FRAUD AND CORRUPTION POLICY

This booklet contains two sections covering the following areas:

- Fraud and Corruption Policy; and
- Information and Communications Technology Policy.

Further advice or guidance on these policies may be obtained from Internal Audit or IT Services, respectively.

This booklet updates the Council's Fraud and Corruption Policy issued in 2000.

FRAUD AND CORRUPTION POLICY

1 INTRODUCTION

1.1 The term “Corporate Governance” came into common use in the United Kingdom in the company context following the publication of the Cadbury Report in 1992. Cadbury defined corporate governance as “the system by which organisations are directed and controlled”. In 1995, CIPFA issued a comprehensive document “Corporate Governance: A Framework for Public Service Bodies”. There followed a series of specific initiatives culminating in the CIPFA/SOLACE guidance “Corporate Governance in Local Government – A Keystone for Community Governance”.

1.2 Corporate Governance is the system by which Local Authorities direct and control their functions and relate to their communities. Good corporate governance underpins credibility and confidence in our services and the principles encourage openness, integrity and transparency. These principles provide the framework for the Council’s approach to fraud and corruption.

1.3 Bracknell Forest Borough Council seeks to provide value for money services to the public whilst encouraging openness and integrity. This requires that all practical steps are taken to minimise the risk of fraud and corruption either by staff, Members or customers. Fraud is the illicit gaining of cash or any other benefit by deception; corruption is the dishonest influencing of action and decisions. This policy outlines the Council position on Fraud and Corruption and details how it is to be dealt with.

1.4 The Borough Finance Officer will ensure that a continuous Internal Audit is carried out within the Authority to evaluate the Council’s systems of control. The Council’s External Auditors are responsible for reviewing the Council’s arrangements for dealing with fraud and report accordingly to the Borough Finance Officer. It remains, however, the responsibility of all managers to ensure that there are adequate controls in place within the systems for which they are responsible; the Council expects that good practice will be followed at all times.

1.5 Controls will be aimed at:

- Deterring,
- Preventing, and
- Detecting

all forms of fraud and corruption.

1.6 In addition, the Council expects all its suppliers, contractors, agents, partner organisations and individuals to act with honesty and integrity. It further expects its Members and staff to lead by example by working within the Council’s framework of guidance i.e. Code of Conduct for Employees, Member/Officer Protocol, Financial and Contract Regulations. Copies of these policies may be obtained from Corporate Personnel and Finance, respectively.

1.7 All cases of fraud will be treated equally regardless of the perpetrator. The Police will be informed if appropriate and disciplinary action will be taken against Members and staff in accordance with the relevant Disciplinary code.

2 GENERAL APPROACH OF THE COUNCIL

2.1 It is the Council's aim to create an atmosphere of honesty and openness and has agreed a Whistleblowing Policy to support that aim. Copies of the policy may be obtained from Corporate Personnel. The Council wishes to encourage all citizens and customers of its services to report any suspicions and concerns they may have about any aspect of the Council's work. This can be done by speaking to either:

- Their Ward Councillor; or
- The Council's Chief Executive; or
- The relevant Service Director.

Staff may notify their concerns to:

- Their Line manager; or
- Their Director; or
- The Director of Corporate Services; or
- The Head of Audit; or
- The Borough Solicitor; or
- The Borough Finance Officer; or
- The Council's External Auditors.

2.2 The Council will ensure that complete anonymity and confidentiality is maintained at all times; all information received will be treated with respect and given appropriate care and consideration. Likewise, where sufficient information is given, anonymous phone calls, letters etc will be seriously investigated. The Public Interest Disclosure Act 1998, means that employees are able to report any suspected cases of fraud or corruption to the Council without fear of reprisal. Alternatively, the Act allows contact to be made with the Audit Commission directly. Leaflets produced by the Audit Commission outlining how the Public Interest Disclosure Act protects the Council and its staff have already been circulated to all Council staff which provide clear guidance on what to do should fraud or corruption be suspected.

2.3 Appropriate investigations will be made and if evidence reveals that there may be fraud or corruption taking place, the Council's Internal Audit section (if not already involved) will be informed. They will then conduct any further investigations necessary and will be responsible for informing and liasing with the Police as outlined in Financial Regulation 17.

