

# THE INFORMATION SECURITY AND COMPUTER USAGE POLICY

## PROTOCOL AS TO ROLES AND RESPONSIBILITIES

### 1. **Introduction**

This Protocol :-

- sets out the general purpose of the Policy;
- identifies the individuals to whom this Policy applies; and,
- describes the roles and responsibilities of individuals and groups of individuals.

Barnsley MBC must operate within the law at all times. This Policy and Protocols must therefore be consistent with and enable actions in accordance with current legislation.

### 2. **Purpose of the Policy and Protocols**

- 2.1 The purpose of this Policy is to set out the principles which the Council is seeking to achieve in the management and security of information entrusted to it in order to ensure the cost effective delivery of services to the community by providing a framework around the usage of computer related equipment
- 2.2 The Protocols associated with the Policy set out in detail the responsibilities and operational issues to be adhered to by all who handle information and computer related equipment provided by the Council. Reference within any of the associated Protocols to the Policy is used for the purposes of brevity but should be taken to include the Policy and all associated Protocols.
- 2.3 The Policy provides a framework within which all those handling information can safely do so in fulfilling their roles with the Council. The Policy also sets out arrangements for the management of the key risks for the Council which include the following:-
- infringement of current legislation with regard to criminal activity and information management.
  - the accidental or deliberate, but unauthorised disclosure of restricted, personal, confidential, or other valuable information.
  - the accidental or deliberate disclosure of information or material by an individual which may cause offence to another individual or organisation
  - E-mail borne viruses, malicious computer code or spyware designed to interrupt the day to day business of the Council or illegally obtain confidential information

### 3. **Application of the Policy**

- 3.1 Information is classified as having one of the following values:-
- Confidential
  - Restricted – Personal Data
  - Un -Restricted – Public or Internal

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

(Examples of the practical application of information values are shown in Appendix A to this Protocol.)

Restricted Personal Data is defined in Appendix B to this Protocol

### **The Policy applies to all information with any value other than Non-Restricted**

- 3.1 The Policy applies to elected members, all employees and third parties (e.g. contractors, partnerships, suppliers or agency workers). It applies at their normal place of work or elsewhere in undertaking their duties with regard to the Council and when accessing information or information systems which the Council is responsible for.
- 3.2 The application of this Policy does not include pupils, students or members of the general public. Special advice and guidance is provided which is suitable to their purpose and is available at all schools and locations where public access is provided.
- 3.3 Provision of access to information in either paper format or through computer equipment, information systems and networks is primarily for the business purposes of the Council / school, although restricted personal usage is permitted, as set out within the Policy. The utilisation of access to any such information must be restricted to the authorised purposes of the individual. All information which is classified as being restricted in any way or confidential shall not be divulged to any person or organisation outside of those who are similarly authorised for access.
- 3.4 Use of any facility, equipment or system used to provide access to information by an individual, is subject to the authorisation and discretion of their Supervisor (Council in the case of members, line manager, contract manager or head-teacher) as relevant.

## **4. Roles and Responsibilities**

### **4.1 Chief Executive, Executive Directors, Assistant Directors, and School Governors**

All Executive Directors, Assistant Directors and School Governors must :-

- ensure that appropriate arrangements are in place as part of their internal control environment to ensure compliance with this Policy and in the context of the services for which they are responsible.
- ensure that arrangements are made such that all current and new Users are aware of and undertake their roles and responsibilities and that they acknowledge this in writing.
- ensure that arrangements are made to define information systems and telecommunications contingency plans appropriate to their service as part of business continuity planning. The non-availability of computer systems, offices and paper based documents through fire or flood, and the loss of power / information systems is seen as a major threat to services provided by the Council.
- undertake an annual risk assessment of the confidentiality, integrity and availability of information utilised in the delivery of services, together with arrangements for a regular risk review and record this within the appropriate

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

operational risk register.

- make arrangements to assure that all suppliers, contractors, partners or other organisations with access to information provided by or the responsibility of the Council have the minimum requirements in place as set out in the Protocol for Data Handling for Suppliers.
- make arrangements to maintain an up to date inventory of all mobile devices such as mobile telephones, PDA's etc. A physical check of equipment and a copy of the signed inventory should be submitted annually to the Assistant Chief Executive Information Services or the Executive Director for Education in relation to schools as part of the Annual Governance Arrangements. (This excludes computer equipment such as PC's, laptops and tablet PC's where responsibility for the ICT equipment register rests with Bull TCL, arrangements are shortly to be made for the ICT equipment register within schools)

### 4.2 Assistant Chief Executive (Information Services)

The Assistant Chief Executive is responsible for providing advice and guidance in order to:-

- establish the processes required for compliance with information legislation in relation to :-
  - Data Protection Act,
  - Freedom of Information Act
  - Computer Misuse Act
  - Local Government (Records) Act and
  - Other legislation that impacts on information management e.g. Human Rights Acts, Children's Act.
- fulfil the role of Data Protection Act and Freedom of Information Act Administrator.
- define Information Governance (IG) policies and standards in relation to Data Quality, ICT Technical Security, Roles & Responsibilities of all Users of information, Data / Records Management and Information Sharing Protocols
- commission audits to verify compliance with the IG policies
- ensure appropriate communication and training arrangements are in place for the Chief Executive, Executive Directors, Assistant Directors, Council and Schools Governors with regard to their roles and responsibilities
- establish appropriate arrangements to record and respond to any identified breaches of this Policy.

