



# Corporate Information Security Policy

## Manual & Electronic Information

Version Number	Author	Version	
		Version Date	Comments
Draft 0_01	Anthony Phillips	24 <sup>th</sup> February 2009	New document following 1998 policy review
Draft 0_02	Anthony Phillips	2 <sup>nd</sup> March 2009	Updated following RS feedback.
Draft 0_03	John Willis	15 <sup>th</sup> June 2009	Updated with Feedback from Users
Draft 0_04	John Willis	16 <sup>th</sup> June 2009	Updated with feedback from HR, Mark Williams
Draft 0_05	John Willis	24 <sup>th</sup> June 2009	Updated with feedback from Legal, Husinara Islam
Draft 0_06	John Willis	6 <sup>th</sup> July	Added the policy summary and statement of Principles Changed numbering to comply with project office standards. Re-named Policy Summary as Summary
Draft 0_07	Nick Daniels	16 <sup>th</sup> October 2009	Amendments made as recommended from audit on 16/10/09 & Additional PCI DSS summary section.
Final 1_00	Rob Scott	22 <sup>nd</sup> October 2009	Agreed by IAB
Draft update 1_01	Rob Scott	11 <sup>th</sup> February 2010	Section 11.12: specific instructions on encrypted memory devices. Section 11.4.3: Clearer guidance added on passwords management and complexity.
Draft update 1_02	Rob Scott	01/03/10	Improved wording and password controls
Draft update 1_03	B Keen	27/06/11	Section 8.6 Updated wording re GCSX use.
Draft update 1_04	Matt Osborn	18/07/11	Section 11.4.3: Password change frequency amended from 30 days to not more than 90 days.
Draft update 1_05	Matt Osborn	01/11/11	Slight correction to formatting and spelling. Addition of paper reference to section 1 and 3.4. Addition of section 13.5 and change of section 13's heading.
Update 1_06	Matt Osborn	12/12/12	Update of documents and fix broken links

Update 1_07	Matt Osborn	12/05/14	Update to Section15

**Version Awareness:**

The audience of this document are made aware that a physical copy may not be the latest available version. The latest version, which supersedes all previous versions, is available at <http://intranet.bcc.lan/informationsecurity>. Those to whom this policy applies are responsible for familiarising themselves periodically with the latest version and for complying with Policy requirements at all times.

## Document Contents

1 Foreword.....	5
2 Policy summary/statement of principles.....	6
3 Summary .....	7
4 Security Management and Responsibilities .....	10
5 Security Aspects of Human Resources.....	13
6 Information Systems, Acquisition, Development, and Maintenance .....	14
7 Information Classification.....	16
8 Enabling the flow of information.....	18
9 Risk management.....	21
10 Business Continuity .....	22
11 Control of Access and Assets .....	24
12 Information Security Incident Management.....	32
13 Physical Security of Information.....	35
14 Using BCC IT Equipment outside of the UK .....	37
15 Home, flexible, and mobile, working Information Security Standards .....	38
16 Compliance And Legal Requirements.....	40
17 Audit of Information Systems .....	43
18 Glossary and Abbreviations .....	44
19 Associated Policies, Procedures, Standards, and Guidance Notes .....	47

# 1 Foreword

The transmission, storage and removal of information within and outside of the Council is an important necessity in every directorate. Ensuring the security of this information in all formats (electronic and paper based) can present significant challenges. If there is a loss of confidentiality, integrity or availability, or the use of the information does not comply with legal requirements, then this has a serious effect on services and could damage the reputation of the Council.

Therefore, to ensure that information systems can continue to operate, to keep information confidential and to maintain accuracy and integrity, a high level of information security is required.

For this reason, on 19/10/09, the Information Assurance Board (IAB), agreed to the implementation of the guidance contained in this document. Adherence to this guidance is compulsory and applies to:

- Council employees (Officers)
- Councillors (Members)
- Temporary and agency staff, contractors, and consultants who support directly or indirectly or have access to Council information systems
- Employees and agents of other organisations who support directly or indirectly or have access to Council information systems

Any breach of this policy may result in disciplinary and/or criminal proceedings.

## 2 Policy summary/statement of principles

- Bristol City Council will keep information and data it needs to do its work, and nothing else.
- The Councils Information will be accurate
- The Councils information will be made available to those who need it and kept from those who don't.
- The requirements of UK Law will be met to an exemplary standard.
- External Standards and guidance will be used if appropriate. Approvals will only be sought where they improve data security, or are necessary to conduct Council business.
- Information will be classified in accordance with the UK Government Document Marking Scheme.
- The Bristol City Council Risk Management Policy will be used to determine appropriate security measures for all information related systems and procedures.
- All Council, staff, contractors, and other users of Council information, must maintain information security.
- All Council, staff, contractors, and other users of Council information, must report security incidents as soon as they become aware of them.
- The Council will provide appropriate security training for staff.
- All users of Council information must be constrained by legally binding contracts to meet the requirements of this policy. Employees through their conditions of employment, non-employees by terms and conditions in the contract or information usage agreement.
- A Information Assurance Board is appointed and will maintain this policy, and related, policies, procedures, standards, and training material.

## 3 Summary

The purpose of this policy is to protect Bristol City Councils information assets<sup>1</sup> from all threats, whether internal or external, deliberate or accidental. The information / data stored in manual and electronic systems used by Bristol City Council represent extremely valuable assets. The increasing reliance on information technology for the delivery of Bristol City Council service makes it necessary to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion in addition to paper based records. The increasing need to transmit information across networks of computers renders the data more vulnerable to accidental or deliberate unauthorised modification or disclosure.

Bristol City Council will seek to ensure that the confidentiality, integrity and availability of its information is maintained by implementing best practice to minimise risk, as defined by the 27000 set of standards produced by ISO.

Bristol City Council's Information Assurance Board has approved the information security policy.

It is the policy of Bristol City Council to ensure that:

- The Information will be protected against unauthorised access,
- That the confidentiality of information will be assured,
- The Integrity of information will be maintained
- Regulatory and legislative requirements will be met,
- Information security training will be provided
- All breaches of information security, actual or suspected, will be reported and investigated
- Standards will be produced to support the policy, these will include virus controls and passwords.
- Business requirements for the availability of information and information systems will be met
- The head of IT has direct responsibility for maintaining the policy and providing advice and guidance on its implementation.
- All business managers are directly responsible for implementing the policy within their business areas and for the adherence by their staff.
- It is the responsibility of each employee to adhere to the information security policy.

### **3.1 Summary of Legal Requirements**

Some aspects of information security are governed by legislation, the most notable U.K. Acts are:

- The Data Protection Act (1998)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)

- Freedom of Information Act (2000)
- Human Rights Act (2000)

### ***3.2 Purpose and Scope of the Policy***

The purpose of security in any information system, computer installation or network is to preserve an appropriate level of the following:-

- **Confidentiality** the prevention of the unauthorised disclosure of information
- **Integrity** the prevention of the unauthorised amendment or deletion of information
- **Availability** the prevention of the unauthorised withholding of information or resources

The level of security required in a particular system will depend upon the risks associated with the system, the data held on the system and the working environment of the system.