3 STAFF

3.1 The Council views its staff as its most important resource. Particular importance is attached to the recruitment process to ensure the best calibre of staff are appointed for each position. Appointment panels will obtain candidate references to verify their suitability, honesty and integrity and agencies used to supply staff will be asked to provide appropriate references.

3.2 All staff employed will be bound by the Council's Code of Conduct for Employees. This code specifically covers the receipt of gifts and declaration of hospitality. Staff who are members of professional bodies will also be expected to abide by any codes of conduct issued by those bodies.

3.3 The Disciplinary Procedure operated by the Council will be used to instigate and progress actions against staff involved in perpetrating fraud. The Procedure will be used regardless of whether the Police have been involved and/or any legal proceedings are being taken against the member of staff.

3.4 Training is recognised as essential for the successful detection, investigation and prevention of fraud. Adequate financial resources will be provided to enable staff to attend training courses and seminars in order to remain conversant with current developments and initiatives.

4 MEMBERS

4.1 As elected representatives of the public, all Council Members have a duty to be fair, honest and open in their role. They are legally bound by:

- Government legislation; and
- The National Code of Local Government Conduct.

4.2 In addition the following internal policies outline best practice:

- Council Standing Orders and Financial Regulations; and
- Locally adopted codes of conduct e.g. Member/Officer protocol.

4.3 In particular, Members are required to declare and register any pecuniary interests they may have in companies, charitable organisations, voluntary groups or other organisations and then abstain from any debate or vote which pertains to those organisations.

5 SYSTEMS

5.1 In order to safeguard against fraud and corruption, the Council defines its operational methods by its Standing Orders, Contract and Financial Regulations. These stipulate the way in which meetings are run and resolutions made, how value for money is to be achieved and the controls necessary for ensuring the Council's finances are administered in a correct and proper manner.

5.2 The Borough Finance Officer, as the Section 151 Officer, has a statutory duty to ensure that proper arrangements are made to administer the Council's finances. The Council therefore supports and takes the advice offered by the Borough Finance Officer on changes to the systems of control, finance and administration and their associated rules and regulations. Support is provided in this by the Internal Audit Service. Their planned work will take into account all factors affecting control systems (including known and perceived risks) and the adequacy of existing controls. Audit plans will be regularly reviewed and revised to take account of new developments.

5.3 Controls are designed to identify, prevent or deter and limit the extent of fraud. Adequate segregation of duties is of fundamental importance to this. Weaknesses in internal or other controls identified by Internal or External Audit will be reported by the Borough Finance Officer, to the relevant Service Director and the applicable manager.

6 INVESTIGATION AND DETECTION

6.1 The Council recognises that even the best controls may not prevent fraud. It therefore requires that any cases of suspected fraud or irregularity are reported to the Borough Finance Officer immediately as specified in Financial Regulations.

6.2 The Director of Social Services and Housing has responsibility for administering Housing and Council Tax Benefits. Support is provided by specialist resources to investigate any claims which are suspected of being fraudulent or containing material untruths. Should investigations reveal wider aspects and/or Council staff are implicated then the matter will be reported to the Borough Finance Officer for further action.

6.3 Given the importance of communication with other Local Authorities, Council officers will be encouraged to join appropriate local and professional groups useful for generating debate and supplying solutions to problems and for passing and receiving of information. This includes participation in the Audit Commission's National Fraud Initiative. Similarly, liaison with Government Departments and Agencies will also be encouraged.

6.4 Each Council section which has a responsibility for preventing and detecting fraud and corruption will construct its own operating systems for the implementation of this Policy.

7 EXCHANGE OF INFORMATION

7.1 The Data Protection Act 1998 allows that personal data processed for any of the purposes outlined below are exempt from non disclosure provisions:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of any tax or duty or of any imposition of a similar nature.

7.2 Personal data is any data which would enable a person to be identified from the information provided. This is a far reaching provision as it includes opinions about an individual and any information about what is intended to happen to them. If personal data is to be disclosed for the reasons detailed above, only the minimum amount of data to satisfy the purpose will be disclosed. The Council recognises that this is particularly important where a significant amount of data is held about the person concerned. The disclosure of data can be either internal within the Council or to an external third party. Questions about the interpretation of this paragraph should be addressed in the first instance to the Council's Data Protection Officer and the Borough Solicitor.

