not to do so.

1.12. Things you must not do

You must not use the Council's email system to facilitate or operate any business/ commercial activity, other than that of the Council.

When using the email system for Council business and for occasional personal use, you are responsible for ensuring that the material accessed or transmitted is not "***Unsuitable***".

"***Unsuitable***" material includes data or images the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of this and other Council policies, or which may bring the Council into disrepute.

Except where it is strictly and necessarily required for your work (for example, corporate advertising, IT audit activity or other investigation), you must not create, download, access, display, transmit or engage in the following:

- full videos or clips
- photographic or cartoon images
- chain letters
- jokes or 'joke' chains
- conversational email
- harassing or bullying content

- entertainment software
- other non-work related software
- advertisements
- global emails (see paragraph 13 below)
- game
- gambling

Again, except where it is strictly and necessarily required for your (work as defined above), you must not create, download, access, display, transmit or engage in the following:

- material that is obscene, offensive, sexually explicit, pornographic, racist, sexist, ageist, defamatory, hateful, or homophobic in nature, incites or depicts violence, or describes techniques for criminal or terrorist acts

- derogatory remarks or express derogatory opinions regarding the Council, its Officers or Members or communicate extreme views that could be to the detriment of the Council or its reputation or bring the Council into disrepute

- play games with opponents over the email system

The above list gives examples of "***Unsuitable***" material but is neither exclusive nor exhaustive.

1.13. Global email

The Council does not permit the transmitting of Everyone email's other than for Council business purposes.

Business related Global email transmission is authorised by, and sent from, the ICT Helpdesk.

If you believe that you need to communicate to all email system users in this manner, contact the ICT Helpdesk on ext. 8323 who will help and advise.

1.14. What should I do if I if I receive an "unsuitable" email?

If you receive an unsolicited "unsuitable" email you can inform the Council's ICT Helpdesk on ext. 8323 you may be requested to forward an example and then delete the email.

If you are subject to substantial, unsolicited "unsuitable" emails, you can raise the issue with your line manager or the ICT Helpdesk.

1.15. The legal implications of email content

You need to be aware that your communication (sent or received) may be used to demonstrate a course of action has been committed to, such as an agreement to enter into a contract. Email content can also be used as evidence.

1.16. Your responsibilities

It is your responsibility to:

- **Familiarise** yourself with the detail, essence and spirit of this policy before using the email facility provided for your work.

- **Assess any risks** associated with each message you send and ensure that e-mail is the appropriate mechanism to use.

- **Know** that you may only use the Council email system within the terms described herein.

- **Read** and abide by the related policies as described in paragraph 3 above.

1.17. Whom should I ask if I have any questions?

In the first instance, you should refer questions about this policy to your Line Manager who will refer you HR or ICT as appropriate. Members should refer questions to the Members ICT Support Officer.

You should refer technical queries about the Council's email system to the ICT Helpdesk on extension 8323.

1.18. What will happen if I don't abide by the email policy?

If you are found to have breached the Council's email policy, you may be subject to the Council's disciplinary procedure. If you have broken the law, you may be subject to prosecution

Copeland Borough Council

Information Security & Acceptable Use Policy

Chapter 6

Access Control Policy

1. Access Control

1.3. Overview

Access to Copeland Council's ICT systems must be protected. Whilst different business applications have varying security requirements, these individual requirements must be identified through risk assessments that will 'control the access' to the ICT systems.

1.4. Scope of this Policy

This policy applies to everyone with any form of access to a Copeland Council computer device or ICT system. This policy applies at all times and should be read in conjunction with the Password Policy.

1.5. User Access Management

Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

User's access rights must be reviewed at regular intervals by the authorising person to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

1.5.1. User Registration

A request for access to the Council's computer systems must first be submitted to the ICT Helpdesk or to the business systems authoriser (for a particular application) for approval. Applications for access must only be submitted if approval has been gained from your line manager or Team Leader.

When an employee leaves the Council, their access to computer systems and data must be suspended on the employee's last working day at the close of business. It is the responsibility of the business authoriser to request the suspension of the access rights via the ICT Helpdesk.

1.5.2. User Responsibilities

It is a user's responsibility to prevent unauthorised access to Council systems by:

- Following the Password Policy
- Ensuring that unattended PC's are locked or logged out
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing ICT Helpdesk and the business authoriser of any changes to their current role.

1.6. Network Access Control

The normal operation of the network must not be interfered with. Specific approval must be obtained from ICT for the use of a modem on any networked PC. The use of modems on PC's connected to the Council's network can seriously compromise the security of the whole Council network.

1.6.1. User Authentication for External Connections

Where remote access to the Copeland network is required, an application must be made via the ICT Helpdesk. Remote access to the network must be secured by two factor authentication consisting of a username and one other component, for example a securid token.

1.6.2. Supplier's Remote Access to the Council Network

Partner agencies or 3rd party suppliers must not be given details of how to access the Council's network without permission from ICT. Any changes to supplier's connections must be immediately sent to the ICT Helpdesk so that access can be updated or ceased. All permissions and access methods must be controlled by ICT.

Partners or 3rd party suppliers must contact a member of ICT before connecting to the Copeland network and a log of activity must be maintained. Remote access software must be disabled when not in use.

1.7. Operating System Access Control

Access to Operating Systems is controlled by a secure login process. The access control defined in the User Access Management Section and the Password Policy must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g. username
- Limiting the number of unsuccessful attempts and locking the account if exceeded
- The password characters being hidden by symbols
- Displaying a general notice warning that only authorised users are allowed

All access to Operating Systems is via a unique login id that will be audited from time to time (and can be traced to the responsible individual). The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that can be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

1.8. Application and Information Access

Access within Software Applications must be restricted using the security features built into the individual product. The authoriser or 'business owner' of the software application is responsible for access to the information within the system. The access must be:

- Compliant with the User Access Management Section and the Password Policy
- Separated into clearly defined roles
- Appropriate to the level of access required for the role of the user
- Unable to be overridden (with the admin settings removed or hidden from the users)

- Free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access
- Logged and auditable.

1.9. Policy Compliance

If you are found to have breached this policy, you may be subject to the Council's disciplinary procedure. If you have broken the law, you may be subject to prosecution.

If you do not understand the implications of this policy or how it may apply to you, seek advice from ICT via the Helpdesk.

Copeland Borough Council

Information Security & Acceptable Use Policy

Chapter 7

Password Policy

Contents

1. Password Policy

1.1. Overview

Protecting the Councils computers, systems and data from unauthorised users is of paramount importance and passwords play an important role in this process. The Council data they protect may be personal, valuable or confidential, and unauthorised access may lead to accidental disclosure, legal liability for the Council or for the User, fraud, financial loss and deterioration of Service.

1.2. Policy Statement

The purpose of this policy is to mandate a standard for the creation of strong

passwords, their protection and frequency of change.

All Copeland Council employees, contractors and system suppliers with access to Copeland Council computers and systems are responsible for taking the necessary steps, as defined below, to ensure that their passwords are chosen well, kept secure and used correctly.

1.3. Scope of This Policy

This policy applies to anyone with an account (or any form of access that requires a password) on a Copeland Council computer device or system. This includes system support staff and the use of privileged administrative passwords.

1.4. Choosing Passwords

Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

Everyone must choose strong passwords with a minimum standard of:

- Have at least seven characters.
- Include one or more numerical digit(s).
- Contain at least one upper case character.
- Are more complex than a single word (such passwords are easier for hackers to crack).

The Government advises using Environ passwords with the following format: consonant, vowel, consonant, consonant, vowel, consonant, number, number (for example pinray45).

1.5. Protecting Passwords

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different Copeland Council systems.
- Do not use the same password for systems inside and outside of work.

1.6. Changing Passwords

All user-level passwords must be changed at a maximum of every 40 days or immediately if the password has been compromised. Users cannot reuse the same password within 20 password changes.

1.7. System Administration Standards

The password administration process for individual Copeland Council systems must be well-documented and only available to designated people.

All Copeland Council IT systems should be configured to enforce the following (exceptions must be documented and agreed with ICT and or Audit):

- Authentication of individual users, not groups of users *i.e. no generic accounts.*
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging - at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.

1.8. Policy Enforcement

Failure to maintain secure passwords in accordance with this policy may result in disciplinary action being taken against you.

In the case of third party suppliers or consultants, non-conformance will result in the immediate removal of access to the system. If damage or compromise of Copeland ICT systems results, Copeland Council will consider legal action against the third party.

1.9. Advice and Policy Interpretation

If you are uncertain about any aspect of this policy please contact the ICT Helpdesk on 8323.

This policy will be reviewed regularly by the ICT Manager. You will be alerted to important changes and updates will be published on the Copeland Intranet site. Always refer to the Copeland Intranet for the latest version of this policy.

Copeland Borough Council

Information Security & Acceptable Use Policy

Chapter 8

Physical Security Policy

Contents

1. Physical and Environmental Security

1.10. Overview

In order to comply with elements of law (Data Protection, Computer Misuse acts etc.), Central Government and industry best practice, (Information Management etc) and, newly mandated security frameworks such as those attending credit and debit card transactions and access to the Government Connect secure network, access to Copeland Council's equipment and information must be protected.

The aim of this policy is to prevent unauthorised access to both physical and electronic information. In summary, the policy requires the following to be protected:

- Sensitive paper records
- IT equipment used to access electronic data
- IT equipment used to access the Council network

This protection may be as simple as a lock on a filing cabinet or as complex as the security systems in place to protect the Council's IT data. The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorised access. Each Department is responsible for assessing the level of protection required for their teams and locations.

1.11. Policy Statement

The purpose of this policy is to establish standards in regard to the physical and environmental security of the Council's information. All Copeland Council employees, contractors and users with access to Copeland Council's equipment and information (electronic and paper records) are responsible for ensuring the safety and security of the Council's equipment and the information that they use or manipulate.