The Assistant Chief Executive (Information Services) is also responsible for the following matters in order to maintain information security arrangements:-

- Ensuring that information security risks (financial, technical and operational) are assessed and appropriate management of the risks are incorporated into new system developments
- Ensuring that information security risks, arising from the use of contractors to implement or maintain computer systems, are assessed and appropriately managed
- Ensuring that advice is provided on the risks associated with the exchange of information with other organisations, (either in the provision of services to the Council / school or otherwise). That these risks are appropriately assessed,

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

- managed and that the arrangements agreed are adhered to.
- Suitably managing information risks once systems ‘go live’ in the technical environment
- Operates in close collaboration with the Assistant Director of Finance (Audit and Risk Management) in managing these risks

### **4.3 Line / Contract Managers and Head teachers (Collectively these roles are referred to as Supervisors)**

The Supervisors are responsible for :-

- ensuring appropriate arrangements are in place to comply with this Policy and actively promoting compliance by all Users within their responsibility
- making sure all Users (to be clear - this includes employees, elected members, contractors and agency workers, whether they be permanent or otherwise) are aware of and undertake appropriate training to understand and comply with this Policy
- ensuring that the training is undertaken before authorising access to computer equipment, information systems or networks of the Council / school.
- providing authorisation to the Bull TCL Service Desk of access permissions to enable all Users (including those on a temporary basis)
  - to be connected to the network,
  - to be allocated an e mail address and
  - to have access to appropriate information systems relevant to the role of the user.
- Providing notification to the Bull TCL Service Desk of all changes (leavers and moves within the service) to amend access permissions relating to all Users
- ensuring that where an authorisation is for a temporary period only an expiry date is stated at the outset
- ensuring that Users are authorised only to have access via the Bull TCL Service Desk and not through bypassing, or attempting to bypass the Council’s secure network connections.
- consulting with the Assistant Chief Executive (Information Services) before
  - any new information system is specified, procured or implemented
  - any existing system is changed in its content or use
- reporting to the Assistant Chief Executive Information Services of the nature and extent of any identified information loss (either misplaced or stolen) in whatever form it may take. This specifically includes loss of computer equipment and mobile data devices.
- ensuring that the procurement of all telecommunications equipment, computer equipment, data storage media and related services is purchased through the Bull TCL Service desk
- discouraging Users to use hand-held mobile telephones, either personally owned or Council / school provided, whilst they are driving.
- seeking advice from the Assistant Chief Executive (Information Services) with regard to the risk associated with any proposed transfer of information to other organisations, either in relation to the provision of services to the Council / schools or otherwise, and subsequently ensuring the ongoing compliance and control of the agreed arrangements

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

- reporting to Internal Audit any information related incidents brought to their attention or for which there is a suspicion on the part of the Users which has the potential for:
  - legal implications for the Council;
  - to impact on services;
  - by passing information security arrangements
  - inappropriate usage of e-mail, Internet or other computer facilities provided by the Council/school
  - the committing of fraud or corruption
  - concealing any of the above

#### **4.4 Elected members, employees and third parties (collectively referred to as Users throughout this Policy)**

##### **All Users are responsible for :-**

##### Understanding and compliance with the Policy

- reading, ensuring they understand the implications for them and that they work within this Policy and the associated Protocols.

##### Security of all information

- Keeping secure all information (paper based and computer based) in accordance with the value attributed to it. (Confidential, Restricted - Personal Data and Non-Restricted)

##### Security of computers and computer information

- only accessing those computer systems which they have been authorised
  - to access, and
  - in the agreed manner and for the agreed purpose.
- ensuring all computer related actions, Internet access and e-mail messages are sent under their own unique user ID.
- ensuring that they do not inform anyone else of their password or allow anyone else to use their user ID.
- exercise due care in the use of computer systems, any computer equipment provided to them and the information stored on them
- other than in exceptional circumstances, Users should not store Council information on mobile devices or local drives (see Usage and Security of Computer Equipment and Systems, paragraph 4.1
- logging all inadvertent misuse or inappropriate use of information or the computer facilities by registering this with the Bull TCL Service desk (01226 773773) and retaining a receipt of the log.
- utilising a password protected screen saver at all times when leaving the computer / device for any short period of time (a maximum period of 10 minutes is advised) – Guidance on setting up approved screen savers is available from the Bull TCL Service desk.
- logging out or locking the computer / device when leaving it for more than 30 minutes.
- following any specific instructions given regarding software, anti-virus procedures, security, or any other aspect of computer systems by the ICT Service desk

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

- ensuring that the visibility of desktop equipment and screens displaying personal or confidential information is restricted as far as is practicable to only duly authorised systems Users.
- Where mediated access to information systems is required then appropriate procedures must be followed relevant to the information value
- contacting the Bull TCL Service Desk to request new or the re-setting of passwords and referring to local systems policies where applicable

### Loss of Information or Breaches of this Policy

- notifying their Supervisor of
  - the nature and extent of any identified information loss (either misplaced or stolen) in whatever form it may take. This includes loss of computer equipment and or storage devices.
  - any incident or situation which may have a potential impact on the security of information systems or networks;
  - unintentional access gained to unauthorised systems, software / data;
  - the identification of a virus or systems failure / weakness
  - legal implications for the Council;
  - to impact on services; or
  - by passing information security arrangements,
- the User receives an e-mail message, which contains unlawful, indecent or objectionable material. The User should make a note of the details of the originator of the message
- there is a suspicion of inappropriate use of the Internet or e-mail system (including the receipt of offensive or inappropriate material). If the User wishes to remain anonymous, they can report any incident by following the Council's **Whistleblowing Policy**

### **4.5 Internal Audit**

The Assistant Director of Finance (Audit and Risk Management) is responsible for:

- conducting and reporting on Information Governance audits as commissioned by the Assistant Chief Executive (Information Services).
- conducting or commissioning periodic audits of the usage and management of Information Communications Technology (ICT) and Information Systems (IS) in accordance with this Policy.
- maintaining a record of any identified computer misuses or abuse of Internet and e-mail in consultation with Bull TCL.
- maintaining a record of all reported ICT or IS security incidents which impact on services of the Council or have potential legal implication
- investigating either independently or in support of a Supervisor reported misuse of computer equipment and other facilities provided by the Council.