8 PROSECUTION POLICY

8.1 The Council will investigate all fraud committed against the Authority by individuals and/or organisations. Investigations will be carried out with due diligence and within the legislative framework governing actions by individuals involved in the investigation of crime and/or offences.

8.2 Where suspicion of fraud exists, early consultation will take place with the Police. This does not necessarily mean that a Police investigation will be pursued but where sufficient evidence of fraud exists the Borough Finance Officer will make a formal statement to initiate a Police investigation.

8.3 Whilst the Council acknowledges that the Crown Prosecution Service make the ultimate decision on whether to proceed with a prosecution, the Police will be involved in all appropriate cases and prosecution sought if there is sufficient evidence.

9 CONCLUSION

9.1 The Council's systems of control will be maintained and regularly reviewed. Managers are charged with ensuring controls are maintained which are sufficient to detect and prevent fraud. The Borough Finance Officer is responsible for ensuring that systems and controls are audited and the Council will ensure that every possible support is given to maintain an environment which makes fraud and corruption difficult to perpetrate.

Information & Communications Technology Policy

ICT Policy

1. Introduction

1.1 The Council is committed to maintaining its stance against computer fraud and abuse and is working towards adopting a British Standard (BS7799) - 'Information Security Management' code of practice. This best practice policy is designed to assist all staff to meet their statutory and other obligations and apply to:

- All employees working for the Council, including working from home or at non-Council locations
- Other persons e.g. Elected Members, Consultants, Contractors working for the Council, external organisations working with the Council, whilst engaged on Council business or using Council equipment and networks
- Any personal use by employees that identify the person as a Council employee and which may bring the Council into disrepute

1.2 It is your responsibility as an employee, contractor or councillor to adhere to this policy.

1.3 Adherence to this policy is a condition for using Council equipment and networks.

1.4 Abuse of the ICT systems or failure to act in accordance with this policy will be regarded as a disciplinary offence.

1.5 Any reference in this policy to 'unauthorised software' refers to importing into or exporting from The Council any unauthorised software (system software, applications, data, screen savers etc) to/from any media (Internet, e-mail, CD, hard disk, floppy disk etc).

1.6 Section 2 below identifies the key points of this policy which you must adhere to. These points are explained in detail in Sections 3 – 16.

2. Policy highlights

2.1 As an ICT user of the Council you must:

- Adhere to the guidelines specified in this document
- Use electronic messaging systems responsibly and legally
    - Use the facilities for Council business – keep personal use to a minimum and ensure you have your manager's permission
    - For the purposes of privacy and security treat electronic communications and information as if it were paper based

- Only use the ‘all user’ distribution list if the information is extremely important and with your manager’s permission

- Log out of screens when leaving your desk unattended

- Comply with password procedures

- Report any suspicious e-mails to the Head of Audit

- Virus scan all downloaded data and software before use

- Immediately report the receipt of any offensive e-mail to the IT Help Desk

- Abide by the principles of the Data Protection Act (1984 & 1998)

- Take regular backups of your own data stored on your local hard disc (C: drive)

- Pay for personal calls on supplied mobile telephones

2.2 You must not:

- Relocate equipment without the prior knowledge and approval of ICT Services

- Leave laptops/mobile telephones unattended

- Use any unauthorised software products

- Create unauthorised databases

- Try to access, distribute or use offensive or illegal material on the Internet

2.3 The Council will:

- Regard abuse of ICT systems or failure to act in accordance with the policy as a disciplinary offence

- Via Internal Audit monitor the use made of the internet to check that misuse is not taking place

- Remove any unauthorised software found on it’s equipment and take disciplinary action where appropriate

- **As part of its Internal Fraud and Corruption Policy, reserve the right to retrieve and access e-mails or faxes at any time, without the permission of the employee and without notice**

- Inform the Police if illegal material is accessed

- Ensure that backup copies of departmental, network and mainframe systems are taken regularly by ICT Services

If in doubt – Contact the IT Help Desk on 01344-351100

3. Policy for using electronic messaging systems, including the Internet

Acceptable and unacceptable usage

3.1 Information and knowledge, the way it is received, how it is used, shared and disseminated, is vital to the effective operation of the Council. Such information and knowledge is a valuable asset and requires security and an effective vehicle to transmit both internally and externally. The guiding principle is that, despite its immediacy and ease of distribution, for the purposes of privacy and security, electronic communication and information should be treated no differently from that on paper. Users should be aware that all e-mails sent or received, internal or external, whether or not marked 'private', using the Council's equipment or systems are the property of the Council and as such must reflect the standards and policies of the Council.