1.12. Scope of the Policy

This policy applies to all users of the Council's owned leased / hired facilities and equipment. The policy defines what paper and electronic information belonging to the Council should be protected and, offers guidance on how such protection can be achieved. This policy also describes employee roles and the contribution staff make to the safe and secure use of Council information.

1.13. Secure Areas

Critical or sensitive information must be stored in secure areas protected by appropriate security controls. A risk assessment should identify the **appropriate** level of protection to be implemented to secure the information being stored. Examples of secure areas for protection are:

- A room with sensitive paper based information,
- A machine room containing IT fileservers.

Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. The building must have **appropriate** control

mechanisms in place for the type of information and equipment that is stored there, these could include:

- Alarms fitted and activated outside working hours
- Window and door locks
- Access control mechanisms fitted to all accessible doors (where codes are utilised they should be regularly changed and known only to those people authorised to access the area / building)
- CCTV cameras
- Staffed reception area
- Protection against damage e.g. fire, flood, vandalism

As an example, access to secure areas such as the data centre and IT equipment rooms, must be adequately controlled and physical access to buildings should be restricted to authorised persons. Staff working in secure areas should be ready to challenge anyone not known to them and/or not wearing a badge. Each department must ensure that doors and windows are properly secured.

Badges, keys, (should be signed for/regularly audited) entry codes etc. must only be held by officers authorised to access those areas and should not be loaned / provided to anyone else.

Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge. An ICT Team Member must monitor all visitors accessing secure IT areas at all times.

In all cases where security processes are in place, instructions must be issued to address the event of a security breach. Where breaches do occur or, a member of staff leaves outside normal termination circumstances keys, badges etc. should be recovered from the staff member and any door / access codes should be changed immediately.

1.14. Paper Based Data Security

Paper based (or similar non-electronic) information must be assigned an owner and a classification If it is classified as personal or confidential, information security controls to protect it must be put in place. A risk assessment should identify the appropriate level of protection for the information being stored. Paper in an open office must be protected by the controls for the building in Section 1.4 and other appropriate measures that could include:

- Filing cabinets that are locked with the keys stored away from the cabinet
- Locked safes
- Stored in a Secure Area protected by access controls

1.15. Equipment Security

All general computer equipment must be located in suitable physical locations that:

- Reduce risks from environmental hazards, for example, heat, fire, smoke, water, dust and vibration.
- Reduce the risk of theft, for example, **if necessary** items such as laptops should be physically attached to the desk
- Facilitate workstations handling sensitive data being positioned so as to eliminate the risk of the data being seen by unauthorised people.

Desktop PCs must **not** have data stored on the local hard drive; data must be stored on the network file servers. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained. ICT can advise on the use of network drives and file storage/security.

All servers located outside of the data centre must be sited in a physically secure environment. Business critical systems should be protected by an Un-interrupted Power Supply (UPS) to reduce the operating system and data corruption risk from power failures. The equipment must not be moved or modified by anyone without authorisation from ICT.

All items of equipment must be recorded on an inventory, both a Departmental and the ICT inventory. Procedures should be in place to ensure inventories are updated as soon as assets are received or disposed of.

All equipment must be security marked and have a unique asset number allocated to it. This asset number should be recorded in the Departmental and the ICT inventories.

1.15.1. Cabling security

Cables that carry data or support key information services must be protected from interception or damage. Power cables should be separated from network cables to prevent interference. Network cables should be protected by conduit and where possible avoid routes through public areas.

1.15.2. Equipment Maintenance

ICT and 3rd party suppliers must ensure that all of Copeland's ICT equipment is maintained in accordance with the manufacturer's instructions and with any documented internal procedures to ensure it remains in working order. Staff involved with maintenance must:

- Retain all copies of manufacturer's instructions
- Identify recommended service intervals and specifications
- Enable a call-out process in event of failure
- Ensure only authorised technicians complete any work on the equipment
- Record details of all remedial work carried out
- Identify any insurance requirements
- Record details of faults incurred and actions required

A service history record of equipment should be maintained so that when equipment becomes older decisions can be made regarding the appropriate time for it to be replaced.

Equipment maintenance must be in accordance with the manufacturer's instructions. This must be documented and available for support staff to use when arranging repairs, for example HP servers are under a support and maintenance agreement.

1.15.3. Security of Equipment off Premises

The use of equipment off-site must be formally approved by your line manager. Equipment taken away from Copeland premises is the responsibility of the user and must:

- Be logged in and out
- Not be left unattended
- Concealed whilst transporting
- Not left open to theft or damage whether in the office, during transit or at home
- Where possible, be disguised (e.g. laptops should be carried in less formal bags)
- Be encrypted if carrying personal or confidential information
- Be password protected
- Be adequately insured

Further information can be found in the Mobile Devices Acceptable Usage Policy on the Intranet.

Users should ensure, where necessary and required that insurance cover is extended to cover equipment which is used off site. Users should also ensure that they are aware of and follow the requirements of the insurance policy. Any losses / damage must be reported to the IS Department and the Insurance Section (if applicable), losses or damage to equipment must be recorded in the departmental and IS inventories.

Staff should be aware of their responsibilities in regard to Data Protection and be conversant with the Data Protection Act. (See DPA on Intranet).

1.15.4. Secure Disposal or Re-use of Equipment

Equipment that is to be reused or disposed of must have all of its data and software removed/destroyed. If the equipment is to be passed onto another organisation (e.g. returned under a leasing agreement) the data removal must be achieved by using professional data removing software tools.

Software media must be destroyed to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

All equipment being disposed of must be prepared for release within the mandated criteria of Copeland Council's recycling policies (see Disposal of Redundant Computer Equipment)

1.15.5. Delivery and Receipt of Equipment into the Council

In order to confirm accuracy and condition of deliveries and to prevent subsequent loss or theft of stored equipment, the following must be applied:

- Equipment deliveries must be signed for by an authorised individual using an auditable formal process. This process should confirm that the delivered items correspond fully to the list on the delivery note.
- Loading areas and holding facilities should be adequately secured against unauthorised access and all access should be auditable.
- Subsequent removal of equipment should be via a formal, auditable process.

Deleted: Page Break

1.16. Policy Compliance

If you are found to have breached this policy, you may be subject to the Council's disciplinary procedure. If you have broken the law, you may be subject to prosecution.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the ICT Department via the ICT Helpdesk on 8323

Copeland Borough Council

Information Security & Acceptable Use Policy

Chapter 9

Communications and Operations Management Policy

CONTENTS

1. Communications and Operations Management Policy

1.17. Overview

This policy covers the key areas in day to day operations management of the Council's IT services. The policy covers topics that include: protection of the service against malware e.g. viruses and Trojans, unauthorised changes and information leakage.

This policy applies in the majority to ICT staff with the exception of sections 1.6.2. and 1.8. that have elements that apply to all employees across the Council.

1.18. Policy Statement

All Copeland Council employees, contractors and users with access to Copeland Council's equipment and information (in any format including electronic and paper records) are responsible for ensuring the safety and security of the Council's systems and the information that they use or manipulate.

1.19. Scope of this Policy

This policy applies to all users of the Council's facilities and equipment including staff and any third party suppliers and contractors. All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

1.20. Operational Procedures and Responsibilities

1.20.1. Documented Operating Procedures

Operating procedures must be documented to an appropriate level of details for the departmental team that will be using them. The procedures must include procedures and work instructions for the following areas:

- Processing and handling of information (information classification, confidentiality requirements)
- Backup procedures (see Section 1.8)
- Work scheduling requirements (considering interdependencies, completion times etc)
- Instructions and guidance for handling errors
- Contact and reporting details in the event of unexpected operational issues
- Procedures for handling special outputs (e.g. special stationery like cheques, payslips)
- System restart and recovery procedures in the event of system failure
- Procedures for all housekeeping functions

1.20.2. Change Management

Changes to the Council's operational systems must be controlled with a formally documented change control procedure. The change control procedure should include references to:

- A description of the change and business reasons
- Information concerning the testing phase

- Impact assessment including security, operational etc
- Formal approval process
- Communication to all relevant people of the changes
- Procedures for aborting and rolling back if problems occur

All significant changes to the main infrastructure (e.g. Network, Directories) need to be assessed for their impact on information security as part of the standard risk assessment.

1.20.3. Separation of Development, Test and Operational Facilities

The development and test environments must be separate from the live operational environment to reduce the risk of accidental changes or unauthorised access. The environments must be segregated by the most appropriate controls including:

- Running on separate computers
- Running on different domains
- Different usernames and passwords

1.21. System Planning and Acceptance

1.21.1. Capacity Management

ICT must monitor the capacity demands of the Council's systems and make projections of future capacity requirements so that adequate power and data storage requirements can be fulfilled.

Utilisation of key system resources must be monitored so that additional capacity can be brought on line when required. These include:

- File servers
- Domain servers
- E-mail servers
- Web servers
- Printers

Increases in business activities and staffing levels must also be monitored to allow for the extra facilities that will be required for example numbers of workstations.

1.21.2. System Acceptance

All departments must inform ICT via the Helpdesk of any new product requirements or of any upgrades, service packs, patches or fixes required to existing systems (ICT will also monitor these areas).

New information systems, product upgrades, patches and fixes all must undergo an appropriate level of testing prior to acceptance and release into the live environment. The acceptance criteria must be clearly identified, agreed and documented and should involve management authorisation.

3rd party applications must be monitored for service packs and patches. These should be tested and applied as soon as possible after release once confirmed to not negatively impact the application.

Major system upgrades must be thoroughly tested in parallel with the existing system in a safe test environment that duplicates the operational system.

1.22. Protection against Malicious and Mobile Code

The Council's information and the integrity of its software applications must be protected from malicious software (malware). Appropriate controls and user awareness procedures must be put in place to ensure this protection.

1.22.1. Patching

All vendor supplied service packs, patches and fixes must be applied as soon as they become available and have passed the system acceptance testing.