### **4.6 Bull Information Systems (IS)**

Under a Services Agreement between the Council and Bull IS, Bull IS are responsible for providing, maintaining and managing computer equipment, the IT networks and associated computer information systems, ensuring its resilience and the integrity of data. (This does not apply to computer equipment utilised within schools)

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

The service is provided on behalf of Bull IS by Bull Tuscan Connects Limited (TCL) under a sub-contract agreement.

Bull TCL is a Joint Venture Partnership Company (JVC) between the Council and Bull IS, and the JVC owned 20% by the Council.

The responsibilities of Bull are set out in detail within the services agreement; the required interactions between all Users and Bull TCL are set out in this Policy.

### **5. Non-Compliance with the Policy**

- 5.1 All breaches of this Policy will be treated as an issue of the utmost concern.
- Employees of the Council may be subject to disciplinary action under the Council's Disciplinary Procedures.
  - Individual agency staff or workers operating for contractors, suppliers and partnership organisations will be subject to the conditions of the individual contracts.
  - Members of the Council will be subject to the provisions of the member Code of Conduct and the jurisdiction of the local Standards Committee and the National Standards Board for England.

Where it is relevant to do so an individual / organisation may be subject to separate criminal prosecution.

- 5.2 It should be noted that for deliberate and knowing breach of this Policy, where an information loss occurs (which may potentially affect the reputation of the Council, confidence of the public in the Council to manage information securely or potentially cause financial loss); or, where a User is found to be abusing information systems, the Internet, Intranet or e-mail facilities of the Council; then,
- in the case of employees this will constitute potential gross misconduct, possibly resulting in dismissal.
  - in the case of agency staff or contractor this is likely to lead to removal of the individual and may jeopardise the continuation of the contract with the Council.
- 5.3 Any cases of suspected misuse or non compliance will be reviewed within the context and spirit of this Policy on an individual basis.

### **6. Advice and guidance on the application of this Policy**

- 6.1 Any User who is unsure on aspects of the application of this Policy should seek advice and guidance from Supervisors or others with specific responsibilities as set out in section 4 of this Protocol.

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

### Examples of Information Values / Impact

Unrestricted		Restricted Personal Data	Confidential
<u>Unrestricted - Public</u>	Unrestricted - Internal	See Appendix B for detailed definition.	Information that could seriously undermine the organisation, damage security, operations,, finance of economic and commercial interests
<b>e.g. Risk regarded as</b>	<b>e.g. Risk regarded as</b>	<b>e.g. Risk regarded as</b>	<b>e.g. Risk regarded as</b>
Information clearly of interest to the public and in the public domain with no risk to the organisation or individuals	Information that has no risk to the organisation or individuals but is not considered of public interest or public domain i.e. not published	Likely to cause some discomfort, stress or embarrassment to any person or embarrassment to any organisation	Likely to cause a serious crime prosecution to collapse
Examples include: Council & Cabinet Reports, minutes, forward plans, policies and documents for conducting Council Business	Examples include: Internal service meetings, procedure manuals, business continuity plans, internal health and safety, e-learning training packages	Likely to cause financial loss to an individual	Cause a financial loss to the Authority in excess of £10,000
		Likely to cause prolonged distress for many citizens	Likely to cause serious illness or injury to any party
		Likely to cause serious risk to any parties personal safety	Likely to cause substantial financial loss to an individual
			Likely to cause loss of reputation for the authority

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

#### Definition of Restricted Personal Data

As a minimum, personal data includes all data falling in to either category A or B below:-

**Category A Any Information that links one or more identifiable living person with private information about them.**

There should be restrictions on a data set that includes:

- One or more of the pieces of information through which an individual may be identified (name, address, telephone number, driving licence number, date of birth, photograph), combined with
- Information about that individual whose release could cause harm or distress, including:
  - DNA or fingerprints
  - Bank/financial/credit card details
  - National Insurance number
  - Passport number/information on immigration status
  - Travel details (for example at immigration controls, or Oyster records)
  - Tax, benefit or pension records
  - Place of Work
  - School attendance / records
  - Material related to social services ( including child protection) or housing case work
  - Conviction / prison/ court records/evidence
  - Groups/affiliations/politics, race, religion, trade union, health, sexual life as defined by the Data Protection Act (Section 2)

**Category B Any source of information about 100 identifiable individuals or more, other than information sources from the public domain.**

This is a minimum standard. Information on smaller numbers of individuals may justify restricted value because of the nature of the individuals, source of the information, or extent of information.

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

# THE INFORMATION SECURITY AND COMPUTER USAGE POLICY –

## PROTOCOL FOR THE USAGE AND SECURITY OF COMPUTER EQUIPMENT AND SYSTEMS.

### 1. Introduction

- 1.1 This Protocol sets out the requirements for Users to adhere to when they are using computer related devices provided by the Council (irrespective of where or how the device is operated) in order to access ;
- the Council’s computer network;
  - the Internet;
  - the Councils e-mail systems; or
  - any information system provided by the Council;
- 1.2 All Users should be aware that facilities exist to automatically log details of each systems access, Internet site accesses (including duration) access or e-mail issued and received. The details logged include user ID, computer name and applies to both business and personal usage. The logging of such information is to ensure that :-
- an appropriate audit trail is maintained of all computers transactions
  - to determine responsibility in the event of a breach of policy and
  - to conform to the requirements of ‘Local Government Data Handling Procedures’. (Published November 2008.