3.2 Electronic messaging systems e.g. electronic mail, Internet, Intranet, faxes must be used responsibly and legally. Users must not misuse them by taking any action that could bring the Council into disrepute, cause offence, interfere with the Council's work or jeopardise the security of data, networks, equipment or software. The data protection principles embodied in the Data Protection Acts (1984 & 1998) must be observed (see section 12). (Also see Section 15, Consequences of Misuse of E-mail).

3.3 All ICT facilities should be used for Council business. However, as part of the Council's wish to encourage staff to explore such facilities in a constructive manner, occasional personal use is permitted. This is subject to the discretion of managers and providing it does not interfere with the Council's work, conforms to this policy and is not associated with personal business interests. (See Section 10 for further guidance on personal use)

3.4 ICT Services provides and supports the Groupware office systems product called Novell GroupWise. GroupWise will allow you to:

- send and receive e-mails across the Internet
- send and receive e-mails internally with other GroupWise users
- send faxes (if enabled) direct from your PC (Word, Excel and PowerPoint documents only)
- make appointments and enter tasks in an electronic diary system

3.5 Full Internet access is provided where it supports Council goals and can be made available on production of a business case and receipt of a completed application form that has been certified by the appropriate Director (or a designated senior manager). However, for users without full Internet access many Internet sites are available via BFNet, the Council's Intranet. The Council logs all activity and monitors Internet use. Suspected misuse will be subject to investigation and may result in disciplinary action, including verbal or written warnings or, in cases of gross misconduct, termination of employment. Incidental personal use is not prohibited, but should be kept to a minimum.

Examples of inappropriate and unacceptable use are:

- Releasing Council information to unauthorised individuals, inside or outside the Council.
- Sending, forwarding, browsing, exporting from, or importing into the Council or storing on Council equipment or systems, any materials that are or could be, in any manner whatsoever, considered to be pornographic, obscene, profane, offensive (whether from a sexual, racial, political, religious, or any other perspective), libellous, slanderous, defamatory, illegal or of a criminal or subversive nature.
- Sending e-mails that may be interpreted as sexual harassment. E-mails are an increasingly common ingredient in workplace sexual harassment cases where innuendoes are taken as intimidating, hostile or humiliating by the recipient.
- Transmission of unsolicited commercial or advertising material
- Violating other people's privacy
- Using chat lines or similar services
- Playing games (see Section 10)
- Disrupting other users' work in any way, including the introduction of viruses or by data corruption
- Committing the Council to purchase or acquire goods or services without proper authorisation
- Downloading unauthorised software (see Section 6)
- Any use that could bring the Council's name into disrepute or that could be damaging to the Council.

3.6 Junk mail (also known as "spam") is a hazard of Internet life. Staff posting to newsgroups should be aware that "spammers" get their mailing lists from newsgroup subscribers. Anyone receiving excessive junk mail should consult ICT Services about the use of mail filters and other ways of blocking unwanted correspondence.

Access and privacy

3.7 The Council provides e-mail and desktop faxing systems to facilitate communication and the sharing of information among its employees and external business and community partners. This system is the property of the Council and is intended for Council sanctioned use only. Whilst the Council does not routinely access or monitor individual mailboxes, there may be instances (i.e. legal, regulatory, security or business reasons) that require e-mails or faxes to be retrieved by the Council, its authorised agents, or legal/regulatory agencies.

3.8 The Council, as part of its Fraud and Corruption Policy, reserves the right to retrieve and access all e-mails or faxes, whether or not they have been marked confidential, at any time, without the permission of the employee or Member, and without notice. Further, once a message or fax has been sent, recipients may intentionally or accidentally forward the information to other individuals (contrary to the Data Protection Act). Therefore, users should have no expectation that any electronic information will remain private.

3.9 All e-mails received from and sent to external sources are scanned for the presence of viruses, video/music clips, executable (.exe) files and profanities. Virus infected files are cleaned by the system, if cleaning is not possible the e-mail will be deleted, the system will also delete any video/music clips, executable files and profanities found.