This policy applies to all information held in both paper and electronic formats.

### ***3.3 Who is affected by the policy***

The Policy applies to all employees. It also applies to contractors and visitors, not employed by Bristol City Council but engaged to work with or who have access to Bristol City Council information.

- Council employees (Officers)
- Councillors (Members)
- Temporary and agency staff, contractors, and consultants who support directly or indirectly or have access to Council information systems
- Employees and agents of other organisations who support directly or indirectly or have access to Council information systems

### ***3.4 Where the policy applies***

The Policy applies to all locations from where information held by Bristol City Council is accessed including home and mobile communication use. Where there are links to enable non Bristol City Council organisations to have access to Bristol City Council information, Bristol City Council must confirm the security policies they operate meet our security requirements or the risk is identified, understood and mitigated.

The Policy applies to all systems and all information in any format.

### **3.5 Security Policy Objectives**

- To ensure each member of staff has proper awareness and concern for information system security and adequate appreciation of their responsibilities with regards to information security.
- To ensure all contractors and their employees have a proper awareness for the security surrounding information held, used and accessed by Bristol City Council.
- To provide a framework giving guidance for the establishment of standards, procedures and computer facilities for implementing computer system security.
- To meet the general principles of ISO 27001 Code of Practice for Information Systems Security.
- To specify Bristol City Council responsibilities.
- To ensure all staff have an awareness of the Data Protection Act (1998) and its implications.
- To ensure that all staff are aware of their accountability and that they are aware that failure to comply with the Information Security Policy is a disciplinary offence which may include action up to and including summary dismissal. Any action taken will conform to the appropriate Bristol City Council Human Resource policies.
- To ensure all sensitive information is stored appropriately, made readily available and accurate.
- To ensure that any organisation that we share information with, commonly called a partner, adopts and adheres to the principles and procedures set out in this information security policy.

### **3.6 Review and Audit**

The Information Security Manager is responsible for regular review of the policy in the light of changing circumstances. The review will occur annually or when there are significant changes. Bristol City Council's Internal Audit Office has a brief to ensure that the Policy is appropriate for the protection of Bristol City Council's interests.

## 4 Security Management and Responsibilities

### 4.1 Rationale

Information Security is a shared responsibility. Confidentiality, integrity and availability of information could be compromised due to a breach of security (which could be accidental or malicious) occurring at any point in the information flow.

### 4.2 Allocation Of Security Responsibilities

<b>Senior Information Risk Owner (SIRO)</b>	<b>Overall responsibility for the security of the council's information</b>
<b>Information Assurance Board</b>	<b>Responsible for implementing and maintaining the policy.</b>
<b>Line Management</b>	<b>Responsible for the proper use and security of information and systems under their control</b>
<b>Officers and Members</b>	<b>Responsible for reporting all actual and suspected security breaches</b>
<b>Information Security Incident Response Team (Convened as needed)</b>	<b>Responsible for dealing with any critical security incidents that may occur.</b>

### 4.3 Service Director: ICT

The Service Director: ICT is responsible for providing help and guidance on all matters relating to information security, BUT, ultimately, data owners and the information security manager are responsible for ensuring compliance with the above policy statements and that the systems under their control have an appropriate level of security.

### 4.4 Data Owner

Each information system must have a senior officer in place to act as data owner.

Key responsibilities include:

- Data subject enquiry procedures (as required by the Data Protection Act 1998).
- Preparing details of who can access what information, how and when, according to the particular classification of the information.
- Ensuring that the system is maintained in an effective and controlled manner.

- Ensuring that staff immediately report any violations or misuse of the system to them. The Data owner will then report it to IT Department, if necessary.
- Media and equipment disposal procedures in liaison with the IT Department.
- Liaison with Service Director: ICT and the information security manager.

The Service Director: ICT will offer advice to data owners as to how they can manage their responsibilities. With existing systems, advice is available to help data owners meet their responsibility in complying with the Information Security Policy. With new and proposed systems, advice must be sought at the planning and development phase to ensure systems will meet the security policy requirements before purchase and installation.

#### **4.5 Management Responsibilities**

In order to maintain Bristol City Council's information security and integrity, departmental managers must view Information Security and the training associated with information security with the same gravity as Health and Safety training.

It is the responsibility of tier 3 and above managers to ensure the following, with respect to their staff and contractors:

- Ensuring that all are aware of and adhere to the requirements of this Information Security Policy.
- All should be instructed in their security responsibilities.
- Computer systems/media users must be trained in their use
- Information systems under their control are protected against unauthorised access which would compromise data integrity.
- Should determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status.
- Should implement procedures to minimise Bristol City Council's exposure to fraud, theft or disruption of its systems such as segregation of duties, dual control, peer review or staff rotation in critical susceptible areas.
- Current documentation must be maintained for all critical job functions to ensure continuity in the event of relevant staff being unavailable.
- All are aware of the confidentiality clauses in their contract of employment.
- Relevant system managers are advised immediately about staff changes affecting computer access (e.g. job function changes leaving department or organisation) so that passwords may be withdrawn or deleted as appropriate.
- That all contractors undertaking work for Bristol City Council have signed confidentiality (non-disclosure) undertakings.
- That all have access to the Bristol City Council Information Security Policy.

#### **4.6 Staff Responsibilities**

- Each employee is responsible for ensuring that no breaches of information security result from their actions.

- Each employee is responsible for reporting any breach, or suspected breach of security.

#### **4.7 System Managers**

- Job descriptions for system managers will include specific reference to the security role and responsibility of the post
- The IT systems within Bristol City Council will have a minimum of two, preferably three individuals with the expertise to manage or administer such a system.
- System Managers will be responsible to the Service Director: ICT for continued system security.
- System Managers are responsible for promptly issuing user accounts
- System Managers must ensure that only those persons who are authorised to have access are provided with that capability.

## **5 Security Aspects of Human Resources**

Every officer or member, having access to information shall be made aware of their responsibilities in relation to the protection and management of that information.

The security responsibilities of users shall be documented in the form of policies and procedures and published on the Source.

### **5.1 Personnel Screening and Staff Vetting**

All new employees will be vetted according to the Councils HR Policies and are required to sign the Councils code of conduct.

### **5.2 Contractors**

Contractors and third parties shall have the same responsibility for protecting the Councils Information and data that they would have if they were an employee carrying out the same function. This must be a legally binding requirement in their contract. This will include;

- Contractors and third parties shall be required to sign a confidentiality undertaking.
- Contractors, partner organisations and third parties shall be required to sign an undertaking in respect of protection of Bristol City Council's legal rights and obligations, including copyright and data protection laws.
- Contracts shall detail the actions to be taken if any user, contractor or third party disregards Bristol City Council's information security requirements.
- Contractors and third parties shall be reminded of their confidentiality agreement and other undertakings prior to termination of contract.

### **5.3 Changes in Employment Status**

Line managers shall be responsible for managing the information security considerations relating to the termination of, or changes to an employees employment status or role.

All employees, contractors and third-parties shall return all Bristol City Council assets (including keys and passes) in their possession upon termination of or change to their employment, contract or agreement.