All other servers must have critical security patches applied as soon as they become available and have passed the system acceptance testing. All other patches must be applied as appropriate. There must be a full record of which patches have been applied and when.

1.22.2. Controls against Malicious Code

Anti malware software must be installed and maintained on all workstations and servers and provided on appropriate points on the network. The software must be from an established vendor with consistent results in recognising and removing malware. All updates must be installed as soon as they are available.

A regular review of all business critical systems must be conducted to identify all software running on the systems. Any unauthorised files or software must be formally investigated and if appropriate deleted.

To protect systems from malware users must not:

- Install software from any external source including the internet, CD / DVD-ROMs, USB memory sticks, floppy disks etc on their workstation.
- Add their own screensavers, desktop images, photos or utilities to the workstation.

All workstation software must be approved and installed by ICT. Software must also be controlled to ensure compliance with licensing requirements (see Chapter 2 - Compliance).

Malware can be introduced through hoax emails and users must be vigilant to guard against this. Users must not forward emails that claim to be warnings these are often chain emails (see Chapter 5 - Email Policy). Users must report the email to the ICT Helpdesk on ext. 8323

All email attachments should be checked for malware at the point of entry onto the network.

1.22.3. Controls against Mobile Code

Mobile code represents newer technologies often found in web pages including:

- ActiveX
- Java
- JavaScript
- VBScript
- MSWord Macros

Mobile code must be prevented from entering the network with the exception of for web sites that have been approved for use after a risk assessment. Controls must also be put in place on the workstation to prevent this code from running by default.

1.23. Back Up

1.23.1. Information Back Up

Regular backups of essential business information must be taken to ensure that the Council can recover from a disaster, media failure or error. An appropriate backup cycle must be used and fully documented.

To ensure all essential business information is backed up all employees must store their information on the network drives and not on local drives e.g. C: drive. All users of portable devices for example laptops, PDA's, smart phones and USB memory sticks must ensure the information is also stored on the network drives. For details of network drives see http://intranet.Copeland.gov.uk/dc.

Any 3rd parties that store Council information must also be required to ensure that the information is backed up.

Full backup documentation including a complete record of what has been backed up along with the recovery procedure must be stored at an off site location in addition to the copy at the main site. This must also be accompanied by an appropriate set of media tapes and stored in a secure area. The remote location must be sufficiently remote to avoid being affected by any disaster that takes place at the main site.

Critical paper files must be identified and backed up with either a scanned digital copy or complete photocopies stored at a remote location.

1.23.2. Information Restore

Full documentation of the recovery procedure must be created and stored. Regular restores of information from back up media must be tested to ensure the reliability of the back up media and restore process.

The retention period for business information (in particular legal requirements) must be defined and applied to the backup data. Long term backup and restore solutions may need to be identified for certain business information.

1.24. Media Handling

1.24.1. Management of Removable Media

Removable computer media e.g. tapes, disks, cassettes and printed reports must be protected to prevent damage, theft or unauthorised access.

Documented procedures must be kept for backup tapes that are removed on a regular rotation from Council buildings. Media stores must be kept in a secure environment e.g. a fireproof safe. Appropriate arrangements must be put in place to ensure future availability of data that is required beyond the lifetime of the backup media.

1.24.2. Physical Media in Transit

Media being transported must be protected from unauthorised access, misuse or corruption. Where couriers are required a list of reliable and trusted couriers should be established. If appropriate physical controls should also be used e.g. encryption or special locked containers. (see Appendix B – Secure Transfer of Information).

1.24.3. Disposal of Media

Media that is no longer required must be disposed of safely and securely to avoid data leakage. Media containing personal or sensitive information must be disposed of through the confidential waste bins provided. Items that should be considered for secure disposal include:

- Paper documents
- Voice or other recordings
- Magnetic tapes
- Removable disks
- USB Memory sticks
- CD/DVD ROMs

Any previous contents of any reusable media that are to be removed from the Council must be erased. This must be a thorough removal of all data from the media to avoid the potential of data leakage.

Please see the disposal guidelines for further information or contact the ICT Helpdesk on ext 8323 for advice on disposal of these types of items.

1.24.4. Security of System Documentation

System documentation must be protected from unauthorised access. This includes bespoke documentation that has been created by ICT staff (not general manuals that have been supplied with software). Examples of the documentation to be protected include descriptions of:

- Applications
- Processes
- Procedures
- Data structures
- Authorisation details

1.25. Exchange of Information

1.25.1. Information Exchange Policies and Procedures

Procedures and protocols must be in place that protects the exchange of information through any format e.g. email, letter and fax (Also see Appendix A - Mobile Devices Acceptable Use Policy and Appendix B - Secure Transfer of Information Policy).

The procedures must be designed to protect exchanged information from:

- Interception
- Copying
- Modification
- Mis-routing
- Destruction

Information must be protected with appropriate controls based on the information's classification e.g. Confidential. (see Asset Management Policy – Chapter 12).

1.25.2. Exchange Agreements

Formal agreements for the exchange of information between the Council and external organisations must be in place. The agreement must detail the classification of the information being exchanged and the controls to be applied to protect it.

1.26. Monitoring

1.26.1. Audit Logging

Audit logs must be kept for a minimum of six months which record exceptions and other security related events. As a minimum audit logs must contain the following information:

- System identity
- User ID
- Successful/Unsuccessful login
- Successful/Unsuccessful logoff
- Unauthorised application access
- Changes to system configurations
- Use of privileged accounts (e.g. account management, policy changes, device configuration)

Access to the logs must be protected from unauthorised access that could result in recorded information being altered or deleted. System administrators must be prevented from erasing or deactivating logs of their own activity.

1.26.2. Administrator and Operator Logs

Operational staff and system administrators must maintain a log of their activities. The logs should include:

- Back-up timings and details of exchange of backup tapes
- System event start and finish times and who was involved
- System errors (what, date, time) and corrective action taken

The logs should be checked regularly to ensure that the correct procedures are being followed.

1.26.3. Clock Synchronisation

All computer clocks must be synchronised to ensure the accuracy of all the systems audit logs as they may be needed for incident investigation.

1.27. Network Security Management

1.27.1. Network Controls

Network management is critical to the provision of Council services and must apply the following controls:

- Operational responsibility for networks should, where possible be separate from computer operations activities
- There must be clear responsibilities and procedures for the management of remote equipment and users
- Where appropriate, controls must be put in place to protect data passing over the network e.g. encryption

The network architecture must be documented and stored with configuration settings of all the hardware and software components that make up the network.

1.27.2. Wireless Networks

Wireless networks must apply controls to protect data passing over the network and prevent unauthorised access. Encryption must be used on the network to prevent information being intercepted.

1.28. Policy Compliance

If you are found to have breached this policy, you may be subject to the Council's disciplinary procedure. If you have broken the law, you may be subject to prosecution.

If you do not understand the implications of this policy or how it may apply to you, seek advice from ICT via the Helpdesk.

Copeland Borough Council

Information Security & Acceptable Use Policy

Chapter 10

Information Security Incident Management Policy

1. Information Security Incident Management Policy

1.29. Overview

The aim of this policy is to ensure that Copeland Council's information systems and data are protected from any actual or suspected security incidents. The definition of an incident is an adverse event that has caused or has the potential to cause damage to an organisations assets, reputation and/or personnel. Incident management in IT is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

This policy applies in the majority to ICT Support staff with the exception of sections 1.4.1. and 1.4.2. that applies to all employees across the Council.

Reported events and weaknesses need to be assessed by an ICT security advisor (selected from experience within ICT Team for the particular incident). The advisor enables the ICT department to identify when a series of events or weaknesses have escalated to become an incident. It is vital for the ICT department to gain as much information as possible from the business users to identify if an incident is occurring.

1.30. Policy Statement

All Copeland Council employees, contractors and users with access to Copeland Council's equipment and information (in any format including electronic and paper records) are responsible for ensuring the safety and security of the Council's systems and the information that they use or manipulate.

1.31. Scope of this Policy

This policy applies to all users of the Council's facilities and equipment including staff and any third party suppliers and contractors. All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

1.32. Reporting Information Security Events and Weaknesses

1.32.1. Reporting Information Security Events for all Employees

Security events for example a virus infection could quickly spread and cause data loss across the organisation. All users must be able to identify that any unexpected or unusual behaviour on the workstation could potentially be a software malfunction. If an event is detected users must:

- Note the symptoms and any error messages on screen
- Disconnect the workstation from the network if an infection is suspected (with assistance from ICT Support Staff)
- Not use any removable media (for example USB memory sticks) that may also have been infected

All security events should be reported immediately to the ICT Helpdesk on ext 8323.

If the Information Security event is in relation to paper or hard copy of information for example personal information files are stolen from a filing cabinet this must be reported to Head of Service and the Audit Section.

1.32.2. Reporting Information Security Weaknesses for all Employees

Security weaknesses for example a software malfunction must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be considered to be misuse.

Weaknesses reported to application and service providers by employees must also be reported internally to ICT. The service provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded by ICT.

1.32.3. Reporting Information Security Events for IT Support Staff

Information security events and weaknesses must be reported to the ICT Helpdesk on ext 8323 as quickly as possible and the incident response and escalation procedure must be followed.

Security events can include:

- Uncontrolled system changes
- Access violations
- Breaches of physical security
- Non compliance with policies
- Systems being hacked or manipulated

Security weaknesses can include:

- Inadequate firewall or antivirus protection
- System malfunctions or overloads
- Malfunctions of software applications
- Human errors

The reporting procedure must be quick and have redundancy built in. All events must be reported to at least two nominated people within ICT who must both be required to take appropriate action. The reporting procedure must set out the steps that are to be taken and the time frames that must be met.

An escalation procedure must be incorporated into the response process so that users and support staff are aware who else to report the event to if there is not an appropriate response within a defined period.