Email best practice

3.10 Users should note that there are a number of considerations to be considered when sending e-mails across the Internet:

- Internet mail uses SMTP (Simple Mail Transport Protocol), which means that unless you have access to strong encryption technology, messages should not be considered as secure.
- Verify with e-mail recipients that they can receive the type of mail attachments you are sending (such as word processing, spreadsheet or program files) or else they may not be able to be read by the recipient and have therefore been a waste of resources.
- Be aware that you could inadvertently breach the Data Protection Act 1998 if you send external email to groups of people (i.e. mailing lists) without hiding the individuals' email addresses. Remember that any distribution list publishes the names of all the people to whom the message is sent, so you could be disclosing a personal email address to a third party without their permission. A person's email address is classified as personal data under the Act. To avoid any possible breach of the Data Protection Act, follow the Council's Email Best Practice and Guidance and The Essential Employee Guide to Handling Personal Information that can be found on BFNet.
- E-mail, whether via Novell GroupWise or the Internet/Intranet, should be regarded as public and permanent. It is never completely confidential or secure and, despite its apparent temporary nature, it can be stored, re-sent and distributed to large numbers of people. If in doubt use methods other than e-mail to send sensitive information.

- Employees should be particularly careful about what they commit to e-mail. It can be used as evidence in industrial tribunals and formal enquiries, including internal disciplinary and grievance hearings, and senders may leave themselves and the Council open to charges of libel and slander.
- E-mail must not be used to harass employees or other recipients. Harassment can take the form of argumentative or insulting messages ("flame mail") or any other message the sender knows, or ought to know, would cause distress to the recipient.
- E-mail must not be used to make derogatory remarks about another person or company. Remember that although you may delete such a message it may be saved or circulated by the recipient(s).
- Staff should not re-send e-mail chain letters and should use caution with any e-mail that asks the reader to forward it to others. Seek your manager's advice if in doubt.

3.11 Users should be aware that, as with paper sources, not all information on the Internet is accurate, complete or reliable. Users should ensure its validity, as they would print publications, before using it.

Relevant legislation

3.12 The use of personal data in newsgroups or web sites is subject to the Data Protection Act (see Section 12) and users should seek the advice of the Data Protection Officer if in doubt.

3.13 Using the Internet to attempt to access any Council or third party IT facility for which the user does not have authority is an offence under the Computer Misuse Act.

3.14 Using the Internet/Intranet to download (see Section 6) or otherwise copy copyrighted software; information or other material without adhering to its licensing conditions is an offence under the Designs, Copyright and Patents Act.

4 Security

4.1 It is mandatory that all users protect their GroupWise accounts by setting a password in accordance with the procedure set out in 4.3.

4.2 It is good practice to log out of screens when leaving your desk unattended. This is to ensure confidential information remains confidential to the authorised user. In no circumstances should confidential data be divulged to anyone.

4.3 Passwords provide the principal means of validating a user's authority to access a computer service. All users should adopt the following procedures:

- allocate individual passwords to maintain accountability
- keep passwords confidential
- avoid keeping a paper record of passwords
- change passwords regularly, and whenever there is any indication of possible compromise

- select a password with a minimum length of six characters
- avoid basing passwords on any of the following: months of the year, days of the week, family names, car registration numbers, company names, birth dates etc. Such passwords are easy to guess and may lead to unauthorised access

4.4 The Council protects its networked systems (by virus scanning measures) down to the server level. All connections to the Internet, with the exception of those covered in the following paragraph, must be via the Council's network and its security protection ("firewall") to ensure that maximum control and protection is achieved. Under no circumstances must users set themselves up with their own ISP (Internet Service Provider, e.g. CompuServe, AOL etc.) on Council equipment.

4.5 In exceptional circumstances, a department can install a stand-alone device with its own Internet connection. The Borough IT Services Manager, who will maintain a register of such connections for audit purposes, must approve this. In these cases the department manager is responsible for ensuring that:

- the connection and associated equipment adhere to the security and access standards defined by the policy guidelines
- all users sign the appropriate declaration
- all access is tightly controlled
- usage is monitored

4.6 Appropriate firewall and network monitoring facilities will be deployed to protect the Council networks as determined by the Borough IT Services Manager.

4.7 Where practical, known offensive sites will be barred to prevent access from Council networks.

4.8 The declaration signed by full Internet IT users will be modified to reflect this policy. Users of stand-alone Internet PCs must sign a further declaration. Declarations will be filed in an individual's ICT Services file.