### 2. Using e-Mail and the Internet

#### 2.1 **General Usage**

- 2.1.1 E-mails have the same legal authority as signed letters on official headed paper, presenting an impression of the Council / school both within the organisation and to the outside world.
- 2.1.2 It should be recognised that some e-mails form part of the formal Records of the Council and should be managed as such.

Note A Record is – information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in transaction of business – ISO 1549

- 2.1.3 E-mail is frequently not the best way to communicate information. Messages by - mail can often be misunderstood, and the volume of e-mail messages can be prohibitive to a meaningful and accurate reply as a result of e-mail overload. It should be the active consideration by the sender to determine if e-mail is the most appropriate method to communicate the information.
- 2.1.4 E-mails sent to external organisations relating to business on behalf of the Council /

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

school all carry an automatic legal disclaimer relating to the nature of the e-mail and the use of the communication by the recipient.

- 2.1.5 Users should not forward an e-mail to an e-mail facility provided by themselves in their private capacity as this will present a security risk where the e-mail contains restricted personal data or confidential information.,
- 2.1.6 The consequences of a User disregarding this requirement is that any transaction conducted in this way will be a personal commitment by the User and not a commitment upon the Council.
- 2.1.7 All e-mail messages which are necessary for the permanent business records should be stored in appropriate computer folders outside of the mail system and they should be filed and titled using the Council's naming convention. A proposal to develop an e-mail archiving system which will automatically secure e-mails filed in the required manner is in course of development. This policy will be revised when this is implemented together with appropriate communications and training to all Users.
- 2.1.8 E-mails should only be printed out when absolutely necessary and not as a matter of course.

### 2.2 Security in using the e-Mail Facility

- 2.2.1 In order to maintain the security and robustness of the e-mail facility for all, Users are required :-
- not to open any suspect e-mails or attachments to e-mails, particular where the sender is unknown. In such situations the user should delete the e-mails.
  - notify their Supervisor in the event of receiving any threatening, lewd or otherwise inappropriate e-mail...
  - to ensure that the "out of office" facility is to another appropriate colleague user if they are unavailable to use and respond to e-mails for more than the occasional day (e.g. on annual leave). The re-direct mail should be used other than in exceptional circumstances this will potentially breach security arrangements.
  - to compress any large attachments, (if assistance is required to do this contact the Bull TCL Service desk)
  - only to use the delivery / read facility when absolutely necessary and not at all when sending an e-mail to a large group of Users.
  - Not to attempt to establish connections to the e-mail system or Internet facility by by-passing the secure connections provided by the Council.
- 2.2.2 Great care should be taken if it is necessary to send individual items of information which can be classified as personal data, confidential or restricted in any way. Additional checks must be undertaken by the User to verify the correct recipient and that the e-mail should not be capable under normal operations to be intercepted by another, unauthorised individual. If in doubt the User should consult the Bull TCL Service desk.
- 2.2.3 E-mail must not be used for the transmission of substantial volumes of personal,

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

restricted or sensitive information unless it is through an approved and secure network facility such as that provided by Government Connects initiative. In the first instance where this is required it should be undertaken in consultation with the Bull TCL Service desk.

### **2.3 Practical issues in using e-mail**

- 2.3.1 Information has been developed with regard to the style, manner and management of the e-mail facilities; This information is made available on the Intranet site and is revised from time to time. Adoption of the approach is expected of all Users.
- 2.3.2 Users should not make personal comments in e-mails that could be used against the Council / school; any personal opinions expressed by the individual must be declared as such and must not appear to be those of the Council / school.

### **3. Personal usage of the e-mail, Internet and Intranet facilities**

- 3.1 It is recognised that use of the Internet and e-mail for personal purposes will support the flexible work-style introduced by the Council. At the same time the Council recognises the beneficial effects of maintaining and improving IT skills of all Users that personal usage supports. For these reasons it is regarded as acceptable for Users to utilise the e-mail and Internet facilities for personal purposes and without charge. All Users should be aware that if they decide to utilise these facilities there is no right of privacy when accessing the Internet or using the Council's e-mail system to convey personal or private messages
- 3.2 It is recognised that information is available on the Internet which is of an illegal or inappropriate nature. The Council is not seeking to moralise with regard to the lawful attitudes of any User, but regard must be made to the perception the general public would have in the case of any inappropriate usage.

Equipment and systems provided by the Council / school from the public purse requires a form of reasonable usage beyond just simply that which is lawful. The Council / school must also be mindful that a number of Users utilising facilities provided in this way may also have a detrimental impact on the responsiveness of networks and systems. This may have the effect of reducing the effectiveness of the main business usage for which it is provided.

In recognition of the above the requirements below set out the circumstances in which personal usage is acceptable. It should be remembered that in general terms the only acceptable personal usage is to support and enable the flexible work style introduced by the Council, use for other than this purpose is unacceptable even when it is used within the Users own time.

- 3.3 Personal usage is permitted within the following general limitations:-
  - Under no circumstances may the facilities be used for the creation, access, download, copy, view, read, store, transmit or to publish any material which is of an illegal, harmful, or of such a nature as be in breach of the Council's Dignity at

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

Work Policy and Procedures or in breach of copyright.

- Use of the Internet and e-mail must be undertaken in the user's own time. - The user must be able to demonstrate that they are not regarded as working and suitable confirmation of this would be entries on the signing-in / flexi sheet. This record should show the date and time the user stopped working and must not be completed retrospectively.
- Usage must not be used for the setting up or for running a private business.

3.4 In order to protect the Council / school and Users during the approved systems monitoring, all personal / private e-mails must be clearly marked in the subject line as:- Personal e-mail, although it should be recognised that such records may still be monitored.