The access rights of all employees, contractors and third-party users shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Any information on the network or email accounts of former employees, contractors or third party users shall be re-assigned as appropriate prior to termination and removal of the account.

Where a former employee, contractor or third party user has knowledge of passwords permitting access to sensitive or confidential information, the passwords shall be reset.

## **6 Information Systems, Acquisition, Development, and Maintenance**

All information system acquisition, development and maintenance must comply with the IS&T. strategy and policies for Bristol City Council. All system developments must include security issues in their consideration of new developments, seeking guidance from the Service Director: ICT or the information security manager where appropriate.

- **Security requirements analysis and specification**

Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

- **Input data validation**

Data input to an information system must be validated to ensure that it is correct and appropriate.

- **Control of internal processing**

Internal processing checks must be performed to minimize the risk of processing failures or deliberate acts leading to a loss of integrity.

- **Message integrity**

Message integrity controls must be used for information systems where there is a security requirement to protect the authenticity of the message content.

- **Output data validation**

Data output from an information system must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

- **Cryptographic controls**

The use of cryptographic controls must be based on the risk of unauthorised access and the classification of the information or information system that is to be protected.

- **Key management**

A key management system based on an agreed set of standards, procedures and methods must be used to support the use of cryptographic controls.

- **Security of system files**

The implementation of software on operational information systems must be controlled.

- **Protection of system test data**

Test data must be protected and controlled using the same procedures as for data from operational information systems.

- **Access control to program source code**

Access control must be maintained for program source libraries.

- **Change control procedures**

Changes to software must be controlled by the use of formal change control procedures.

- **Technical review of applications after operating system changes**

Information systems must be reviewed and tested when operating system changes occur.

- **Restriction on changes to software packages**

Modification of commercial-off-the-shelf software is limited to essential changes that are strictly controlled and documented.

- **Outsourced software development**

Controls must be applied to secure outsourced information system development.

- **Vulnerability Management**

Regular assessments must be conducted to evaluate information system vulnerabilities and the management of associated risks.

# 7 Information Classification

## 7.1 Classification Guidance

- Information shall be classified according to its value, legal requirements, sensitivity and criticality to Bristol City Council.
- A seven-part classification has been adopted, in line with the national protective marking scheme, for all information assets and documents held by and published by Bristol City Council.

The levels of classification and examples of information within each level are detailed below. Summarised guidance notes are available from the Information Classification Guidance document available at:

<http://intranet.bcc.lan/informationsecurity>

## 7.2 Classification Levels of Protectively Marked Information

### 7.2.1 Level 0 - Unclassified Information

This level of classification relates to information that has no current local, national or legal restrictions on access or usage.

### 7.2.2 Level 1 - Due Care

Information that is not intended for public use or disclosure, but where disclosure would not materially impact the Council in terms of financial loss, service delivery failure, loss of reputation or embarrassment.

### 7.2.3 Level 2 - Protected Information

Information that if made public, or even shared within the Council, could cause harm to the Council, its customers and partners. It is information that needs to be secured for legal proprietary, ethical or privacy reasons and access restricted to users who have a legitimate business need to see it.

### 7.2.4 Level 3 - Restricted Information

The compromise of this information or material would be likely: to affect diplomatic relations adversely; to cause substantial distress to individuals; to make it more difficult to maintain the operational effectiveness or security of UK or allied forces; to cause financial loss or loss of earning potential to or facilitate improper gain or advantage for individuals or companies; to prejudice the investigation or facilitate the commission of crime; to breach proper undertakings to maintain the confidence of information provided by third parties; to impede the effective development or operation of government policies; to breach statutory restrictions on disclosure of information; to disadvantage Government in commercial or policy negotiations with others; to undermine the proper management of the public sector and its operations.

### **7.2.5 Level 4 - Confidential Information**

The compromise of this information or material would be likely: materially to damage diplomatic relations (i.e. cause formal protest or other sanction); to prejudice individual security or liberty; to cause damage to the operational effectiveness or security of UK or allied forces or the effectiveness of valuable security or intelligence operations; to work substantially against national finances or economic and commercial interests; substantially to undermine the financial viability of major organisations; to impede the investigation or facilitate the commission of serious crime; to impede seriously the development or operation of major government policies; to shut down or otherwise substantially disrupt significant national operations.

### **7.2.6 Level 5 - Secret Information**

The compromise of this information or material would be likely: to raise international tension; to damage seriously relations with friendly Governments; to threaten life directly, or seriously prejudice public order, or individual security or liberty; to cause serious damage to the operational effectiveness or security of UK or allied forces or the continuing effectiveness of highly valuable security or intelligence operations; to cause substantial material damage to national finances or economic and commercial interests.

### **7.2.7 Level 6 - Top Secret**

The compromise of this information or material would be likely: to threaten directly the internal stability of the UK or friendly countries; to lead directly to widespread loss of life; to cause exceptionally grave damage to the effectiveness or security of UK or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations; to cause exceptionally grave damage to relations with friendly Governments; to cause severe long-term damage to the UK economy.

## **8 Enabling the flow of information**

### **8.1 Regular Sharing of Data / Information with other organisations**

Bristol City Council works with partner organisations which all have a legitimate role to play in delivering services. Partners, in this context, include, but not limited to:

- Central Government
- Educational institutions
- Industrial partners
- NHS
- Other local authorities
- Other local authorities
- Police
- Private sector providers
- Social Services
- Voluntary sector providers

An information sharing agreement shall be agreed between the council and any partner before any information is shared.

### **8.2 Ad-Hoc Sharing Data / Information with other organisations**

Bristol City Council receives ad-hoc requests for personal data. Organisations requesting such information include, but not limited to:

- Insurance companies
- Members of the public
- Police
- Solicitors

Whilst such requests may be legitimate, Bristol City Council will ensure the use of such information is not abused and is in line with the Data Protection Act 1998, by applying the following principles when considering the release of the information to non-partner organisations:

- Information will not be released without the consent of the individual concerned
- The Police will be asked to provide a 'section 29 certificate' These requirements may be waived in certain conditions (E.G. as a result of a court order, or where this information is required by law) but only after authorisation has been obtained from Bristol City Councils legal department.

### **8.3 Purpose and usage of information systems**

Bristol City Council provides employees with access to a variety of information technology systems and electronic communication media for the pursuance of Bristol City Council business. For further information see the code of conduct.

### **8.3.1 Intent to Enforce and Monitor Information Systems**

Bristol City Council reserves the right to carry out monitoring exercises on its systems, possibly without prior notice. Monitoring, via software may be used to block and read any email on the Bristol City Councils network, and access to the Internet.

### **8.4 Intruder and Malevolent software protection**

The Bristol City Council ICT department provides protection against intruders and malevolent software sufficient for its business use.

The responsibility for this protection must be clearly defined for all ICT systems, used for Council Information, that are not owned by the Council. This includes home & mobile computing.

Users must not bypass this protection, test it, knowingly take advantage of gaps, or pass information about it to other parties.