1.33. Management of Information Security Incidents and Improvements

A consistent approach to dealing with all security events must be maintained across the Council. The events must be analysed and the security advisor must be consulted to establish when security events become escalated to an incident. The incident response procedure must be a seamless continuation of the event reporting process and must include contingency plans to advise the Council on continuing operation during the incident.

1.33.1. Collection of Evidence

If an incident may require information to be collected for an investigation strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care. Internal Audit must be contacted immediately for guidance and strict processes must be followed for the collection of forensic evidence. If in doubt about a situation for example concerning computer misuse contact the ICT Helpdesk on 8323 for advice.

1.33.2. Responsibilities and Procedures

Management responsibilities and appropriate procedures must be established to ensure an effective response against security events. The security advisor from ICT must decide when events are classified as an incident and the most appropriate response.

An incident management process must be created and include details of:

- Identification of the incident, analysis to ascertain its cause and vulnerabilities it exploited
- Limiting or restricting further impact of the incident
- Tactics for containing the incident
- Corrective action to repair and prevent reoccurrence
- Communication across the Council to those affected

The process must also include a section referring to the collection of any evidence that might be required for analysis as forensic evidence. The specialist procedure for preserving evidence must be carefully followed.

The actions required to recover from the security incident must be under formal control. Only identified and authorised staff should have access to the affected systems during the incident and all of the remedial actions should be documented in as much detail as possible.

1.33.3. Learning from Information Security Incidents

To learn from incidents and improve the response process incidents must be recorded and a Post Incident Review conducted. The following details must be retained:

- Types of incidents
- Volumes of incidents and malfunctions
- Costs incurred during the incidents

The information must be collated and reviewed on a regular basis by ICT and any patterns or trends identified. Any changes to the process made as a result of the Post Incident review must be formally noted.

1.34. Policy Compliance

If you are found to have breached this policy, you may be subject to the Council's disciplinary procedure. If you have broken the law, you may be subject to prosecution.

If you do not understand the implications of this policy or how it may apply to you, seek advice from ICT via the Helpdesk.

Copeland Borough Council

Information Security Policy

Chapter 11

Business Continuity

Contents

Business Continuity

Overview

Business Continuity Planning (BCP) is a corporate process designed to protect critical business processes and services from the effects of major system failures or disasters and to ensure their timely and prioritised resumption following any business continuity incident. BCP is a part of corporate risk management. As our organisation is highly dependent on computers, networks and communications systems, a large area of BCP is concerned with the effects of major failure of information systems. This policy covers that area.

The Council accepts that there are risks associated with heavy reliance on information systems, and that major incidents will happen. It therefore requires that each department:

- Identify and assess potential risks that loss of information system(s) may have on their service
- Develop plans to minimise the impact a loss of information system(s) would have on their service
- Ensure the information system(s) that support their service can be restored in an acceptable timeframe.
- Identify any critical business processes and services without which there would be a serious risk to the health and well-being of citizens

These plans can then be used by supporting services (ICT, Personnel, Technical Services etc.) to focus and prioritise their recovery efforts.

Policy Statement

This policy defines the baseline requirements for the Council and its departments to develop plans to counteract interruptions to business activities, to protect critical business processes from the effects of major information system(s) failures or disasters and to ensure their timely and prioritised resumption following any business continuity incident. This policy covers not only the computer systems but also the people and processes that use them to provide services.

Scope of the Policy

This policy applies to all departments and staff of Copeland Council. The contents of this policy must be communicated to any Third Parties, Partners or External Service Providers responsible for the provision or support of any information system (e.g. hardware, software, network/telephony, personnel, technical facilities etc), service or business process.

Requirements

Business Continuity Management Process

A managed process must be developed by the Council and maintained to ensure adequate business continuity throughout the organisation in the event of major failures of information systems. This process must address all information security requirements. At minimum:

- Responsibility for corporate BCP must be assigned and documented.

- Any BCP related to Information Systems must align with all existing Corporate Risk Management functions, (e.g. the Contingency and Emergency Planning functions and Financial Risk Management).

- The Council must ensure that adequate financial, technical, organisational and environmental resources are available to address the identified requirements.

- The range of information systems-related risks faced by the organisation, in terms of threats, vulnerabilities, likelihood of occurrence and the potential impact of failure on departments, must be fully understood by each department of the Council. This assessment must cover not only the computer systems but also the risks related to people, processes that use them to provide service.

- All critical departmental processes, and the information assets they rely upon, must be identified. (This may be done using an extension of the Asset Management process defined in Chapter 12.)

- Each department must understand and document the range of impacts that identified risks may have on their service

- The process must ensure the safety of staff and the protection of key information systems and organisational assets.

- The process must consider insurance where appropriate and ensure premiums are kept up to date.

Business continuity and risk assessment

The Council's strategy and plans for maintaining business continuity must be developed on the basis of appropriate risk (probability and impact) assessment. Events that can cause interruptions to business processes must be identified, along with the probability and impact of such interruptions and their consequences for information security.

The risk assessment must identify, quantify and prioritise risks against organisational and departmental objectives.

All identified risks must be analysed. Steps must be taken to eliminate or mitigate any threats and vulnerabilities where appropriate thus reducing the risk of occurrence. Residual risks must then be addressed by the BCP framework.

Developing and implementing continuity plans

Corporate and Departmental plans must be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required timescales following interruption to or failure of critical business processes.

Business continuity planning framework

A single corporate framework business continuity plan must be developed and maintained to ensure all plans are coherent, consistently address information security requirements, and identify priorities for testing, maintenance and reassessment of departmental and corporate plans.

BCP for Information Systems must align with all existing Corporate Risk Management, (e.g. Corporate BCP, Contingency and Emergency Planning and Financial Risk management.

Documentation

At minimum, BCP plans must document the following in such a way that the documentation remains available in the event of failure of critical information and communications systems. Basic requirements are that:

- Key responsibilities are documented and accepted by the owner.
- Key contacts, both external and internal, required to support restoration of service to normal are documented.
- Escalation procedures must be clear and documented, showing how to assess the situation and whether to initiate a major incident response.
- Mobilisation and briefing procedures for internal staff are documented.
- Mobilisation and briefing procedures for third party suppliers are documented.
- Emergency procedures are documented.
- Fallback procedures for alternate facilities are documented.
- Temporary Operational procedures are documented.
- Resumption Procedures are documented.
- Critical assets (including key skills) are documented.
- All third party support contracts and details of their invocation processes are documented.

Training

All staff involved in the recovery have been adequately trained in the recovery process and any technical skills required.

Testing, maintaining and reassessing business continuity plans

Business continuity plans must be tested at least annually and updated annually; following a test; following a major change to information systems, staffing, organisational structure or business environment to ensure that they remain effective and that they comply with all requirements for information security.

At a minimum change management processes across the Council must ensure that the needs of the BCP framework are addressed. Every change to hardware, software, people, processes, organisational structure, buildings or business environment must be assessed for its impact on any business continuity plans currently in place. Likely changes include:

- Addresses.
- Telephone numbers.
- Personnel.
- Locations.
- Facilities.
- Resources.
- Legislation.
- Contractors.
- Suppliers.
- Key customers.
- Business processes.
- Risk appetite and overall business strategy.

To avoid a large overhead generated by the above, BCP documentation must be designed to avoid unnecessary detail.

A walkthrough of each BCP plan must be carried out at least annually using 'real-life' scenarios.

Technical Disaster Recovery processes must work in the required timescale, and must not be impacted by practical problems, out-of-hours restrictions and availability of staff and third party services.

Third party supplier services upon which Business Continuity depend must be tested at least annually to ensure that they will meet their contractual obligations.

Rehearsals of dealing with major incidents must be held annually.

Policy Compliance

If you are found to have breached this policy, you may be subject to the Council's disciplinary procedure. If you have broken the law, you may be subject to prosecution.

If you do not understand the implications of this policy or how it may apply to you, seek advice from ICT via the Helpdesk.

Copeland Borough Council

Information Security & Acceptable Use Policy

Chapter 12

Asset Management

Contents

Asset Management

Overview

For information systems to be used effectively, efficiently and legally the assets that make up those systems must be properly controlled. This is referred to as asset management.

Asset management is not limited to covering the stocks of information (electronic data or paper records) that the Council maintains. It also addresses the people that use them, the processes they follow and the physical computer equipment used to access them. Any asset management policy should address all these areas as they can all limit the confidentiality, quality and availability of information.

The following Policy details the basic requirements and responsibilities for the proper management of information assets at Copeland Council.

Policy Statement

The purpose of this policy is to achieve and maintain appropriate protection of organisational assets. It does this by ensuring that every information asset has an owner and that the nature and value of each asset is fully understood. It also ensures that the boundaries of acceptable use are clearly defined for anyone that has access to the information.

Scope of the Policy

This policy applies to all the systems, people and business processes that make up the Council's information systems.

Asset Management Requirements

Definition of important information assets

The process of identifying important information assets should be sensible and pragmatic. The Council has vast uncontrolled stocks of information. Items of information that have no security classification (See section 2.5) and are of limited practical value do not need a formal owner or inventory.

Important information assets will include:

- filing cabinets and stores containing paper records
- computer databases
- data files and folders
- software licenses
- physical assets (computer equipment and accessories, PDAs, cell phones)
- key services
- key people
- intangible assets such as reputation and brand

Inventory of Information Assets

The organisation must draw up and maintain inventories of all important information assets that it relies upon. These should identify each asset and all associated data required for risk assessment, information/records management and

disaster recovery. At minimum it must include the type, location, designated owner, security classification (See section 2.5), format, backup and licensing information.

Assigning Asset Owners

All important information assets must have a nominated owner and should be accounted for. An owner must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner's responsibility for the asset and the requirement for them to maintain it should be formalised and agreed.

Unclassified and trivial information assets

Items of information that have no security classification (See section 2.5) and are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it and temporary owners should be assigned within each department too ensure that this is done. Details of how to approach this task are available in the FOI resources page of the intranet.