3.5 There are no income tax and national insurance implications arising as a result of permitted personal usage.

3.6 Examples of acceptable and non-acceptable personal usage of e-mail and the Internet are set out within the table below. This list is not exhaustive and whilst it will be updated from time to time the spirit of the examples must also be observed at all times.

### Acceptable Usage

The following are acceptable personal usage in order to support and enable a flexible work-style:-

- To organise an ad hoc social activity on behalf of your section, department, directorate or school
- Promotion of a charitable event
- To confirm a meeting / lunch arrangement with a colleague
- To confirm an urgent personal booking
- Shopping online (e.g. for groceries)
- Booking a holiday
- To read the latest news headlines
- Use to assist with a Council / school sponsored course of study
- Use for research and development purposes, or other study course (e.g. night which have been approved by their Users.
- Preparation of CV's in connection with an internal job application

### Non-Acceptable Usage

Illegal usage includes:-

- National security – instructions on bomb making, illegal drug protection, terrorist activities
- Protection of minors – abusive form of marketing violence, pornography
- Protection of Human Dignity – incitement or promotion of racial hatred or racial discrimination
- Economic Security – fraud, instruction on pirating credit cards
- Information Security – malicious hacking
- Protection of Privacy – unauthorised communication of personal data
- Protection of Reputation – any form of libellous statement
- Intellectual Property – unauthorised distribution of copyrighted works e.g. software or music.

### Unacceptable usage

It is unacceptable to utilise equipment, Internet or the e-mail system which

- may contravene the Council's

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

### Dignity at Work Policy

- is prejudicial to the Council's / school's interests
- is defamatory or abusive
- is for playing games (other than loaded as part of the standard system package).

### Blocked Sites for the Internet

Access to a number of sites available on the Internet will be blocked by the IT systems as follows:-

- Social Networking Sites ( e.g. MySpace, FaceBook)
- Personal Messaging Systems (e.g. MSN, ICQ)
- Personal Trading (e.g. e-Bay)

## 4. Secure use of computer equipment and systems

### 4.1 Computer and Mobile Computing Equipment

4.1.1 Other than for schools, all computer and mobile computing equipment (including mobile telephones) will be provided by Bull TCL. The equipment will be security tagged and an ICT Equipment register of all equipment, its location and the person it is assigned to (this may, or may not be the User; it may be a named Users where equipment is used by more than one person). It is the responsibility of Supervisors to ensure that information is provided to the ICT Service Desk to enable the ICT equipment register to be updated when the location of equipment is changed or relocated when Users leave / move role.

4.1.2 All information stored on mobile / non-network computer related equipment, such as :-

- mobile phones
- laptops
- tablet Personal Computers
- PDA's, blackberry's,

and removable devices such as:-

- CD/DVD
- magnetic disks

**must** incorporate password protection.

Where equipment is provided with preset factory passwords or pin numbers these must be changed immediately following receipt.

4.1.3 Any restricted personal information held on equipment identified above in 4.1.2 or which relates to a group of people or otherwise classified as being confidential must also incorporate the added protection of encryption, for which advice can be obtained from the Bull TCL service desk.

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

Memory sticks shall only be used for the storage of presentations, such as Microsoft Powerpoint, they shall not be used for the storage or transfer of any other data or information.

### Safe use of Mobile Telephone

- 4.1.4 Users should never make or receive calls using a hand-held mobile telephone whilst driving; this includes periods when the vehicle is stationary at traffic lights or during short traffic delays.
- 4.1.5 Users should utilise the message and / or call divert facilities to enable access to messages only when the vehicle is parked and the engine has been switched off.

### 4.2 Information Systems

- 4.2.1 Many computers contain information which is restricted and must be kept private and confidential to the relevant service or users group, and must only be used for the purpose stated to the person or organisation who is the information subject.

In order to maintain security:

- information systems must be protected by password security to ensure only authorised access is allowed to computer related equipment or information systems.
- all new information systems shall force password renewal automatically at a minimum of 6 monthly intervals. For existing systems, a phased development plan to meet this target must be agreed.
- services should assess whether, information systems containing restricted information, additional password protection security is required. Advice in this regard should be sought from the Assistant Chief Executive (Information Services)
- Supervisors must make arrangements to ensure that the Bull TCL Service Desk is notified with regard to all officers who leave the employment of their service or where their role changes (which changes their information access rights) to enable information systems access rights and ID's to be de-activated.
- Users, who use their own computer equipment when working from home, must be aware of other family usage and ensure that no-one other than the approved User gains access to Council information systems. Information under the responsibility of the Council must not be stored on personally owned equipment.
- the use of a standard, password protected screensaver, where a computer has not been active for a period of time, may be automatically enforced in order to safeguard information and to prevent static screensavers burning images into the screen.

### 4.3 Software Licensing

- 4.3.1 Legal and contractual terms for software licences must be complied with.

It is the responsibility of Bull TCL to maintain an ICT equipment register of all

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

computer equipment and computer software utilised by the Council in order to advise the Council accordingly and to assure compliance. (This does not currently apply to schools)