### **8.5 Encryption of security marked information**

Information marked at level 2 protect or above must be encrypted when transmitted electronically, unless it is transmitted using the Government Secure Extranet (GCSX). Encryption should meet FIPS 140-2 standard.

The encrypted file must be sent using a pre-arranged procedure that ensures secure delivery.

### **8.6 Email**

Bristol City Council provides email for the pursuance of Bristol City Council business. Email sent to users outside the council's internal email system and outside of specialist secure systems such as the Government Secure Extranet (GCSx), should not be used for sensitive information.

#### **8.6.1 Care in drafting email**

Emails must be drafted carefully, taking into account any form of discrimination, harassment, Bristol City Council representation, and defamation of Data Protection issues. Staff emails are a form of corporate communication and therefore should be drafted with the same care as letters. Before sending proof read to make sure your message is understandable and appropriate. Do not send sensitive or emotional emails. If you are angry re-read it after you have calmed down. Never draft an email solely using CAPITALS, use normal sentence case.

#### **8.6.2 Government Connect Secure Email (GCSx)**

GCSX Mail is the preferred method of communication with other government organisations.

It is accredited for transmitting security marked information up to 3 Restricted, but the information must not be encrypted.

### **8.6.3 Retention and Purging**

Deletion of old emails must be managed by each individual user, keeping in mind storage levels, archival levels, contractual evidence and legal discovery issues.

### **8.6.4 Junk Mail (Spam)**

Email should not be sent to large numbers of people unless you are sure that it is directly relevant to their job. Sending unsolicited mail to many users ('spamming') is wasteful of user time and can disrupt the service, via performance delays, for other users.

### **8.6.5 Very Large Files**

Sending of large files should be avoided where possible. The use of appropriately licensed compression software (e.g. \*.zip files) is advised. Extremely large files should be sent by means other than email.

## **8.7 Internet**

Bristol City Council provides internet access for the pursuance of Bristol City Council business.

The Internet is not secure and it is possible for web sites to download malevolent software (malware). Bristol City Council runs software to prevent this happening on its internal computers. To reduce the risk, users must not attempt to access sites for non business uses.

Confidential information must only be used on computers that are protected from Internet malware.

There must be a legally binding agreement with the computer owner, that malware protection will be maintained effectively, for all computers not managed by the Councils ICT department.

## **8.8 Postal Security**

All sensitive data sent by post, both internally and externally, should be done so in a secure manner. Every effort should be made to ensure sensitive documents reach the intended recipient with minimal risk to the integrity and confidentiality of the information. For guidance on postal security see the handling sensitive paper records standard available [here](#).

## **8.9 Telephone Security**

The credentials of all callers requesting information that may be of a personal or sensitive nature must be checked.

## **8.10 Fax Security**

Bristol City Council management shall ensure that fax communications are protected at all times and that faxes containing personal or sensitive information are sent, and received in a secure manner.

## **8.11 Verbal Communications**

Bristol City Council management shall ensure that verbal communication is discreet with due regard to the sensitivity of the subject under discussion.

## 9 Risk management

### 9.1 Background

Information is a valuable asset of the council, and even the best and most rigorous security measures cannot eliminate the risks of loss, corruption or disclosure. These must be dealt with according to the council's [Risk Management Policy](#). All information systems and changes to information systems must have a robust risk assessment as outlined in the Risk Management Policy, and identified risks must be entered in the Corporate or Departmental Risk Registers where appropriate.

### 9.2 Types of Risk

The main information risks are those of loss (the council no longer has the information); corruption (the information is unusable or wrong); and disclosure (to someone who shouldn't have the information).

For IT systems the risk of Denial of Service (i.e loss or degradation of computer facilities of any kind) should also be considered.

Computer Viruses may lead to any of the above risk types.

### 9.3 Risk Assessment

Risk should be assessed by normal methods in terms of probability:

<b>High</b>	Likely (occurring once or more in 3 years)
<b>Medium</b>	Possible (occurring once in 4 - 10 years)
<b>Low</b>	Unlikely (occurring once in 10 years or more)

and potential consequences :

- Effect on Service Provision
- Financial
- Fraud
- Corruption risk
- Reputation
- Legal
- Environmental
- Personal Safety

### 9.4 Security Incidents

Many security incidents represent increased risk to information, rather than actual loss, disclosure etc. (E.G. a lost memory stick may or may not lead to data being disclosed). In these circumstances risk assessment should be done in the normal way, but probability of harm should normally be assessed as High.

## 10 Business Continuity

Departmental management will be responsible for their own department's contingency plan, its ongoing review and maintenance. This should be seen as part of the wider organisational plan.

The IT Department will be responsible for the technical aspects of all contingency plans and can provide advice on aspects of system data "catch up". They will maintain a Disaster Recovery Plan to ensure that all critical systems can be restored if necessary.

### 10.1 Need for effective plans

Bristol City Council recognises that some form of disaster may occur, despite precautions, and therefore seeks to contain the impact of such an event on its critical business through tested disaster recovery plans.

Bristol City Council recognises that IT systems are increasingly critical to its business and that the protracted loss of key systems/user areas could be highly damaging in operational terms.

Bristol City Council requires tried and tested disaster recovery plans for its computing facilities to be maintained.

#### 10.1.1 Planning Process

The main elements of this process are:

- Service level / business owner identification of critical computer systems and data, key users and recovery time objectives
- Mitigation of risks by developing resilience
- Corporate agreement on prioritisation of key systems and data. Prioritisation into four categories: Systems that support
  - Life and limb services / activities
  - Emergency Response activities
  - Financial and reputational activities
  - Critical Lines of Business
- Identification of areas of greatest vulnerability based on risk assessment
- Developing disaster recovery plans identifying tasks, agreeing responsibilities and defining priorities, including service continuity plans for individual critical systems and disaster recovery plans for the recovery of major infrastructure
- Testing and reviewing plans

#### 10.1.2 Planning Framework

Disaster recovery plans cater for different levels of incident including:-

- loss of a key building
- power failures

- loss of a key part of a computer network
- loss of critical data
- loss of a computer's processing power
- loss of key staff

Disaster recovery plans include:-

- emergency procedures covering immediate actions to be taken in response to an incident (E.G. alerting disaster recovery personnel)
- recovery time objectives for key systems
- fall back procedures describing the actions to be taken to initiate the recovery of systems in a "warm start" scenario
- fall back procedures describing the actions to be taken to initiate the recovery of systems in a "cold start" scenario
- resumption procedures describing the actions to be taken to return to full normal service
- testing procedures describing how the disaster recovery plan will be tested and evidence of regular and adequate testing of Disaster Recovery Plans will be required.

For further information, contact the Civil Contingencies team on 0117 922 4313

## **11 Control of Access and Assets**

### **11.1 Equipment and Software Registers (Asset Control)**

#### **11.1.1 Equipment Inventory**

An inventory of all computer equipment including peripherals will be maintained. It is the responsibility of each business manager or their named representative to detail each item of computer related equipment and software purchased, or disposed of, to the ICT Department. This department will keep a copy of the inventory and will periodically audit software that is installed. This policy will enable differences over time to be seen and then accounted for.