Information assets with short term or localised use

For new documents that have a specific, short term, localised use, the creator of the document will be the originator. This includes letters, spreadsheets and reports created by staff. All staff must be informed of their responsibility for the documents they create. Specific requirements are highlighted in the Records Management Policy available on the intranet.

Corporate information assets

For information assets whose use throughout the Council is widespread and whose origination is as a result of a group or strategic decision, a corporate owner must be designated and the responsibility clearly documented. This should be the person who uses it the most, or has the most control over it.

Acceptable use of information assets

The Council must document, implement and circulate Acceptable Use Policies (AUP) for information assets, systems and services. These should apply to employees, contractors and third parties and use of the system must be conditional on acceptance of the appropriate AUP. This requirement must be formally agreed and auditable.

At minimum this will include e-mail and internet usage, mobile devices (telephones, PDAs and laptops) and usage of information beyond the Council's fixed perimeter (home working, VPN access, Portals).

Information classification (PERSONAL, CONFIDENTIAL, UNCLASSIFIED)

On creation, all information assets must be assessed and classified by the owner according to their content. At minimum all information assets must be classified and labelled if they are personal or confidential. The classification will determine how the document should be protected and who should be allowed access to it. Any system subsequently allowing access to this information should clearly indicate the classification.

Classification alone is only a pointer. There are different degrees of personal and confidential and access and appropriate protection and use of information will be determined by risk assessment by the owner.

Personal Information

Personal information is any information about living, identifiable individual. The Council is legally responsible for it. Its storage, protection and use are governed by the Data Protection Act 1998. Details of specific requirements are in Chapter 3 - Data Protection Policy.

Confidential Information

Confidential information is any information for which the Council has a legal duty to protect. This is normally as a result of a contractual agreement, copyright and intellectual property issues. Definition of confidential should be as defined in the Freedom of Information Act 2000. For advice and assistance see below.

Unclassified information

Anything that is not either personal or confidential should be considered public. The Freedom of Information Act 2000 gives the public a right of access to all information held by a public body unless there is a valid exemption in the Act that allows them to withhold it. The two main exemptions used are confidentiality and personal information*. An 'internal' classification is therefore meaningless.

* There are other exemptions. For advice and assistance on classification see the FOI resources page on the intranet or contact the Information Owner or the Data Protection Officer (Martin Jepson)

Sharing classified information with other organisations

There is at present no simple common data classification scheme that is practically applied across the public sector. To avoid confusion where classified Council information is to be shared with or transferred to different organisations it is essential that both parties must understand any classification system in place at the other end. Non-disclosure agreements must be in place where appropriate (See 2.7 below).

Any sharing or transfer of Council information with other organisations must comply with all Legal, Regulatory and Council Policy requirements. In particular this must be compliant with the Data Protection Act 2000, The Human Rights Act 2000 and the Common Law of Confidentiality.

A detailed summary of how to transfer Council Information securely can be found in the Secure Transfer of Information Policy available on the intranet. For advice and assistance on whether to share Council Information see the FOI resources page on the intranet or contact the Information Owner or the Data Protection Officer (Martin Jepson).

Non-disclosure Agreements and Information Sharing Protocols

Where the Council needs to share classified information with a third party organisation an appropriate risk assessment must be carried out and the results of this must be reflected in a non-disclosure agreement that the third party is required to sign. This must be drafted by a legal specialist and should contain details of

controls required to ensure that the organisation is able to respect the classification of the information being shared.

Where regular sharing of classified information between the Council and other organisations is required then an Information Sharing Protocol must be agreed between the organisations. For advice and assistance on Information Sharing protocols, contact the Information Owner or the Data Protection Officer (Martin Jepson).

Information labelling, handling and disposal

The Council must implement a set of procedures for appropriate information labelling and handling that reflects the information classification scheme above. It must cover all formats of information, both physical and electronic. The labelling must inform the user of the contents without revealing unnecessary details or attracting attention. These procedures must cover the processes for acquisition, copying, chain of custody, logging security events, storage, transmission, transfer and ultimate destruction of information.

Detailed requirements for secure handling and disposal of classified information are contained in the Records Management Policy available on the intranet. Detailed requirements for the transfer of confidential and personal information are contained in the Secure Transfer of Information Policy and the Records Management Policy.

Legal disclaimers

Faxes and e-mails are widely used to transfer information. Both can be unreliable and subject to user error so there is a high risk of deliberate or accidental delivery to the wrong address. Policies must be established on the use of such mechanisms, and all such messages should carry a standard disclaimer clearly printed on the fax cover sheet and it should be a procedural requirement that all faxes include a standard cover sheet. The disclaimer must cover:

- A statement that the information is classified and for the addressee only.
- Request that the recipient to notify the sender immediately if they are not the correct recipient.
- A statement to cover liability for errors or omissions in transmission.
- A statement that any opinions are those of the author and do not reflect in any way those of the organisation.

Any disclaimer used must be approved by the Legal department to ensure compliance with current legislation.

Deleted: Page Break

Policy Compliance

If you are found to have breached this policy, you may be subject to the Council's disciplinary procedure. If you have broken the law, you may be subject to prosecution.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the ICT Department via the ICT Helpdesk on 8323.

Copeland Borough Council

Information Security & Acceptable Use Policy

Chapter 13

Information Systems Acquisition Development and Maintenance Policy

CONTENTS

1. Information Systems Acquisition Development and Maintenance Policy

1.35. Overview

Copeland Council holds large amounts of personal and confidential information. It has a variety of statutory, regulatory and internal obligations to process this information in a way that assures its confidentiality, quality and availability at all times. Security can be compromised by vulnerabilities or inadequacies in the design and maintenance of these systems. 'Systems' in this policy include infrastructure, commercial off the shelf packages, external systems, operating systems, business applications and user developed systems, in any format, e.g. paper or electronic.

Basic security requirements should be identified, justified and built into information systems from its conception and design, through creation and maintenance. This can be achieved by sound risk assessment and mitigation at every stage.

This policy applies in the main to ICT Support staff with the exception of section 1.4 which applies to all employees across the Council.

1.36. Policy Statement

Copeland Council must ensure that information security is considered throughout the lifecycle of any system that holds and processes Copeland Council information assets, from conception and design, through creation and maintenance, to ultimate disposal. This policy outlines the basic requirements and responsibilities to achieve this.

1.37. Scope of this Policy

This policy applies to any information system that contains Council information, in any format, e.g. paper or electronic, and to anyone involved in its creation, maintenance and ultimate disposal. Compliance is mandatory for Copeland employees.

For any third-parties involved in this process these basic requirements must be included in any contract or service level agreement. Responsibility for ensuring this lies with the Copeland Council employee that oversees the contract for the Council.

1.38. Security Requirements of Information Systems

Business requirements documentation for new systems or enhancements to existing systems must contain the requirements for security controls. Security vulnerabilities must be recognised from the outset through undertaking a risk assessment and the security requirements must be developed alongside the functional requirements.

Any department with requirements for IT systems must discuss them with ICT Services at the project initiation stage.

1.39. Correct Processing in Applications

Appropriate controls and audit trails must be designed into applications to prevent errors, loss and unauthorised modification or misuse of information in application systems.

Data input to application systems must be validated to ensure the data is correct. Controls must apply to data types such as names, addresses and reference numbers. Controls must be appropriate and at a minimum be based on a risk assessment. Checks could include:

- Out of range values
- Invalid characters
- Missing or incomplete data
- Exceeding upper or lower limits on data volumes
- Unauthorised or inconsistent use of control data

Simple procedures must be in place for responding to errors detected from the above controls.

Process validation checks must be incorporated into systems in order to detect any corruption of the data processed. Security controls should include checks for:

- Session or batch controls
- Balancing controls
- Validation of system generated data
- Integrity and authentication checks on downloaded or uploaded data
- Hash totals of records and files
- Checks that programs are run at the correct times in the correct order
- Logging of activities

1.40. Security in Development and Support Processes

1.40.1. Security of System Files

Controls must be applied to the implementation of software applications in the operational environment. Large scale application rollouts must only be conducted after a period of extensive testing against predetermined criteria.

Third Party supplied software applications must be maintained at the level supported by the software vendor. Upgrades, patches and hot fixes must be applied as they become available. 3rd party suppliers that are involved in remotely administered work must follow the access control policy (see Chapter 6).

3rd party application software must be appropriately checked by an ICT after purchase to ensure that the software is free from malware and from Trojan code or covert channels that could result in information leakage.

1.40.2. Protection of System Test Data

Any Council data that is used during the development and test phase of preparing application software must be protected and controlled. If personal information is used it must be in line with the Data Protection Act (see Chapter 3) and where possible depersonalised. If operational data is used controls must be used including:

- An authorisation process
- Removal of all operational data from the test system after use
- Full audit trail of related activities
- Any personal or confidential information must be protected as if it were live data

1.40.3. Change Control Procedures

The implementation of changes to application software must use a formal change control procedure. The change control procedure must:

- Have a centralised scheme that all proposed changes must be submitted to
- Have an audit trail of requests indicating what decisions were made for each and why
- Ensure existing controls and procedures will not be compromised by the change
- Ensure formal approval of the change from a change control board
- Ensure system documentation and user procedures are updated once the change is implemented

Further details of change control procedures are in Chapter 9 section 1.4.2.

1.41. Policy Compliance

If you are found to have breached this policy, you may be subject to the Council's disciplinary procedure. If you have broken the law, you may be subject to prosecution.

If you do not understand the implications of this policy or how it may apply to you, seek advice from ICT via the Helpdesk.

Appendix A

Mobile Devices Acceptable Use Policy

This policy document also provides guidance on the use of Council supplied mobile devices.

Contents

1. What information is contained within this document?

This policy document tells you how you should use Council supplied mobile devices. It outlines your personal responsibilities and tells you what you should and should not do.

This policy replaces all locally agreed acceptable usage policies for mobile devices.