4.3.2 In order to assure compliance the following requirements must be adhered to:

- Computer software, including upgrades, patches and additions to systems required by the Council must be obtained through Bull TCL. No BMBC employee may purchase computer information systems or computer software of any description.
- The installation of software, including patches, upgrades and additions to computer information systems must be applied using change control procedures without due delay (unless other factors prevail) and only be undertaken by employees of Bull TCL, unless authorised in writing by Bull TCL.
- Changes required to information systems or desktop based software must be requested through the Bull TCL Service Desk and undertaken by Bull TCL in order to maintain the ICT equipment register. This will include changes from one device to another.
- All computer related equipment, mobile devices (including mobile phones PDA's etc), and computer information systems must be disposed of by Bull TCL.
- All licence agreements and original media must be supplied to Bull TCL and retained for the ICT equipment register.
- Software received via e-mail or Freeware; Shareware; Public Domain; Evaluation Software; and fonts (additional to those provided as part of the standard desktop), are bound by the requirements above. Users must not under any circumstances install such software.
- No software whatsoever may be downloaded from the Internet by Users, Supervisors who believe that there is a justifiable service / business need to do so should apply to the ICT Service desk for an exception. The only exception is plug-ins (i.e. RealPlayer, QuickTime, Flash, Shockwave and Java) required enabling the web browser to correctly display pages from acceptable web sites.
- All computer related equipment, including mobile devices are where possible installed with BMBC auditing software for regular checks. Equipment which does not have auditing software installed will be subject to periodic manual audits. As a minimum Bull TCL will audit installed software on an annual basis

4.4 Information Security – (Virus Protection, Data Backups and System Recovery)

4.4.1 To protect the integrity of computer equipment, and information systems:-

Bull TCL will ensure that up to date virus checking software is installed on all servers and computer equipment. For equipment normally connected to the BMBC network this will be done automatically. Where the role of Users is such that they would normally only very rarely connect equipment provided to the network they should ensure that equipment is made available at least on a quarterly basis through the ICT service desk, in order to enable virus updates to be made.

4.4.2 All viruses identified by a User as infecting their computer related devices must be reported to the Bull TCL Service Desk, through their Supervisor.

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

- 4.4.3 Bull TCL is responsible for the back-up and required recovery arrangements of all information held on drives and systems secured on the Councils networks.
- 4.4.4 Users should only use network drives to store information, particularly when using desktop applications such as Word or Excel. Any information held on local storage hard drives or local servers not administered by Bull TCL or the Information Services Division will not be backed up by Bull TCL. Information lost that is not stored on network drivers is likely to be irrecoverable.

### 4.5 Network Security

- 4.5.1 To safeguard the telecommunications network and information transmitted across it:-
- No equipment will be connected to the telecommunications network before an impact assessment has been carried out by Bull TCL. The assessment will confirm that the equipment conforms with appropriate IT security standards.
  - Secure network connection methods will be deployed for remote connection of Users such as Virtual Private Networks (VPN) and Remote Secure Access (RSA) authentication. Firewalls will be provided and managed by Bull TCL.
  - Connections to the Internet and e-mail systems must be authorised by the appropriate Supervisor and will be made available through one of the secure methods provided by Bull TCL. Use of the e-mail, Internet and Intranet must be in accordance with sections 2 and 3 of this Protocol.
  - Authentication equipment (e.g. RSA tokens), which facilitates access to the network and / or specific information systems will be issued and managed by Bull TCL and only used by the User to which it has been allocated and in accordance with instructions provided by Bull TCL.

### 4.6 Disposal of Computer Equipment (including all mobile devices / mobile telephones etc.)

- 4.6.1 All computer equipment must be disposed of by Bull TCL, this will normally be undertaken as part of the technical refresh arrangements.
- 4.6.2 Where special arrangements are required for the disposal or return of equipment, (such as when an employee leaves their role with the Council and a replacement is not to be recruited) the Supervisor should contact the Bull TCL Service Desk.

## 5. Mis-Use of Computer Equipment and Information Systems

- 5.1 The Council views any misuse of its computer systems or equipment very seriously. The following actions (or inactions) by Users could constitute misuse and a breach of this Policy.
- 5.2 Mis-Use by any User includes:
- an attempt to access or actually access and / or use of any Council computer system without authorisation from their Supervisor
  - Revealing any information (by whatever means) from any computer system(s) to

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

- any unauthorised person or organisation
- Misuse of any Council computer system that they are authorised to use. – Misuse will include (but not necessarily limited to) using the system or the information held within the system:
  - for other than its intended purpose,
  - other than in the authorised manner, or
  - for personal gain
- Introducing onto any Council computer system any unauthorised information illegally (as this will infringe licence arrangements)
- loading any software (including screensavers) from whatever source onto Council IT equipment or the network. Where there is a business need to load any such software, this must be undertaken through Bull TCL.
- copying any Council software or data onto a non-Council computer or device
- The use of any computer desktop background / wallpapers, other than those approved by the Council, or those which form part of the standard operating system. (The reason for this is to prevent permanent burning of images onto screens)
- Failure to exercise due care in the use of Council computer equipment, systems which may / does result in the loss of restricted information or damage to the reputation of the Council / school for breach of confidentiality.
- Using, CD's / DVD's or any other removable mobile storage device for the storage of restricted personal or or confidential data which is not encrypted.
- Using memory sticks other than to save and transport presentations such as Microsoft Powerpoint

### Mis-use by a Supervisor includes

- Inducing any person to carry out any of the above actions
- knowingly allow or condone :-
  - any other User to undertake any of the above actions
  - allow any User to induce another User to undertake any of the above actions

# THE INFORMATION SECURITY AND COMPUTER USAGE POLICY

## PROTOCOL ON THE MONITORING AND CONTROL

### 1. Introduction

This Protocol sets out the arrangements for the control and monitoring of the implementation and compliance with of this Policy

### 2. Monitoring and Control of Compliance

- 2.1 Information governance is part of the overall governance and risk management arrangements for the Council / school; information security is a key component of information governance.

The Executive Director, Assistant Director and School Governor, are accountable through their annual statements for providing assurance that the provisions of this Policy are operated effectively within their service.

Increasingly there is a dependence on Executive Directors, Assistant Directors and School Governors to ensure that they have a clear understanding of Information Security risk, how these relate to key business functions and how, through the application of this Policy these risks can be managed.