4.9 Files and e-mail attachments can transfer viruses, thus threatening the security of Council networks. A mail scanner is in place to minimise the risks from virus infection.

5 ICT asset management

5.1. IT Services maintain the Council's inventory of all hardware and software. Each asset is clearly identified for the purposes of:

- security protection
- insurance
- financial asset management
- health and safety
- equipment maintenance
- software licensing

5.2 No equipment is to be relocated without prior knowledge and approval of IT Services.

6. Downloading software

6.1 Although all e-mails received through the Council's network are virus checked, files downloaded from the Internet (or 'uploaded' from CDs or diskettes) are not. Therefore all downloaded software must be virus scanned before being used or moved to another device (see Security above).

6.2 All licensing requirements, payment conditions and deletion dates associated with downloaded software must be met. Anyone acquiring software must be aware of the differences between: ''copyrighted software''- requires a license payment; 'free ware' – licensed but requires no payment; 'shareware' – copyrighted but often free for a trial period and 'public domain software' which is free. If in doubt, contact the Borough IT Services Manager.

6.3 When downloading software or other information directly from the Internet, please observe the following points:

- Software may be acquired or downloaded only under arrangements authorised by the Borough IT Services Manager. Always verify licensing, copyright obligations and Council policy before downloading software or data (including screensavers etc) onto Council systems. All hardware and software is procured centrally and the Help Desk hold all licensing details on the asset register which is subject to regular audits.

- Scan all executable code (programs, applications etc) and documents imported directly from the Internet, or brought in on floppy disk or CD, for the presence of computer viruses by use of the McAfee Virus Toolkit loaded on your PC. If you do not know how to use this software, contact the IT Help Desk.

- Do not download games or leisure software.

- Follow all laws and regulations (e.g. The Computer Misuse Act, Designs, Copyright and Patents Act) governing the import and export of technology, software and data.

7. Database development

7.1 The Microsoft Database Access application is available to many users who need the product in order to access data developed within the Council. Any requirement for a new database must be made through Corporate IT Services or Social Services, Education, Environment departments local IT teams as appropriate.

7.2 Under no circumstances should users set up a new Microsoft Access database (or install from any external source) without the express permission of ICT Services. Such installations may lead to virus problems, omission from the asset registration and possible licensing issues as well as the obvious problems of lack of support and documentation.

8. Offensive and illegal material

8.1 Offensive material is anything that is pornographic; involves threats or violence; promotes illegal acts, racial or religious hatred or discrimination of any kind. It also covers material that the person knows, or ought to know, would offend a colleague with particular sensitivities.

8.2 **The Internet contains far more useful information than it does offensive material. However, offensive material does exist and any member or employee using Council facilities for such material will face disciplinary action. If illegal material is accessed, the Council will inform the Police and criminal prosecution may follow.**

8.3 People receiving offensive or sexually explicit mail should inform their manager, the Council's Internal Audit Section and the IT Help Desk immediately. Such material may not be identifiable until an e-mail is opened and in these cases staff will not be held responsible providing they report it immediately.

8.4 Newsgroup messages often link to web pages and staff should be aware of the risk of accessing inappropriate sites. Any one accidentally accessing offensive material should inform their manager and the IT Help Desk immediately. Accidental access will not result in disciplinary action but failure to report it may do so.

8.5 Staff who have to monitor offensive material as part of their jobs, e.g. child protection, equal opportunities and trading standards, may access relevant material with their departments manager's permission. Permission must only be given to named individuals and a record placed in their personal files. Each site visit must be recorded in a log, which identifies the site and the date and time of the visit. The manager must review the log regularly.

9. Monitoring

9.1 **The Council will monitor the use made of the Internet and may inspect the contents of electronic mail and files. Users should not expect them to be private.** The Council's Internal Audit Section in conjunction with the Borough IT Services Manager to ensure that misuse is not taking place will carry out regular checks. Any misuse will be reported to the Director of Corporate Services.

10. Games and personal use of equipment

10.1 The Council wishes to encourage the use of Internet and electronic mail facilities by staff and to grow their competence and understanding of its potential. Staff may use their Internet connections for occasional personal purposes, at the discretion of their managers, provided:

- It does not interfere with Council work
- It is not related to a personal business interest
- It is not used for commercial purposes, including the sale or purchase of goods and services
- It does not involve the use of irrelevant newsgroups, chat lines or similar services
- It complies with this policy, including its provisions regarding misuse

10.2 Managers are responsible for monitoring time spent by staff on personal use. Staff spending what their manager considers excessive time on personal use may have their connection withdrawn and may be subject to disciplinary proceedings.