2. Who audits compliance with this policy?

Policy compliance is audited Councils ICT or Audit Section.

3. Related Copeland Council codes, policies and guidance

The Copeland Council:

- Email Policy
- Internet Policy
- Mobile Phone Standards
- Data Protection Policy
- Information Security Policy
- Freedom of Information Act Guidance
- Employee Code of Conduct

4. To whom does the policy apply?

This policy applies to all employees, agency and contract workers using Council supplied mobile devices.

External contractors accessing Council systems or data using non-Council supplied mobile devices must have approval to do so from the IS Director.

5. When does the policy apply?

At all times.

6. What is the definition of a mobile device?

A mobile device is a portable device that is used to access Council IT systems and store or transmit data from any location. Examples include laptops; tablet PC's, Personal Digital Assistants, Smartphones, Blackberry's, mobile phones and USB flash drives.

7. Purpose of providing mobile devices

The Council provides mobile devices to enable staff to access IT and telecommunications systems from any location as part of their employment.

Mobile devices that are not supplied by the Council **must not** be connected to the Council network.

Personal mobile phones are permitted but they should be set to silent or discreet mode during working hours and only used in emergency situations.

8. Personal use of council supplied mobile devices

In emergency situations, including circumstances where you are unexpectedly required to work out of hours or at an alternative location, minimal use of your mobile device for personal use is permitted, as long as it does not interfere with work commitments and does not constitute misuse as outlined in the Council policies listed in paragraph 3.

Minimal personal use means infrequently and for seconds, rather than minutes and should be kept to unavoidable, emergency situations.

9. Things you must not do

Except where it is strictly and necessarily required for your work, you **must not** use your mobile device to do the following:

- ***X*** Transmit picture messages.
- ***X*** Transmit video messages.
- ***X*** Download music or video files.
- ***X*** Download ring tones or games.
- ***X*** Make international phone calls.
- ***X*** Send international SMS text messages.
- ***X*** Dial or text premium rate phone numbers (e.g. Orange 177 & 241)
- ***X*** Use multimedia services.

The above list gives examples of "*inappropriate*" use but is neither exclusive nor exhaustive.

10. Monitoring the use of mobile devices

The Council has a duty to monitor how the organisation operates and how its individual employees perform whilst at work. Lawful monitoring is undertaken to safeguard employees as well as protect the interests of the Council and its customers. It is also undertaken so that Managers can ensure the smooth running of their Department and to enable the management of resources.

Be aware that the usage of mobile devices will be monitored by ICT to ensure that it is in accordance with the policies and procedures of the Council.

If you need to use your mobile for personal use you must sign up to the Council's split billing facility. Further information can be obtained from ICT or HR.

A summary of personal usage above the accepted minimum (see section 8) and the associated costs will be provided to individuals. These costs will be reclaimed by the Council.

Any personal usage above the permitted minimal use that is not repaid will be dealt with in accordance with the Council's disciplinary procedure where necessary. In disciplinary situations the Council will be the arbiter of whether or not the minimal personal use test has been met

All mobile devices must be available to be returned to the Council on request for updates and auditing purposes.

11. Mobile devices and the Law

Your Mobile Device must not be used in a way that contravenes the Law.

Under the Freedom of Information Act, any copy of a file held on a Copeland mobile device will be accessible to the general public. If you choose to delete this file after you know that it has been requested then you are committing an offence for which you, not the Council, will be personally liable.

Under the Data Protection Act we have a duty to protect personal or sensitive information. Some mobile devices have very limited security facilities and should not be used to store personal, sensitive or confidential information without additional controls. See the appendices for examples of these controls and advice on how to assess risks.

The law (Road Vehicles (Construction and Use) (Amendment) (No. 4) Regulations 2003) prohibits drivers from using a hand-held mobile phone, or similar device, while driving. Employees must never use a phone while driving and ensure that their phone is switched off when driving.

12. Your responsibilities as a mobile device user

It is your responsibility to:

- ✓ **Familiarise** yourself with this policy, supporting guidance and the related policies listed in paragraph 3 before using a council supplied mobile device.
- ✓ **Assess the risks** associated with using your mobile device. A recommended assessment process is provided at Appendix C.
- ✓ **Keep** your mobile device secure at all times. Advice on protecting your mobile device and using your mobile device in a public place are attached as appendices.

13. Whom should I ask if I have any questions?

In the first instance, you should refer questions about this policy to your Line Manager who will refer you to HR if appropriate.

You should refer technical queries about mobile devices to the ICT Helpdesk on extension 8232.

14. What will happen if I do not abide by this policy?

If you are found to have breached this policy, you may be subject to the Council's disciplinary procedure. If you have broken the law, you may be subject to prosecution.

Appendix A – Advice on Protecting Your Mobile Device

There are many products available to help protect your mobile device from loss, damage or theft. You should choose them based upon how you intend to use the device. The following are a selection.

- USB/password locking devices to prevent access to sensitive contents.
- A proximity detector device will sound an alarm if the distance between you and your device goes over 100m. This helps prevent users from accidentally leaving devices in public places.
- A special plastic sheet to limit the viewing angle of a flat screen when viewing sensitive data in public
- Cables to secure devices to immovable objects e.g. a desk.
- Bolt-down cages for transporting devices in a car boot.
- Permanent UV marker pen to mark mobile devices with a postcode (the police will return these items if found)
- Mark the device with a phone number so that lost items can be returned.
- Carrying cases that do not advertise or identify their contents.
- Special locks to secure the equipment where necessary.
- Cryptographic Controls e.g. encryption software. The best and easiest way to secure data on a mobile device is to encrypt it. I.e. scramble the contents of the disk in some way that can only be unscrambled by a specific password or device. If the machine is stolen, the thief cannot access the data.

The above controls introduce an extra level of complexity and may incur a maintenance overhead. Some controls introduce a new password or security device that can accidentally make data unavailable to the user. All these factors must be considered before implementation.

If you need further advice on protecting your mobile device please contact the ICT Helpdesk for assistance on 8323

Appendix B – Using Your Mobile Device in a Public Place – a Quick Guide

Care should be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the Council's premises.

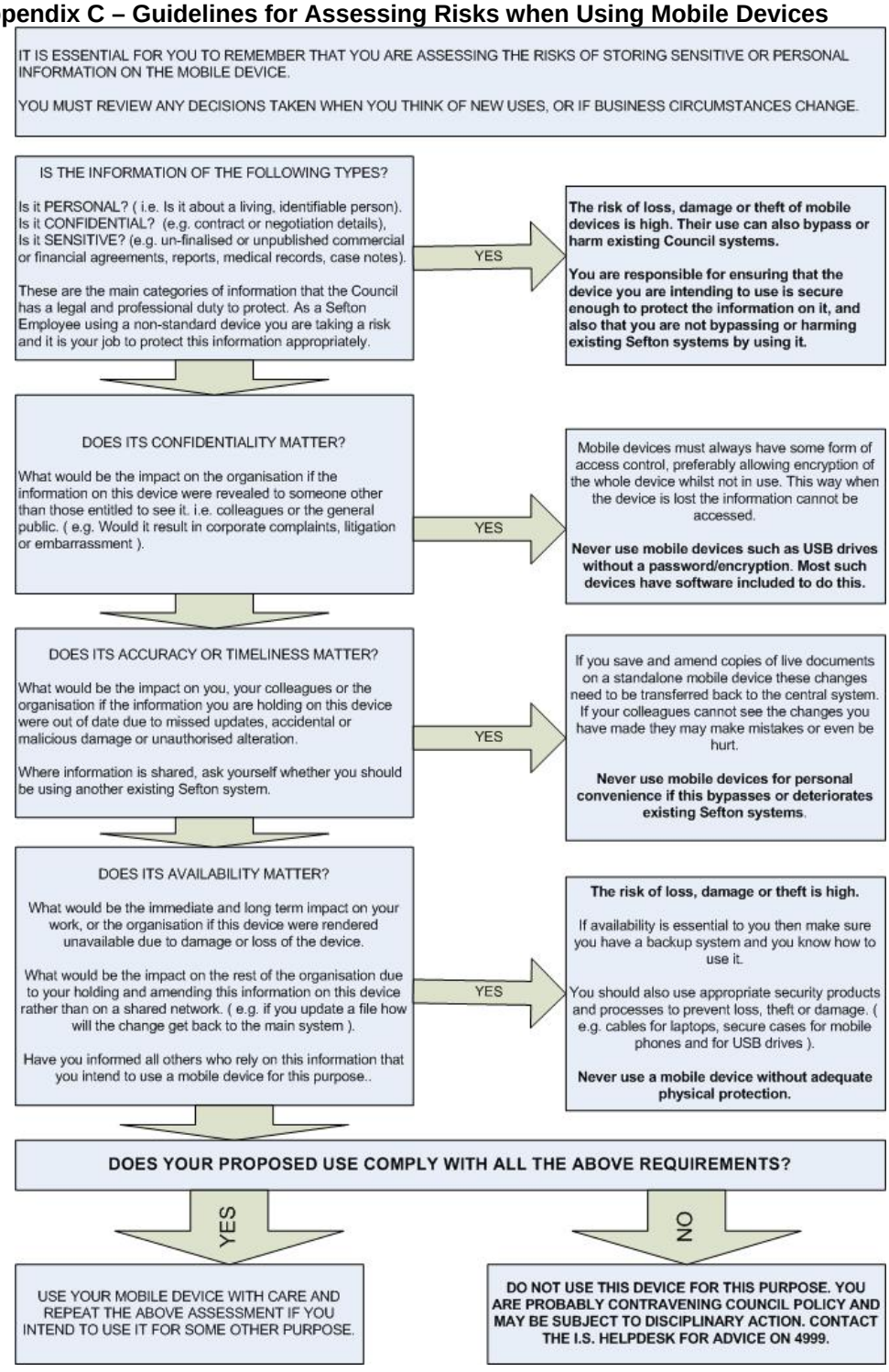
Be vigilant and don't invite crime.