#### **11.1.2 Software Register**

An up to date register of all proprietary software will be maintained to ensure that Bristol City Council is aware of its assets and that licence conditions are followed. This register will normally be maintained by the ICT Department.

### **11.2 Access Control to Secure Areas**

#### **11.2.1 Physical Security**

All central processors / networked file servers/central network equipment will be located in secure areas with restricted access.

Bristol City Council's central computer suite will be a high security area housing corporate computer systems. An entry restriction and detection system will be incorporated to protect the suite.

Local network equipment/file servers and network equipment will be located in secure areas and where appropriate within locked cabinets.

#### **11.2.2 Entry Controls**

Unrestricted access to the central computer facilities will be confined to designated staff whose job function requires access to that particular area/equipment.

Restricted access may be given to other staff where there is a specific job function need for such access.

Authenticated representatives of third party support agencies will only be given access through specific authorisation.

All secure areas will have an entry log which staff and visitors must use.

Regular reviews of who can access these secure areas should be undertaken.

## **11.3 Security of Third Party Access**

### **11.3.1 Access Control**

No external agency will be given access to any of Bristol City Council's networks unless that body has been formally authorised to have access. All non Bristol City Council agencies will be required to sign security and confidentiality agreements with Bristol City Council, this will include all organisations that exchange Information with Bristol City Council.

Bristol City Council will control all external agencies access to its systems by enabling/disabling connections for each approved access requirement. Bristol City Council will put in place adequate procedures to ensure the protection of any information being sent to external systems. In doing so, Bristol City Council will make no assumptions as to the quality of security used by any third party but will request confirmation of levels of security maintained by those third parties. Where levels of security are found to be lower than those at Bristol City Council, alternative ways of sending data will be used.

All third parties and any outsourced operations will be liable to the same level of confidentiality as Bristol City Council Staff

## **11.4 User Access Controls**

### **11.4.1 Access to Systems**

Officers, Members and contractors will only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation. All contracts of employment, conditions for contractors who have system access agreements should have a non disclosure clause, which means that in the event of accidental unauthorised access to information, the member of staff, contractor is prevented from disclosing information which they had no right to obtain.

### **11.4.2 Registering users**

Formal procedures will be used to control access to systems. An authorised manager must authorise each application for access. Access privileges will be modified/removed as appropriate when an individual changes job/leaves.

Each application for access should be authorised by the manager against the rules agreed by the Service Director: ICT. Officers and Members will be provided with an account after registration which can be activated by answering security questions.

### **11.4.3 User Identification & Password Management**

A User ID / Account is a means of identifying and authenticating a person, it provides accountability to a person for actions taken.

A password is “Confidential authentication information composed of a string of characters” used to access computer systems. Passwords must be kept confidential. Passwords are the responsibility of individual users; they must not be given to or used by anyone else even for a short period of time. Giving an authorised password to someone unauthorised is a disciplinary offence.

Passwords should be changed regularly and should be sufficiently complex to make them hard to guess. The minimum requirement is:

- Password to be changed at a frequency of not more than 90 days.
- Passwords to be at least 7 characters and contain both alphabetic and non-alphabetic characters.
- None of the previous 20 passwords should be re-used.
- No sequence of more than 3 characters to be used in both new and previous passwords.

Software and hardware systems should enforce the above rules wherever possible, and should force the user to change their password on the first logon and after password resets by system administrators.

Users should avoid “guessable” passwords such as their own name or user id; month names; the name of their team or section or names of spouses and pets.

### **11.4.4 Generic / Shared Credentials**

Generic / shared credentials, accounts or passwords should not be used unless it is in exceptional circumstances, operationally unavoidable and agreed by the Information Security Manager.

Initial and re-issued passwords for generic accounts must be subject to confirmation that the requestor & users identification and authorisation for use is correct and current.

## **11.5 Visitors and Contractors**

All visitors to Bristol City Council owned or operated premises should have official identification issued by Bristol City Council and their arrival and departure times recorded. Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation. If temporary passwords need to be issued to allow access to confidential systems these need to be disabled when the visitor has left or remote access is no longer required. There is a requirement for System managers to have a procedure in place for the secure control of contractors called upon to maintain and support computing equipment and software. The contractor may be on site or working remotely via a communications link. The IT Department will advise on the most suitable control.

## **11.6 Housekeeping**

### **11.6.1 Data backup**

Data should be held on a network directory where possible, to ensure routine backup processes capture the data. Should information be held on a local PC hard drive, the PC "user" is responsible for backups. Data should be protected by clearly defined and controlled back-up procedures which will generate data for archiving and contingency recovery purposes. The IT Department and all other systems managers should produce written backup instructions for each system under their management. The backup copies should be clearly labelled and held in a secure area. Procedures should be in place to recover to a usable point after restart of this backup. A cyclical system, whereby several generations of backup are kept, is recommended. Archived and recovery data should be accorded the same security as live data and should be held separately, preferably at an off-site location. Archived data is information which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes. Recovery data should be sufficient to provide an adequate level of service in the event of an emergency. To ensure that the back-up data is sufficient and accurate, it should be regularly tested. Recovery data should be used only with the formal permission of the data owner or as defined in the documented contingency plan for the system. If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data.

## **11.6.2 Equipment, Media and Data Disposal**

Disposal should only be arranged through the IT Department who will arrange for disks to be wiped to a satisfactory level.

## **11.7 Software and Information Protection**

### **11.7.1 Licensed Software**

All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to disciplinary action. Each user should ensure that a copy of each licence for commercial software is held. The loading and use of unlicensed software on Bristol City Council computing equipment is NOT allowed. All staff must comply with the Copyright, Designs and Patents Act (1988). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired. Bristol City Council monitors the installation and use of software by means of regular software audits; any breaches of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under Bristol City Council Disciplinary Policy.

### **11.7.2 Unauthorised Software & Use**

Bristol City Council will only permit authorised software to be installed on its PCs etc. Approval will be via the IT Department. Bristol City Council will require the use of specific general purpose packages (E.G. word-processing, spreadsheets, databases) to facilitate support and staff mobility. Where Bristol City Council recognises the need for specific specialised PC products, such products should be registered with the IT Department and be fully licensed. Software packages must comply with and not compromise Bristol City Council security standards.

It is recognised that computers and information services owned or provided by Bristol City Council may occasionally be used for personal reasons unrelated to council business, this should be kept to a minimum and undertaken according to the Code of Conduct. Excessive personal use is unacceptable. There are public access points provided for personal use such as webmail and social networking.

The copying or installing of unauthorised software on to computing equipment owned by Bristol City Council is not allowed. Copying or installing unauthorised software may result in disciplinary action under Bristol City Council Disciplinary Procedure. Unauthorised software is one of the main sources of software corruption and viruses which may lead to the destruction of complete systems and the data contained on them. Educational software for training and instruction should be authorised, properly purchased, virus checked and loaded by the IT Department staff or its authorised representatives. Where a software training package includes 'games' to enable the new user to practise their keyboard skills e.g. Windows, then this will be allowed as long as it does not represent a threat to the security of the system.

### **11.7.3 Virus Control**

Bristol City Council seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software positioned in the most vulnerable areas.