10.3 Staff wishing to spend significant time outside working hours using the Internet – for example, for study purposes – should obtain their manager's prior approval and inform the Help Desk of their late working requirements.

10.4 Staff or Members posting items/comments to relevant newsgroups should add the disclaimer:

"*The views contained in this post are those of the originator. They are not the views or opinions of Bracknell Forest Borough Council*" (as is automatically placed in the footer of all outgoing e-mails).

10.5 In principle the Council does not sanction the use of games software. However it is prepared to allow staff to use the pre-loaded Microsoft games package only in break periods within the normal working day. Staff should obtain their manager's prior approval.

11. Portable computer equipment

11.1 All guidelines in this document apply equally to portable equipment e.g. laptops and PDA's (e.g. Section 10)

11.2 Staff issued with portable equipment such as laptops or mobile telephones (which are not asset registered) must take sensible precautions to prevent their loss or misuse:

- Do not leave such equipment unattended
- Ensure it is password protected (see Section 4)
- Ensure your laptop has a current version of anti-virus software (contact the IT Help Desk to obtain the latest version)
- Report any suspected misuse/theft immediately
- Pay for personal mobile calls

11.3 While in the office

- Ensure that the laptop is in a secure place at all times
- If left unattended ensure that it is secured and hidden from sight

- Be aware of any strangers or contractors around your premises. Alert the relevant people if you have cause for concern.
- If you leave your laptop, formally close it down to prevent unauthorised access to your data.
- When leaving the office either lock the portable away or remove it from the premises.

11.4 Outside the office

- If staying in a hotel the laptop should not be left unattended or in an obvious place in your room – one option is to leave it in the hotel's secure area.
- At home laptops should be afforded the same protection as your other household valuables e.g. not left in the garden or conservatory.

11.5 Travelling

- When in transit consider how your laptop can best be carried e.g. in a standard briefcase or sports bag rather than just the manufacturer's carry case.
- If taken aboard aircraft laptops should be carried as hand luggage to prevent damage and loss.
- During car journeys laptops should be out of sight e.g. in the boot to prevent traffic lights theft.
- When travelling on public transport your laptop should be in your sight and control at all times.
- Due to the vulnerability of laptops, PDA's to theft, sensitive data should never be stored on the hard disk (C: drive).

12. Data Protection Act

12.1 The eight data protection principles embodied in the Data Protection Act 1984 (and in the 1998 Act) relates to information about individuals and must be observed. They are as follows:

1) The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.
2) Personal data shall be held only for one or more specified and lawful purposes.
3) Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.
4) Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
5) Personal data shall be accurate and, where necessary, kept up to date.
6) Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
7) An individual shall be entitled:
   a) at reasonable intervals and without undue delay or expense –
      (i) to be informed by any data user whether he holds personal data of which that individual is the subject; and
      (ii) to access to any such data held by a data user; and

b) where appropriate, to have such data corrected or erased.

8) Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

12.2 The Act further specifies four categories of sensitive data which users should consider as requiring effective security. These are:

- Racial origin
- Political opinions or religious or other beliefs
- Physical or mental health or sexual life
- Criminal convictions

12.3 If you are in any way doubtful as to the security of such sensitive data, contact the Borough Data Protection Officer, Legal Services.

12.4 It is each individual user's responsibility to ensure that he/she abides by these principles.

12.5 Further advice on the Data Protection Act may be obtained from the Data Protection Officer in Legal Services.

13. 'All Users' broadcasting

13.1 This section aims to define the acceptable use of the 'Bracknell All Users' e-mail addressing facility. With the growth of e-mail use within the Council (1600+ mail addresses) and the successful take up of the technology as a communication medium, the problem of 'junk' e-mail has become an issue. As a user of e-mail an individual has the facility to mail anyone and everyone on the distribution list, though the subject matter may be of no interest or relevance to the recipient. The volume of legitimate e-mail a recipient receives is increasing, thus it is important that they are not hindered with unnecessary e-mail filling up their mailbox.