- Make sure you have the right data access controls such as user account names and passwords or security tokens and that you use them properly.
- Secure your device to an immovable object if possible.
- Never leave your device unattended in public places.
- Enter passwords securely, just as you would enter a PIN number.
- Beware of shoulder surfers (people who watch your screen over your shoulder).
- Log out or use a screen saver with a password when you are not using the device.
- Do not give mobile devices to unauthorised persons (including members of your family).
- Carry mobile devices discretely on your person or in hand luggage.
- Never leave your device in view when left in a car.
- Report theft or loss of your device to the police and obtain an incident number.
- Report theft, damage or loss of your mobile device to the IT Helpdesk.

Do your housekeeping.

- Make sure you take regular backups of the data on your mobile device if it is the only copy of the data.
- Make sure your anti-virus software is kept up to date.
- If you no longer need a file then delete it.
- Don't eat or drink near your device.

Appendix C – Guidelines for Assessing Risks when Using Mobile Devices



Copeland Borough Council

Information Security & Acceptable Use Policy

Appendix B

Secure Transfer of Information

Contents

Secure Transfer of Information

Overview

There are many occasions when information is transferred between departments, to third-party service providers, to other public bodies, commercial organisations and individuals. This is done using a wide variety of media and methods, in electronic and paper format.

In every transfer there is a risk that the information may be lost, misappropriated or accidentally released. The Council often has a duty of care in handling information. Recent high-profile losses have highlighted this.

For legal reasons such as confidentiality or data protection, and to maintain the trust of our service users and partners it is essential that the transfer is performed in a way that adequately protects the information. It is the role of the Sender to assess the risks and ensure that adequate controls are in place. This policy outlines the responsibilities attached and the minimum security requirements for transfer.

Scope

This policy states the minimum security requirements for physical transfer of information into, across and out of the organisation, in any format.

For the purpose of this document, Information refers to both textual information (e.g. word-processed documents, reports and spreadsheets), and raw unformatted data (e.g. backup tapes), in any format and on any medium.

This policy applies to all employees of the Authority and any Third-party that processes the organisation information.

Exclusions

This policy does not cover the transfer of information over the Copeland internal network, which has its own automated security controls. It does not cover proprietary secure transfer mechanisms such as BACS financial transfers that have their own separately implemented security requirements.

Policy Statement

The organisation recognises its responsibility to process its information correctly and in line with all legal, regulatory and internal policy requirements.

It is the Sender's responsibility to risk assess what they are intending to do and ensure that all associated risks are adequately understood and covered, and that the transfer is properly authorised. The baseline security requirements for various methods are listed below.

The ICT and Audit will monitor compliance with this Policy.

If a user is found to have breached this policy, they may be subject to the Council's disciplinary procedure. If they have broken the law then they may be subject to prosecution.

If a user does not understand the implications of this policy or how it may apply to them, they should seek advice from either their Line Manger or the Council's Data Protection Officer (Martin Jepson).

Definitions

Requester – Any individual that requests records from a Council department. They may be another Council department, a Service provider, or an external Agency.

Sender - The Sender is the individual acting for the Council that initiates a Data Transfer. They must have the authority, and the sufficient knowledge of the nature of the data to determine whether it should be sent, and that it is sent securely. Where the final actual task is delegated to administrative, untrained or inexperienced staff, the original Sender remains responsible for ensuring the Transfer complies with this policy.

Information Owner - Every major type of record (e.g. Invoices, Purchase Orders, Adoption case files) must be assigned an owner within the Council who will be responsible for it throughout its lifecycle. This Owner may work in any department but must have sufficient ability, authority and experience to understand the contents and approve the processing of the record. Record owners must be formally documented.

Roles and Responsibilities

Proper definitions of roles and responsibilities are essential to assure compliance with this Policy. In summary these are:

The Sender

The Sender is responsible for ensuring the following requirements of this Policy are met.

- Assessing the information to be sent, in line with Section 2 of this policy.
- Ensuring that the identity and authorisation of the recipient has been formally confirmed and documented.
- Obtaining the consent of the Data Owner for the transfer.
- Ensuring that the information is sent and tracked in an appropriate manner in compliance with section 3 of this policy.

IT Auditor

The IT Auditor in the Internal Audit section will monitor and audit departments to ensure compliance with all statutory and regulatory obligations, and internal policies.

Departmental Managers

Departmental managers are responsible for ensuring that this Policy is communicated and implemented within their area of responsibility, and for ensuring that any issues such as resourcing or funding are communicated back to their strategic directors in a timely manner.

Individual employees

Individual employees will be responsible for familiarising themselves with this Policy and ensuring that any information transfer for which they are responsible is done in a compliant manner.

Individual employees must report any suspected or actual security breaches related to data transfer in line with the Organisations Incident Management Policy.

Departmental information management specialists

Departmental information management specialists will provide first line advice to departments on Information transfer related issues.

Risk assessment

The sender's responsibility

With each information transfer there is a risk that the information may be lost, misappropriated or accidentally released. It is the responsibility of the sender to assess all risks and ensure that adequate controls are in compliance with this policy. This section contains some of the things that must be considered before transferring information.

If in doubt, contact the Data Protection Officer (Martin Jepson).

Is the transfer legal and necessary?

It is dangerous to assume that because someone asks for information that they are necessarily authorised or legally entitled to have it. If you are in doubt then you should check with your manager.

Once you are sure that the transfer is legal and necessary then you must decide what kind of information you are dealing with. This will determine what security is appropriate.

To transfer personal or confidential information without these checks may leave the Council open to Legal and Reputational damage and the sender may be subject to disciplinary action.

Is it Personal information?

Personal information is about a living, identifiable individual. If it contains details of racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, commission of offences, court appearances and sentences it is further classified as sensitive personal information.

Anything we do with personal information must comply with the Data Protection Act 1998. Basic requirements of the Act are listed in Appendix 1. If in doubt contact the Data Protection Officer or the Caldicott Guardian.

Before you make any transfer you must:

- Ensure transfers to Media organisations are approved by the Communications Department.
- Obtain and document the approval of the Information Owner for transfer
- Ensure that the transfer is legal (in particular under the Data Protection Act. See Appendix below)
- Ensure that the transfer is necessary (is there a less intrusive way)
- Remove or blackout anything that is not essential for the recipient's purpose
- Have a documented agreement in place to ensure the recipient understands their responsibilities under the law, particularly what to do with the transfer file after they have extracted the information to their system

Is it confidential information?

Confidential information is that for which the Council has a duty of confidentiality. This may include information that affects the business interests of a third party, or for which the sender does not hold copyright e.g. bank details, salary details, contracts, agreements.

Unauthorised release of confidential information can leave the Council open to legal sanction or litigation. It can also erode the trust of the Public and its Partners in the Council itself.

Before you transfer you must:

- Ensure transfers to Media organisations are approved by the Communications Department
- Obtain and document the approval of the information owner for transfer
- Ensure that you are not breaching a Duty of Confidentiality
- Ensure that the transfer is necessary (is there a less intrusive way)
- Remove anything that is not essential for the recipient's purpose
- Have a documented agreement in place to ensure the recipient understands their responsibilities under the law, particularly what to do with the transfer file after they have extracted the information to their system

Does Public information need any special controls?

Public information is any information that is freely released or exchanged and presents minimal risk to the Council in terms of content, quality or timeliness e.g. promotional brochures. In general there are no special security requirements for transfer of Public information because their release represents no special risk. Public information will be transferred in the most cost-effective method available.

Before you transfer you must still:

- Ensure any transfers to Media organisations are approved by the Communications Department.
- Seek the permission of the Department that produced or owns this information before making any transfer, even if the transfer appears harmless.

Requirements for Transferring Personal or Confidential Information

Having decided what kind of information you have, and prepared it for transfer, the sender must consider the various methods of transfer available and whether they are appropriate. This section lists the main methods and sets out any restrictions and the requirements for secure transfer of Personal or Confidential information.

For all transfers of Personal or Confidential information it is essential that the identity and authorisation of the recipient has been appropriately authenticated by the sender.

Electronic Mail

Information must be enclosed in an attachment and encrypted using a product approved by the Council set at an appropriate strength. Minimum standard for encryption is AES (256 bit). WINZIP 11.1 and above offer this.

- Any password must be to Organisation standard. 7 characters, mix of alpha, uppercase and numeric. Further details of the password policy can be found in Chapter 7 of the Information Security policy.
- Any password to open the attached file must be transferred to the recipient using a different method than e-mail, e.g. a telephone call to an agreed telephone number, closed letter.
- E-mail message must contain clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipient.
- An accompanying message and the filename must not reveal the contents of the encrypted file.
- Check with the recipient that their e-mail system will not filter out or quarantine the transferred file.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to their line manager.

Electronic Data Transfer (FTP, Secure FTP, BACS, DCSF's COLLECT)

Standard FTP without encryption is inherently insecure and should not be used for transmitting personal or confidential information.

SFTP file transfers are acceptable but such transfers must be set up and administered by the Information Services department.

External secure transmission systems such as BACS or DCSF's COLLECT system are designed to be secure provided that they are implemented configured and used correctly. However, it is the responsibility of the sender to ensure that the use of such a system is appropriate for the use they propose. If in doubt, advice should be sought from the system owner.

Electronic memory, (CD, DVD, Floppy, USB drive, Memory Card)

Information must be enclosed in a file and encrypted using a product approved by the Council set at an appropriate strength. Minimum standard for encryption is AES (256 bit).

WINZIP 11.1 and above offer this.

- Any password must be to Organisation standard. 7 characters, mix of alpha and numeric. Further details of the password policy can be found in Chapter 7 of the Information Security policy.
- Any password to open the attached file must be transferred to the recipient using a different method than e-mail, e.g. a telephone call to an agreed telephone number, closed letter.
- An accompanying message should contain clear instructions on the recipient's responsibilities, and instructions on what to do if they are not the correct recipient.