Users should report any viruses detected/suspected on their machines immediately to the ICT Service Desk. No newly acquired disks from whatever source, are to be loaded unless they have previously been virus checked by a corporate virus checking package.

Users must be aware of the risk of viruses from email, and the Internet. If in doubt about any data received please contact the ICT Service Desk for anti-virus advice.

### **11.7.4 Time-Out Procedures**

Inactive terminals etc, should be set to time out after a pre-set period of inactivity. The time-out facility should clear the screen. In high risk areas the time-out facility should also close both application and network sessions.

A high risk area might be a public or external area outside the control of Bristol City Council. The time-out delay should reflect the security risks of the area.

Users should log off terminals or PCs when leaving them unattended. PCs or terminals should be secured by a key lock or equivalent control (for example, password access control) when not in use.

For high risk applications, connection time restriction should be considered. Limiting the period during which terminal connection to IT services are allowed reduces the window of opportunity for unauthorised access.

## ***11.8 Equipment Security***

### **11.8.1 Equipment Siting and Protection**

IT equipment must always be installed and sited in accordance with the manufacturers specification. Equipment must always be installed by, or with the permission of the IT Department. Where appropriate environmental controls will be installed to protect central or key equipment. Such controls will trigger alarms if environmental problems occur. In such cases where equipment is sited in a secure area, only authorised entry will be permitted.

## ***11.9 Power Supplies***

Where appropriate, all sites within Bristol City Council will have either UPS or generator backup to the mains electricity supply.

## **11.10 Network Security**

It is the responsibility of the Service Director: ICT to ensure that access rights and control of traffic on all Bristol City Council networks is correctly maintained. Access rights to networked applications will be controlled by system managers. The Service Director: ICT will control access to personal data held on networked servers.

Each system manager has a responsibility for keeping the Service Director: ICT informed of their requirements. This will include the number and names of users, their access requirements in terms of times and locations, the activities requiring network support and the needs of the support contractors.

System managers must keep the Service Director: ICT informed of new users requiring access and those users who no longer need access either through changing jobs or leaving the employment of Bristol City Council. It is the responsibility of the Service Director: ICT, to ensure that data communications to remote networks and computing facilities do not compromise the security of Bristol City Council systems. All communications cabling will be arranged by the IT Department and cannot be authorised without their involvement.

## **11.11 Use of Modems and other communications equipment**

Any unauthorised modification to computers is prohibited and only 'approved modems' and other communicating devices may be attached to laptops not connected to any of Bristol City Council's networks.

## **11.12 Mobile, Portable and Hand-held computing equipment**

### **11.12.1 General**

The person to whom a portable device is issued is responsible for that device and accountable for the security of the information held on it.

Equipment, information in any format or software must not be taken off site by employees without documented management authorisation. (Management may provide authorisation on a 'once only' basis as long as it is subject to regular review) Portable devices must have appropriate access protection, for example passwords and must not be left unattended in public places. Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptop and hand held equipment when leaving an office unattended.

To preserve the integrity of data, frequent transfers must be maintained between portable units and the main Bristol City Council system.

All policy statements regarding the use of software and games apply equally to users of portable equipment belonging to Bristol City Council.

### **11.12.2 Encryption**

Laptops must not store sensitive, protectively marked or payment card data unless there is whole disk encryption deployed on the equipment. The use of a password to start work with the computer when it is switched on, known as a 'power on'

password, is mandatory.

Memory sticks and other devices used to transfer data to or from council owned computers must be encrypted. Only devices obtained through or tested by the council's ICT Service may be connected to computers on the council's internal network. This includes mobile phones, cameras, MP3 players, and any other device containing memory.

**USB sticks supplied by the Council's ICT service are encrypted and suitable for transporting data classified up to IL2.**

## **12 Information Security Incident Management**

### **12.1 Security Incident Definition**

A security incident is defined as any real or suspected incident to the security of information whether electronic or manual and the systems that protect it.

### **12.2 Security Incident categorisation**

There are 4 levels of incident classification, **Critical**, **Significant**, **Minor** and **Negligible impact**.

### **12.3 What is monitored under this policy**

This policy will enable the reporting and recording of security incidents occurring from internal access security breaches, remote access breaches, virus infiltrations, firewall penetration, internet access misuse, software piracy and mobile device breaches. This list is by no means exhaustive.

### **12.4 Actions to take on the discovery of an incident.**

Upon discovery of an incident you should make a conscious effort to gather the following information:

- a) The date and time of the incident.
- b) Your location
- c) What the incident is
- d) Any actions you have taken.

Once you have all this information you should contact the service desk on 0117 92 23456 and report it as soon as possible.

### **12.5 Lines of Internal Reporting**

All incidents shall be presented to the Information Assurance Board (IAB) for their consideration on a monthly basis, this report will also include details of incidents that have been reported to external bodies. Where further investigation is required on a particular incident, the IAB shall provide the direction, focus and intentions of the extended investigation.

### **12.6 Lines of external reporting**

Bristol city council has requirements to report incidents that are categorised as significant or above to external bodies. The purpose of this is to ensure that we are taking all necessary actions to control the incident. The reporting bodies are GOVCERT UK (Government Computer Emergency Response Team, United Kingdom) and CINRAS (The Communications and Cryptographic Incident Notification, Reporting and Alerting Scheme).

## **12.7 Handling a reported security incident**

Upon receipt of a security incident, the service desk should make a judgement on its criticality using the above classifications and information security policy appendix.

Once a criticality has been assigned it should be handled to the following team or officer:

Critical

Service Director: ICT, Information Security Manager, Internal Audit, Security Team.

Significant

Security Team, Information Security Manager, Internal Audit

Minor

Security Team, Information Security Manager

Negligible impact

Security team

## **12.8 Investigation and Reporting lines for incidents**

Once an incident has been passed to the appropriate team, the designated criticality needs to be rechecked and then the following actions taken;

For Critical Incidents

Either the service director for ICT or the information security manager will activate the ISIRT members and a full and complete investigation, action plan and risk assessment should be carried out. Once all actions have been completed, the incident will be reported to GOVCERT UK (an external body who record and monitor public sector organisation security incidents) by the information security manager.

For Significant incidents

The Information security manager will liaise with the security team and an internal audit representative to carry out an investigation and take any actions necessary to protect Bristol City Council from reputational or financial loss. Once all actions have been completed, the incident will be reported to GOVCERT UK (an external body who record and monitor public sector organisation security incidents) by the information security manager.

For Minor Incidents

The Security team and Information Security Manager will carry out a low level investigation to make sure that the incidents criticality has been assigned correctly in the first incidence, and then take necessary actions, usually disabling accounts or informing line managers where necessary.

For negligible impact incidents

The Security team will carry out a low level investigation to make sure that the incidents criticality has been assigned correctly in the first incidence, and then take

necessary actions, usually disabling accounts or informing line managers.

## **13 Physical Security of Information**

### **13.1 Security within Bristol City Council Offices**

Financial and corporately sensitive information should be stored in a secure area and not left in an unattended, unlocked room. They should only be retained for the minimum length of time that they are absolutely required.