- 2.2 The Assistant Chief Executive (Information Services) has a responsibility for working in collaboration with Executive Directors, Assistant Directors and Schools Governors to ensure that this Policy is revised on a regular basis, and the provision of advice and guidance on the practical application of it within their area of responsibility.

The Assistant Chief Executive (Information Services) will prepare an annual information risk assessment based upon

- o the annual statements of the Executive Directors, Assistant Directors and School Governors,
- o the findings of compliance audits commissioned from time to time, and
- o the findings arising from any investigations into reported potential or actual breaches of this Policy.

Arising from this assessment an annual plan for any identified improvements in the management of information risks will be prepared by the Assistant Chief Executive (Information Services), in consultation with SMT, and the Assistant Director of Finance (Audit and Risk Management)

The communication of all agreed changes will the responsibility of those with specific roles set out in the Protocol as to Roles and Responsibilities.

- 2.3 The Assistant Chief Executive (Information Services) and the Assistant Director of Finance (Audit and Risk Management) have the authority to commission or conduct periodic audits of compliance with this Policy.

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

- 2.4** The Assistant Chief Executive (Information Services) shall report to the Audit Committee of the Council at least on an annual basis, and further if so required.
- 2.5** The Council has authorised the reporting on all aspects of information, computer systems, Internet, e-mail or telephone calls usage and the recording of usage of computer systems, e-mail and the Internet, without the consent of either the Users or any other party to a transaction or communication. This is always undertaken where this is lawful under the Telecommunications (Lawful Business Practice ) (Interception of Communications) Regulations 2000, published under the Regulation of Investigatory Powers Act 2000, and where this is lawful under the Data Protection Act, and in accordance with this Policy.
- 2.6** Detailed personal analysis of Internet or e-mail usage will only take place where:-
- a concern arises from a service audit report or investigation;
  - general usage reports indicate an area of concern requiring further detailed investigation,;
  - where there is a suspicion / allegation of inappropriate usage raised by the Supervisor; or
  - where a concern is raised under the Whistle-blowing Policy of the Council.

# THE INFORMATION SECURITY AND COMPUTER USAGE POLICY

## PROTOCOL ON PROCEDURES RELATING TO MOBILE TELEPHONES

### 1. Introduction

- 1.1 This Protocol sets out the procedure for providing and managing the use of mobile telephones in relation to Council, school and employee-owned mobile telephones

### 2. Criteria

- 2.1 The following factors should be considered when determining whether a User should be provided with a Council / School owned mobile telephone:
- Whether the provision of / access to existing 'land phones' is adequate to meet the role of the User. This is especially significant given the high cost of mobile telephone calls.
  - The need to receive calls in an emergency.
  - The need to make calls outside of working hours or in an emergency.
  - The frequency of occurrence i.e. the above features must be a regular part of the Users role.

### 3. Procedures

#### 3.1 Administration

- Where the above criteria are satisfied, authorisation must be obtained from the Supervisor.
- The requirement for the User to have a mobile telephone should be reviewed at least on an annual basis
- The model of mobile telephone to be purchased must be appropriate for use and without excessive functionality.
- The Users must be informed that the mobile telephone is issued primarily for Council use.

#### 3.2 Purchasing

- The purchase of a Council owned mobile telephone must be made via the Bull TCL Service Desk. Schools will make their own arrangements for purchases in accordance with the Authority's Financial Regulations.
- The Supervisor will be required to communicate and authorise the purchase of the mobile telephone to the Bull Service desk setting out briefly the nature of the work involved anticipated frequency of use and the expenditure code to be charged.
- Advice will be provided by the Bull TCL Service desk with regard to tariffs, model and other options based upon the information provided.
- All mobile telephone invoices received from suppliers must include an itemised call statement.

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

### 3.3 Rental / Call Charges

- The Council / school is responsible for the payment of rental charges, i.e. all rental expenses and any special payments for emergency maintenance.
- The Supervisor of authorised Users should check and arrange to pay the invoice by the EBP system. The invoice should be checked for private call usage
- Payment for private usage is required from the User. (see section on Payment of Private Telephone Calls).
- Head teachers should arrange payments in accordance with the agreed school financial procedure.

### 4. 4.1 Use of the Telephone whilst driving

4.1.1 The use of hand-held mobile telephones (whether it is User/Council or school provided) whilst driving is strictly prohibited in accordance with the Road Vehicles (Construction and Use) (Amendment) (No 4) Regulations 2003. Whilst the use of hands-free kits is not presently unlawful, drivers who become distracted by the use of such kits may face prosecution for not having proper control of the vehicle.

4.1.2 It is strongly recommended that on Health and Safety grounds Users do not use hands free equipment whilst driving during working hours. This includes periods of time whilst waiting in stationary traffic and applies to both phones supplied by the Council / schools and privately owned telephones.

4.1.3 This Protocol should be read in conjunction with the Health and Safety Codes of Practice which can be found on the Health and Safety Website. All Users who are required to drive a Council / school-provided vehicle as part of their role are issued with The Drivers Handbook, which they should refer to as appropriate.

### 5. **Payment of Private Telephone Calls**

5.1 Users **must** pay for all private telephone calls and messages made using Council / school owned mobile telephones

5.2 All private calls should be recorded by highlighting on the itemised invoice and paid for at the charged tariff rate, for the private use of the mobile telephone or recorded on the Record of Private Use of Council, School and Employee-owned Mobile Telephones RCM1 form.

Non-school employees

5.3 Employees should pay for their personal phone calls on a quarterly basis (March, June, September and December) by credit or debit card via an e-Form on the BMBC Intranet. This can be accessed via the home page on the BMBC Intranet site.