13.2 The members of the Corporate Management Team have approved a number of appropriate message types which can be used for 'Bracknell All Users' distribution:

- Press Releases issued by the Media and Information Officer
- Notices from the Chief Executive and/or Directors
- Corporate Emergency Notifications
- Fund raising and charity events relating to the Mayoralty or other Council approved causes
- Staff training course information
- ICT Services Help Desk notifications

13.3 Users are reminded that the procedure for approval for using the 'Bracknell All Users' facility is as follows;-

- Seek Assistant Director or Head of Service approval for content
- Forward the details to the IT Help Desk for 'Bracknell All Users' distribution

- Refer any disputes to the Director of Corporate Services

13.4 Message types outside the scope of the approved message types for the 'Bracknell All Users' are as follows;-

- Item for sale)
- Starters and Leavers) These items will eventually
- Retirement, marriages etc) be catered for by the Intranet
- Telephone number changes)
- Personal social events)

- Lost & found items) These items should be
- Build specific issues) approved and sent to
- E.g. Notification of building works) recipients via local
- Car lights etc) departmental distribution
- Fire test arrangements) lists

14. Keeping records

14.1 Where e-mail users believe proof of sent or received e-mails may be required, they should be printed off and filed in case of accidental deletion.

14.2 Where it is anticipated that an e-mail message may need to be referred to in any form of proceedings such e-mail should not be deleted but retained in hard copy format.

14.3 Users must not discuss any litigious or potentially litigious matters or issues arising therefrom through the medium of e-mail.

15. **Consequences of misuse of E-mail**

15.1 Misuse of e-mail, whether intentional or accidental, may create a liability for both the sender and the Council.

15.2 The medium of e-mail often seems to encourage a lack of professional discipline that would not be present in other more formal means of business communication.

15.3 Users should ensure that their e-mails couldn't be interpreted as defamatory or libellous through poor use of grammar or punctuation.

15.4 Users should ensure they are not bound to any commercial agreement due to poor use of grammar or punctuation.

15.5 Similarly users must ensure that personal comments are not interpreted as harassing due to poor presentation.

15.6 Merely deleting information may not remove it from the system and deleted material may still be recovered and reviewed by the Council.

15.7 Unauthorised access or attempted unauthorised access to another's e-mail account (or to any system or application to which the user does not have rights) will result in an employee facing disciplinary action.

15.8 Unauthorised access or any form of computer misuse as defined in this policy will result in an employee facing disciplinary action.

15.9 If any criminal actions or activities are discovered, the Council will inform the Police and criminal prosecution may follow.

16 Procurement

16.1 The Council makes a significant investment, on a yearly basis, in the purchase of ICT equipment and services and has awarded a 'framework supply agreement' contract for the supply of all ICT hardware and software. This uses a simplified and quicker procurement process to replace the Council's standing orders, resulting in reduced costs and administrative overheads. Adhering to this process is important to ensure the Council undertakes its responsibility for sound management practices, security and a clear audit trail for the cost effective procurement of assets.

16.2 Purchases will either be directly initiated through the Help Desk for small volume straight forward (commodity) purchases, or possibly via the Borough IT Services Manager or an ICT Project Leader (where appropriate) for more complex/higher volume requirements which may be part of project development.

16.3 If the Help Desk is contacted directly, you will be required to complete a request form specifying the details of the order and the cost code. The form will need to be authorised by management as appropriate. For commodity purchases, such as for PC's, the service will include building and installing the system.

17 Data backup

17.1 And finally……'Be Secure!' – backup copies of departmental, network and mainframe systems are taken regularly by ICT Services and are checked by the local database administrators. Users should therefore, wherever possible, save their data on a file server (e.g. *YourName on 'Fs-…..(F:*) to enable ICT Services to back it up.

17.2 Users are responsible for taking backup copies of data stored on their local hard disk (the C: drive) onto floppy discs and keeping such discs secure. If you are in any doubt please check with the Help Desk.

This Policy was approved by the Corporate Management Team - Information & Communications & Technology Steering Group - 23 April 1999 *(*Revised 6/2/03*)*

This Policy is designed to conform to BS7799, the Council's Audit requirements, and is in line with the standards used throughout UK public and private sectors

The latest version of this policy may be found in the Financial Management Handbook, which is located in your workplace and also accessible via the Council's Intranet System BFNET