### **13.2 Security Outside Bristol City Council Offices**

All other areas where information is stored should follow general the best practice guidelines of:

- Stored in a secure area
- Not left unattended
- Not kept for longer than necessary

### **13.3 Transportation**

Where it is necessary to transport information in paper format around or outside Bristol City Council sites, the individual is responsible for ensuring their security. When being transported by car, paper based information should be stored in a concealed area.

### **13.4 Responsibility**

All Bristol City Council Staff who use, or come into contact with protectively marked documents are individually responsible for their safekeeping. Staff should be aware of their contractual and legal confidentiality obligations.

### **13.5 Disposal**

Bristol City Council management shall provide access to secure disposal facilities for use by all staff. This includes cross cut paper shredders and confidential waste sacks (and secure storage of sacks containing any confidential waste, until collection) for collection and disposal. All staff are responsible for the disposal of sensitive data in the correct manner and ensuring that information that is Impact Level 2 (Protect) or above is disposed of securely.

Any data stored on electronic equipment (e.g. printers, hard disks, cameras, phones ) needs to be disposed of in accordance with the Waste Electrical and Electronic Equipment (WEEE) Regulations. Contact the ICT department for disposal of any electronic equipment that contains data.

**For information and guidance please see the [Handling sensitive paper records standard](#) available on the Information Security page of the Source**



## 14 Using BCC IT Equipment outside of the UK

- No Bristol City Council owned equipment can be taken out of the UK without the approval of your line manager. In the instance of the equipment being used by a member, then authorisation to remove the equipment from UK soil should be sort from member services.
- No access to Bristol City Council internal systems services can be attempted from outside the UK without the approval of your line manager.
- Equipment can be confiscated at a country's point of entry. Generally you should assume that if this happens you are unlikely to get it back during the time frame of your visit and should therefore have a contingency plan. It is possible that the equipment will not be returned.
- As IT Equipment can be confiscated at point of entry to a non-UK country you should ensure there is no data on the equipment that could result in a security breach. This includes encrypted data that when decrypted could result in a security breach.
- Always be mindful that using your equipment in public will increase the risk of opportunistic criminal activity.
- Do not leave Equipment unattended at any time. All Equipment must be securely stored (E.G. in an hotel secure storage area) when not being used or carried on your person.
- You should always check the up to date advice from the Foreign and Commonwealth Office (web site here: <http://www.fco.gov.uk/en/> ) for the country you intend to visit. Review all the FCO advice to help you determine if this country has an increased risk of Equipment being lost or stolen. Where the FCO advise against visiting a country, you are not permitted to take BCC equipment to that destination.
- Do not access internal BCC services from abroad or in any location where you can connect to the Internet, e.g wifi hotspots, internet cafes, unless you are sure the equipment being used and the location of the Equipment are secure. Do not assume that Internet cafes or hotel wifi connections are secure.

## **15 Home, flexible, and mobile, working Information Security Standards**

### ***15.1 Authorisation to Work Flexibly***

Authorisation to work flexibly (home or mobile working etc.) must come from the applicants Bristol City Council Line Manager. Staff are only allowed to commence flexible working after reading and understanding the '[Welcome to your new laptop](#)' information that is supplied with your flexible working solution.

In all matters of information security, this policy (the Information Security Policy) has precedence.

### ***15.2 Authorisation to Remove Data Files***

Formal written authorisation by your line manager is required before any identifiable data files can be taken home. Each line manager must inform the head of ICT of all staff who regularly work with information at home.

### ***15.3 The Transfer of personal data files***

Data files that identify individuals, must not be sent via email to a user's home mail box. Internet mail is not secure and should not be used to transmit confidential information.

### ***15.4 Protecting data files***

All electronic files used at home *must* be protected at least by file level password control. All sensitive information must be encrypted

### ***15.5 Use of privately owned IT equipment for Non-PSN users***

General Internet access carries with it a security risk of downloading viruses or programs that can look around a network and infiltrate password security systems. This information can then be sent back to the originator of the program in order to allow them unauthorised access to our systems. Therefore you must use care when transferring data between your home PC and Bristol City Council network. All home PCs which are used for the manipulation of Bristol City Council data must have a current virus checker.

All use of remote access to Bristol City Council's email services must be done in accordance with the Bristol City Council [Email Security Standard](#).

### ***15.6 PSN users and privately owned IT equipment***

Any member of staff, contractor or councillor that accesses services delivered over the Public Sector Network (PSN) is expressly forbidden from using privately owned equipment to access Bristol City Council systems and information. There will be both procedural and technical controls in place to prevent this.

PSN delivered services include, but are not exclusive to:

GCSx Email  
Customer Information System (CIS)  
Blue Badge Improvement Scheme  
Local Welfare Provision

### ***15.7 Transportation of data or confidential documents***

You should take reasonable care to minimise the risk of theft or damage, IT equipment must be transported in a clean, secure environment. During transfer of equipment between home and work you should keep the equipment out of sight and not leave it unattended at any time.

### ***15.8 Storage of Equipment***

You should take all reasonable steps to minimise the visibility of computer equipment from outside the home, and to secure windows and doors when the home is unoccupied.

Computer equipment or hard copy information should not be left in your car overnight.

### ***15.9 Storage of confidential data or reports***

You should secure confidential data or reports that you are not actively using in the most secure area of your home.

## **16 Compliance And Legal Requirements**

### **16.1 Legislative Acts relating to Information Security**

Although this information security policy seeks its focus and direction from ISO, there are several acts present in the UK that have reference and bearing on an Information Security Policy. The main acts that have significant relevance are listed below.

#### **16.1.1 Data Protection Act (UK) 1998**

The purpose of the Act is to protect the rights of the individual about whom data is obtained, stored, processed or supplied rather than those of the people or the authority that controls and uses personal data. The Act applies to both computerised and paper records.

Bristol City Council will comply with the registration requirements of the Data Protection Act 1998 and any replacement European Union (EU) law. This Act requires that appropriate security measures will be taken against unauthorised access to, or alteration, disclosure or destruction of personal data and against accidental loss or destruction of personal data.

The Act is based on eight principles stating that data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subjects rights
- Secure
- Not transferred to other countries without adequate protection

#### **16.1.2 Copyright, Designs and Patent Act 1988**

This Act states that it is illegal to copy and use software without the copyright owners consent or the appropriate licence to prove the software was legally acquired. Each manager is responsible for ensuring that all items of software in their department are either purchased through, or sanctioned by, the Information Systems Department.

All software purchased will have an appropriate licence agreement which may or may not be a site-wide licence. Bristol City Council, through the Information Systems Department will carry out periodic spot checks to ensure compliance with Copyright Law. Any infringement or breach of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under Bristol City Council Disciplinary Policy.

### **16.1.3 Computer Misuse Act 1990**

This Act states that it is a criminal offence to attempt to gain access to computer information for which you have no authorisation. If it is suspected that any unauthorised access is made to a computer system then disciplinary action may be taken under Bristol City Council Disciplinary Policy. On ending their employment or work for Bristol City Council, employees and contractors must not disclose information which was confidential.