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

- 5.4 Payments by credit card will attract an additional fee that employees will stand the cost of. The fee is a percentage of the total cost of the calls and will be calculated as the payment is made.
- 5.5 The system will prompt the employee through the necessary stages to make the payment. Employees should have their debit or credit card ready to enter their details.
- 5.6 Employees should print a receipt and attach it to their record of private use of telephone call RS1 form.
- 5.7 Employees who do not have access to the Intranet should arrange access to make payment via their Supervisor.

### School Based Employees

- 5.8 Payments should be made in accordance with the agreed School Financial Procedure.

## **6. Business Calls made using Privately-owned Mobile Telephones**

- 6.1 In cases where a User utilises a privately owned mobile telephone to make a business call, the cost of the call can be reclaimed using the **Claim for Expenses CE1 form**. A copy of the mobile telephone bill should be attached.
- 6.2 In cases where the Users have a 'Pay as you go' arrangement, a log should be maintained of the calls made, detailing times of the call made and the tariff rates.

## **7.. Return / Disposal of Mobile Telephones**

- 7.1 Supervisors must ensure that mobile telephones are recovered from Users who are leaving their role with the Council / school, and should ensure that the inventory is updated.
- 7.2 Any debts outstanding in respect of private telephone calls must be paid prior to the User leaving their role.
- 7.3 Supervisors should consider if any replacement User is to be issued with a mobile telephone in the short term, or whether it will be more cost effective to suspend / cancel the telephone contract.
- 7.4 Any mobile telephones which are to be replaced or taken out of service should be disposed of through Bull TCL, who will make appropriate arrangements for the disposal of the equipment.

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

# THE INFORMATION SECURITY AND COMPUTER USAGE POLICY

## PROTOCOL FOR DATA HANDLING REQUIREMENTS FOR SUPPLIERS

### 1. Application of this Protocol

This Protocol sets out the minimum requirements required of all suppliers, contractors, partners or other organisation (Referred to collectively as Suppliers) that have access to information for which the Council is responsible.

Access to information can be either direct access through the use of information in order to undertake their contracted role with the Council OR Information which the Supplier may have access to indirectly through for example the maintenance of information systems on behalf of the Council.

### 2. Contractual Arrangements

2.1 The Office of Government Commerce (OGC) has provided a Procurement Policy Note (Information Note 08/08 – 1 July 2008) which provides guidance on the adoption of model contract clauses and provisions relating to the security and information assurance in contracts. The following issues are included in this regard:-

- Vetting of contractor personnel having access to information
- Provision of access to Authority Data
- Protection of Personal Data
- Freedom of Information
- Confidentiality
- Security Requirements
- Warranties
- Secure Requirements
- Standards
- Quality Assurance and Performance Monitoring
- Audits
- Business Continuity and Disaster Recovery
- Commercially sensitive Information
- Exit Management

2.2. All new contracts for the provision of services to the Council by any Supplier must include appropriate clauses and provisions to safeguard data handling arrangements where the supplier will have direct or indirect access to information which have a value other than non-restricted.

2.3 Where contractual arrangements are already in place and consequently services cannot require suppliers over which they have no direct control to accept such additional clauses, services required to use all appropriate influence to encourage them to accept such changes.

### 3. Data Handling requirements for Suppliers

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

- 3.1 Supervisors should ensure that, in all partnership and supplier contractual arrangements, it is determined at the outset who is responsible for the information and therefore who the 'owner' and responsible person, irrespective of who is allowed to have access, handle and process information.
- 3.2 Services should ascertain in writing that Suppliers have the following processes in place to manage information risk:-
- An information risk policy must exist, setting out how measures are implemented and how compliance and effectiveness of the policy is monitored.
  - A risk assessment of the confidentiality, integrity and availability of information must be carried out at least quarterly
  - Information which is designated with a value to be either restricted or higher and which is held on paper must be locked away when not in use, or the premises on which it is held must be secured.
  - In all cases remote computers should be password protected, configured so that functionality is minimised to its intended business use only, and have up to date software patches and anti-virus software.
  - All material that has been used for restricted or above should be subject to controlled disposal
  - No unencrypted laptops or drives or removable electronic media containing personal data should be taken outside secured office premises
  - No transferring of any restricted or personal data from Council or Council approved information systems to third party owned laptops, PC's USB Keys, external drives and any other removable media is permitted.
- 3.3 Where it is ascertained that the Supplier is not already complying with the above requirements the service is required to give notice to the Supplier that they must make arrangements to do so immediately. In such cases this includes:-
- No unencrypted laptops or drives or removable electronic media containing personal data should be taken outside secured office premises until further notice
  - Where such laptops or drives or any other removable electronic media containing restricted or personal data are currently outside secured premises, to make arrangement for them to be returned to secure premises within 24 hours.
  - Laptops and drives or any other removable / portable electronic media containing protected personal data to be held in locked cabinets or drawers when not in use.
- 3.4 The Supplier should be reminded that where it is specified in Council contracts, the Council shall be entitled at any time and without giving notice to the Supplier, carry out tests as it may deem necessary to ensure compliance with these criteria, including auditing internal security policy and procedures and interviewing staff engaged on Council work.
- 3.5 In addition to the above, the Supplier should be required to provide a copy of their data security policy.

#### **4. Remote Access to Information Systems**

This Policy and Protocols relating to it are reviewed on a regular basis to take account of developments in technology, in the light of practical experience, changes in legislation and developing best practice. It was last revised in December 2008, copyright Barnsley MBC.

- 4.1 Where the nature of the work undertaken on behalf of the Council requires Suppliers to have remote access to information systems of the Council (e.g. supplier of software maintenance and support), the supplier must sign and comply with a Virtual Private Network (VPN) access agreement before any form of access will be permitted.