- An accompanying message and the filename must not reveal the contents of the encrypted file.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to their line manager.

FAX Transmission

FAX is inherently insecure and is not recommended for transfer of sensitive information. However it is acknowledged that certain circumstances demand it.

- Sender must check that the Fax number is correct and that the receiver is awaiting transmission.
- For high sensitivity information the number must be double-checked by a colleague before transmission, and telephone contact should be maintained throughout transmission.
- Both sender and receiver must have an agreed process to avoid their copy being left on the Fax machine, and a clear requirement to securely destroy the message when no longer required.
- The message should contain clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipient.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to their line manager.

Delivery by Post or by Hand

It is essential that the file, whether electronic or paper is kept secure in transit, tracked during transit, and delivered to the correct individual.

- An appropriate delivery mechanism must be used.
- Package must be securely and appropriately packed, clearly labelled and have a seal, which must be broken to open the package.
- Package must have a return address and contact details.
- The label must not indicate the nature or value of the contents.
- Package must be received and signed for by addressee.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to their line manager.

Telephone/Mobile Phone

As phone calls may be monitored, overheard or intercepted either deliberately or accidentally, care must be taken as follows.

- Transferred information must be kept to a minimum.
- Personal or Confidential information must not be transferred over the telephone unless the identity and authorisation of the receiver has been appropriately confirmed.

Internet Based Collaborative Sites

Must not be used for Personal or Confidential information.

Text messaging (SMS), instant Messaging (IM)

Must not be used for Personal or Confidential information.

Appendix 1 - The principles of data protection

The Data Protection Act 1998 stipulates that anyone processing personal information must comply with **Eight Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met.
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.
4. Shall be accurate and where necessary, kept up to date.
5. Shall not be kept for longer than is necessary for that purpose or those purposes.
6. Shall be processed in accordance with the rights of data subjects under the Act.
7. Shall be kept secure i.e. protected by an appropriate degree of security.
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

In most cases the consent of the data subject is required.

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and sensitive personal data. Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

The data subject also has rights under the act. These consist:

- The right to be informed that processing is being undertaken;
- The right of access to one's personal information within the statutory 40 days;
- The right to prevent processing in certain circumstances;

The right to correct, rectify, block or erase information regarded as wrong information.

Appendix 2 - Other resources and links

Internal guidance on implementation of the Data Protection Act, Information Security and related documents are available from ICT and the Data Protection (Martin Jepson) will be able to advise further.

Copeland Borough Council

Acceptable Usage Policy and Personal Commitment Statement GCSX & Copeland Networks

28 July 2009

Document Control

Organisation	Copeland Borough Council
Title	GCSx Acceptable Usage Policy & Personal Commitment Statement
Author	Martin Stroud
Filename	GCSx-APP01060709.DOC
Owner	ICT Manager
Subject	IT Policy
Protective Marking	None
Review date	July 2010

Revision History

Revision Date	Revisor	Previous Version	Description of Revision

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

Contributors

Development of this policy was assisted through information provided by the following organisations:

- Devon County Council
- Dudley Metropolitan Borough Council
- Herefordshire County Council
- Plymouth City Council
- Sandwell Metropolitan Borough Council
- Sefton Metropolitan Borough Council
- Staffordshire Connects
- West Midlands Local Government Association
- Worcestershire County Council

Contents

1 Policy Statement

It is Copeland Council's policy that all users of the Councils Networks understand and comply with corporate commitments and information security measures associated with GCSx and the Councils own Information Security Policy

2 Purpose

GCSx stands for Government Connect Secure Extranet. It is a secure private Wide-Area Network (WAN) which enables secure interactions between connected Local Authorities and organisations that sit on the pan-government secure network infrastructure.

All Council staff will be required to have access to the facilities operated on this network in order for them to carry out their business. This may include staff having access to a secure email facility. All staff requiring access to the GCSx and Copeland Councils own network in any way will be required to read and understand this Acceptable Usage Policy (AUP) and sign the Personal Commitment Statement.

This policy and statement replaces the Council's existing acceptable usage, or any other policies.

3 Scope

All users of the GCSx connection must be aware of the commitments and security measures surrounding the use of this network. This policy must be adhered to by all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council using the GCSx facilities.

All users of Copeland Councils Networks must be aware of the commitments and security measures surrounding the use of this network. This policy in addition to the Councils Information Security & Acceptable Use Policy must be adhered to by all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council using the Copeland Borough Councils Networks and Services facilities.

4 Definition

This policy **must** be adhered to at all times when accessing GCSx facilities and Copeland Borough Councils own networks and service.

5 Risks

Copeland Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- Non-reporting of information security incidents.
- Inadequate destruction of data, the loss of direct control of user access to information systems and facilities etc.
- Un acceptable use of the GCSX Connections and services.
- Un acceptable use of the Councils networks and services

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers**.**

6 GCSx & The Councils Acceptable Usage Policy

All user must read, understand and sign to verify they have read and accepted this policy.

- I understand and agree to comply with the security rules of my organisation.

For the avoidance of doubt, the security rules relating to secure e-mail and information systems usage include:

1. I acknowledge that my use of the GCSx and or the Councils network may be monitored and/or recorded for lawful purposes.

2. I agree to be responsible for any use by me of the GCSx and the Councils Network using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address; and,

3. will not use a colleague's credentials to access the GCSx and the Councils Network and will equally ensure that my credentials are not shared and are protected against misuse; and,

4. will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises); and,

5. will not attempt to access any computer system that I have not been given explicit permission to access; and,

6. will not attempt to access the GCSx and the Councils Network, other than from IT equipment and systems and locations which have been explicitly authorised to use for this purpose; and,

7. will not transmit information via the GCSx that I know, suspect or have been advised is of a higher level of sensitivity than my GCSx domain is designed to carry; and,

8. will not transmit information via the GCSx that I know or suspect to be unacceptable within the context and purpose for which it is being communicated; and,

9. will not make false claims or denials relating to my use of the GCSx and or the Councils Network (e.g. falsely denying that an e-mail had been sent or received); and,

10. will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the GCSx to the same level as I would paper copies of similar material; and,

11. will appropriately label, using the HMG Security Policy Framework (SPF), information up to RESTRICTED sent via the GCSx; and,

12. will not send PROTECT or RESTRICTED information over public networks such as the Internet; and,

13. will always check that the recipients of e-mail messages are correct so that potentially sensitive or PROTECT or RESTRICTED information is not accidentally released into the public domain; and,

14. will not auto-forward email from my GCSx or Copeland Council account to any other non-GCSx or Copeland Council email account; and,

15. will not forward or disclose any sensitive or PROTECT or RESTRICTED material received via the GCSx unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel; and,

16. will seek to prevent inadvertent disclosure of sensitive or PROTECT or RESTRICTED information by avoiding being overlooked when working, by taking care when printing information received via GCSx and or The Council's Networks (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc) and by carefully checking the distribution list for any material to be transmitted; and,

17. will securely store or destroy any printed material; and,

18. will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via GCSx and or the Council's Network(this will be in accordance with the Information Security & Acceptable Use Policy - Computer, Telephone and Desk Use - e.g. logging-off from the computer, activate a password-protected screensaver etc, so as to require a user logon for activation); and,

19. where ICT has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked requiring a user logon for reactivation), then I will not attempt to disable such protection; and,

20. will make myself familiar with the Councils security policies, procedures and any special instructions that relate to GCSx; and,

21. will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of Information Security & Acceptable use policy - Information Security Incident Management; and,

22. will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended; and,

23. will not remove equipment or information from council premises without appropriate approval; and,

24. will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist theft) in accordance with the Councils Security & Acceptable use policy – Mobile working; and,

25. will not introduce viruses, Trojan horses or other malware into the system or GCSx; and,

26. will not disable anti-virus protection provided at my computer; and,

27. will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that the Council informs me are relevant; and,

28. if I am about to leave the Council, I will inform my manager prior to departure of any important information held in my account and manage my account in accordance with the Council's email and records management policy.

Document Date:	[Date signed and agreed by staff member]
Name of User:	[Surname, First Name]
Position:	[Position]
Department:	[Department]
User Access Request Approved by:	[Line Manager Name – Position} [Date]
User Access Request Approved by:	[IT Services Asset Owner(s)] [Date]
Username Allocated	[Username]
Email Address Allocated:	[Email Address]
User Access Request Processed:	[IT Services] [Date]

7 GCSx Personal Commitment Statement

I, [insert User's Name], accept that I have been granted the access rights to GCSx and the Copeland Borough Council Network. I understand and accept the rights which have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access services or assets that I am not authorised to access, may lead to disciplinary action and specific sanctions. I also accept and will abide by this policy, personal commitment statement, and Copeland Council's Security and Acceptable use policy. I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to the invocation of the Council's disciplinary policy.

Signature of User: ……

A copy of this agreement is to be retained by the User and HR services

8 Policy Compliance

If any user is found to have breached this policy, they may be subject to Copeland Councils disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the ICT Manager

9 Policy Governance

The following table identifies who within Copeland Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	ICT Manager
Accountable	Section 151 Officer, Head of Finance & MIS
Consulted	HR Services
Informed	All Copeland Council Employees, Councillors, Contractors, Partners and 3rd parties requiring GCSx Access

10 Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by ICT Manager.

11 References

The following Copeland Council policy documents are directly relevant to this policy, and are referenced within this document:

- Information Security & Acceptable use Policy.
- Computer, Telephone and Desk Use Policy.
- Remote Working Policy.
- Legal Responsibilities Policy.

The following Copeland Council policy documents are indirectly relevant to this policy:

- Email Policy
- Internet Acceptable Usage Policy.
- Software Policy.
- IT Access Policy.
- Removable Media Policy.
- Information Protection Policy.
- Human Resources Information Security Standards.
- Information Security Incident Management Policy.
- Communications and Operation Management Policy.
- IT Infrastructure Policy.