### **16.1.4 Freedom of Information Act (2000)**

The Freedom of Information Act gives everyone a legal right to see information held by public authorities. (Bristol City Council is classified as a Public Authority). The aim is to open up public organisations and to make them more accountable to the electorate.

The Act complements the Data Protection Act 1998; if a disclosure is permitted under the Data Protection Act then the Freedom of Information Act gives the right of access to it. Human Rights Act

The part of the Act most relevant to Information Security refers to Article 8 of the European Convention on Human Rights. Personal data is part of an individual's "private life" and as such they have the right to have such information treated in the strictest confidence

- Everyone has the right to respect for his private and family life, his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

## **16.2 Non-Legislative Acts**

### **16.2.1 ISO 27001**

ISO 27001 is the International Standard on Information Security Management initially developed by the British Standards Institute and the Department of Trade and Industry with the co-operation of various private and public sector organisations, including Healthcare. There are two parts to the application of this standard:

**Part 1** is a "Code of Practice for Information Security Management" and provides a comprehensive set of security objectives and control requirements for those organisations seeking to demonstrate compliance with the British Standard.

**Part 2** is a specification for Information Security Management, suitable for

certification of an organisation's information security system.

They provide a set of key controls considered necessary to comply with the standard and detailed guidance to assist the implementation of Information Security. The objective is to provide organisations with "a common basis for providing information security and to enable information to be shared between organisations", which is particularly significant with the increasing exchange of electronic information.

### **16.2.2 PCI DSS**

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. As BCC currently process and store cardholder data we are required to adhere to the PCI DSS controls. PCI have the potential to impose financial penalties for non-compliance.

## ***16.3 Security Policy, Standards and Technical Compliance***

Business managers shall ensure that all security procedures within their area of responsibility are carried out correctly and all systems subjected to at least annual review to ensure their compliance with the security policy and standards.

The technical compliance of information systems shall be reviewed regularly by the ICT Department for compliance with security implementation standards. Risk assessments shall be carried out to identify areas for particularly regular review (E.G. Firewalls). Checks shall only be carried out by, or under the supervision of, suitably qualified persons.

Access controls shall prevent unauthorised persons from doing this work.

## **17 Audit of Information Systems**

### ***17.1 Audit Planning***

Audit requirements and activities involving checks on operational systems shall be planned and authorised in advance to minimise the risk of disruption to business processes.

### ***17.2 Protection of Audit tools***

Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

### ***17.3 Systems Monitoring***

Audit logs recording user activities, exceptions and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

Procedures shall be established for monitoring the use of information processing facilities and the results of the monitoring shall be reviewed regularly.

Logging facilities and log information shall be protected against tampering and unauthorised access.

System faults shall be logged, analysed and appropriate action taken.

The clocks of all information processing facilities shall be synchronised with an agreed accurate time source.

## 18 Glossary and Abbreviations

For the purposes of this document the following definitions apply:

### **Access control**

The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.

### **Accountability**

The property that will enable the originator of any action to be identified.

### **Asset owner**

Individual or organisation having responsibility for specified information assets and for the maintain of appropriate security measures

### **Audit trail**

Data collected and potentially used to facilitate any reconstruction of events in a system

### **Authentication**

Corroboration of the origin and correctness of any part of the system

### **Authorisation**

The granting of rights which includes the granting of access based on access rights

### **Availability**

Information is delivered to the right person, when it is needed

### **BCC**

Bristol City Council

### **Confidentiality**

Data access is confined to those with specified authority to view the data

### **Data Owner**

The person who internal to City Bristol City Council determines the purpose for which the information is to be used.

### **Data user**

Data user means a person who holds data. A person holds data if: The data forms part of a collection of data processed or intended to be processed by or on behalf if that person *and* that person either along or jointly or in common with other persons controls the contents and use of the data comprised in the collection *and* the data are in the form in which they have been or are intended to be processed and with a view to being further so processed on a subsequent occasion [*Data Protection Act (1998)*]

### **Degauss**

To remove unwanted magnetic fields and effects from magnetic disks, take or read/write heads

### **Denial of service**

The prevention of authorised access to resources or the delaying of time critical operations

### **Employee**

Any officer or member of Bristol City Council

### **Impact**

The embarrassment, harm, financial loss, legal or other damage which could occur in consequence of a particular security breach

### **Information Security**

Protection of information for confidentiality, integrity and availability

### **Integrity**

All system assets are operating correctly according to specification and in the way that the current user believes them to be operating

**IT**

Information Technology

**Member**

An elected member of the public.

**Officer**

An employee of Bristol City Council.

**Password**

Confidential authentication information composed of a string of characters

**PC**

Personal Computer

**Personal Data**

Data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in possession of the Data User), including any expression of opinion about the individual but not any indication of the intentions of the Data User in respect of that individual [Data Protection Act (1998)]

**Person Identifiable Data**

Any of the following items:

Surname, forename, initials, address, postcode, date of birth, other dates, sex, NI number, ethnic group, and occupation

**Protectively Marked**

Information in any format that has been classified level 1 or above

**Recovery**

Restoration of a system to a desired date following a failure in the operation of the system

**Risk**

The likelihood of occurrence of a particular threat, with the degree of vulnerability to that threat and the potential consequence of that impact if the threat occurs

**Risk assessment**

Comprehensive concept for defining and assessing the potential impact of threats, and vulnerabilities of, system assets and capabilities, and for supplying management with information suitable for a (risk management) decision in order to optimise investment in security counter measures

**Security breach**

Any event that has, or could have, resulted in loss to Bristol City Council assets, or action that is in breach of Bristol City Council security procedures

**Security Policy**

A statement of the set of rules, measures and procedures that determine the physical, procedural and logical security controls imposed on the management, distribution and protection of assets and information

**Sensitivity**

A measure of importance assigned to information to denote its confidentiality

**Staff**

As employee, any officer or member of Bristol City Council

**System Manager**

The person charged with the technical administration of the computer system.

**System Owner**

The person who determines the purpose(s) for which the system is to be used.

**Threat**

An action or event which might prejudice security

**Vulnerability**

A security weakness

## **19 Associated Policies, Procedures, Standards, and Guidance Notes**

Listed below are the relevant legislative acts and Bristol City Council policies and procedures supporting this document:

Data Protection Act 1998

Copyright, Design, & Patents Act 1988

Computer Misuse Act 1990

Freedom of Information Act

Human Rights Act

Health & Safety (DSE) Regulations

Companies Act 1985

Enterprise Act 2002

Bristol City Council's Modern Records Retention Schedule

Bristol City Council's Acceptable Use Policy

Bristol City Council's Email Security Standard

Bristol City Council's Employee Code Of Conduct

Bristol City Council's Member Code Of Conduct

Bristol City Councils IT Security Guide

Bristol City Council's Backup Policy

Bristol City Council's Disciplinary Procedures

Bristol City Council's Information Classification Guidance

Bristol City Council Corporate Secure Sanitisation of Equipment Standard

Bristol City Council's Security Incident Response Procedure

Bristol City Council's Handling Sensitive Paper Records Standard

Bristol City Council's Guide to Data Management