WIRRAL COUNCIL

ICT SECURITY POLICY

CONTENTS

1 INTRODUCTION

1.1 Information and Communications Technology (ICT) is an integral part of the Council's activities: investment in equipment such as personal computers (PCs) and the communications infrastructure is significant. Because access to information via ICT is essential to the provision of services, policies and procedures need to be laid down and enforced in order to safeguard the information required by those services and the Council's interests. These include:

- the physical assets
- access to the information on those assets
- services continuity
- users of the systems and equipment
- compliance with legislation

1.2 This Policy therefore applies to:

- all employees and elected members of the Council
- all employees and agents of other organisations who directly or indirectly support or use the Council's computer systems or networks
- all temporary and agency staff directly employed or indirectly engaged by the Council

1.3 This Policy applies to all areas of ICT, including:

- PCs and associated equipment, including personal digital assistants (PDAs) and mobile equipment
- all servers including, mainframe, Unix, Novell and Microsoft based systems
- printers, faxes and reprographics equipment
- network communications
- software

1.4 This Security Policy should be read in conjunction with Audit Guidelines for ICT Systems, produced by Internal Audit.

2 ENFORCEMENT

2.1 All users of the Council's information and ICT equipment are personally responsible for compliance with this Policy.

2.2 **Information and ICT security is viewed seriously by the Council and any failure to comply with this Policy could lead to disciplinary action being taken against any individual involved.** Non-compliance may be considered gross misconduct and as such may lead to the dismissal of the employee or employees concerned.

Examples of non-compliance include:-

- the installation and use of unauthorised software (including screensavers & wallpaper),
- any unauthorised access, deletion or amendment to software held on a computer,
- the installation and use of any unauthorised computer or telecommunications equipment, to Council networks,
- unauthorised and/or illicit use of the Internet,
- access to inappropriate websites and the downloading or storage of inappropriate images or material,
- the use of data for illicit purposes (including breach of any law, regulation or any reporting requirement of any law enforcement or government agency),
- the copying of software which breaches copyright agreements,
- exposing the Council to actual or potential loss (monetary or otherwise) through the compromise of ICT security,
- the unauthorised disclosure of confidential or personal information or the unauthorised use of corporate data,
- any disclosure of data to an unauthorised member of staff or any other person who is not authorised to see it,
- unauthorised personal use of equipment or changes to equipment configuration,
- unauthorised deletion or alteration of files or data,
- avoidable damage to the Council's equipment,
- sharing of passwords or otherwise compromising password security,
- any theft, damage or loss of IT equipment (eg – theft of PCs or components),
- any unsolicited e-mail which is offensive or appears to be fraudulent,
- use of IT facilities or systems to engage in fraudulent activities.

This is a list of examples and is not intended to be exhaustive.

2.3 Any individual who has knowledge of a breach of this Policy must report it immediately to his or her line manager. Failure to do so could result in disciplinary action being taken. The procedures for reporting a breach are in Appendix 1.

3 LEGISLATIVE FRAMEWORK

3.1 The Council and all staff must comply with all relevant legislation. Users may be held personally responsible for any breach of any relevant legislation. Relevant legislation includes, but is not restricted to:

Data Protection Act 1998 (see paragraph 5.2 below)
Copyright, Designs and Patents Act 1988
Computer Misuse Act 1990
Health & Safety Act (Display Screen Equipment) Regulations 1992

Freedom of Information Act 2000

Anyone who is unsure of their responsibility should seek clarification from their line manager.

4 USE OF COUNCIL ICT EQUIPMENT & NETWORKS

4.1 Access by outside bodies into any of the Council's networks or equipment is not permitted without prior recorded agreement between IT Services and the appropriate Chief Officer.

4.2 Access to departmental systems or information by representatives of external bodies (eg – Department of Work & Pensions) should be authorised by the system owner.

4.3 Telephone numbers allowing access to the Council's networks must not be disclosed to unauthorised persons/bodies.

4.4 No equipment may be

- connected to the network, or
- attached to any equipment connected to the network or which could be connected to the network (e.g. laptops)

without prior recorded authorisation from IT Services.

5 DATA AND PROGRAM OWNERSHIP

5.1 The Council's Data

(a) All computer programs and data resident on the Authority's hardware are for the sole use of the council in undertaking its business; access by members and employees is solely for this purpose, except by express recorded permission of the Chief Officer in consultation with the Director of Finance.

(b) Copying, alteration or interference with computer programs is not permitted, without the recorded agreement of IT Services or the appropriate Chief Officer.

(c) To enable staff to recognise the security level appropriate to the information or data they are using it is necessary to classify the information. To ensure consistency in the way Wirral staff use and protect the information we hold and exchange with partners in the public sector Wirral Council has adopted the Government Protective Marking Scheme (GPMS). Details are in appendix 2.

5.2 Data Protection Legislation

(a) Systems (manual or computer based) which process personal

data about living persons must comply with current data protection legislation. The person responsible for such a system must ensure that the Director of Finance has details of the system. Copies of the official registration - and any subsequent amendments - must be kept in both Finance and user departments.

(b) There must be no unauthorised disclosure of personal data. Personal data may only be disclosed by the officers who are responsible for the data, with the express permission of the owner, in accordance with data protection legislation. Disclosures must only be made by and to the parties specified on the Data Protection Registration form and in accordance with current data protection legislation.

(c) Key data protection principles include, but are not limited to:

- Personal data must be processed fairly and lawfully.
- Personal data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data must be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes must not be kept for longer than is necessary.
- Personal data must be processed in accordance with the rights of data subjects under the Data Protection Act.
- Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against loss or destruction of, or damage to, personal data.
- Personal data must not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

6 ACCESS TO SYSTEMS

6.1 General

The approval, setting up and control of all networks and systems is the responsibility of IT Services in conjunction with user departments. This includes

- access to the internet, and
- systems which are being accessed from public areas.

The data contained within each system will be subjected to a risk analysis to determine its sensitivity (Information Classification – see Appendix 1) and the impact of it being lost or accessed by, or disclosed to, unauthorised persons. Access must be controlled in accordance with procedures approved by IT Services.

6.2 All schools and sites providing public access to electronic services that connect to the corporate broadband network will be connected via a supplementary firewall managed by IT Services. Changes must not be made to any network settings, or additional equipment installed, without the prior recorded agreement of IT Services.

6.3 Day-to-day management of each system may reside outside IT Services: nonetheless, each system has a Systems Administrator, part of whose duties is to ensure adherence to the principles of access control. The appropriate Systems Administrator must be consulted before access can be given to that system. Requests for access to systems will be accepted only from authorised departmental representatives.

6.4 Password Controlled Access

(a) Each user must have a unique user-ID and password. The use of another person's user-ID is not permitted. Users must not disclose their user-ID or password or visibly record them on or near equipment providing access to networks or systems. Users must not use anyone else's account.

(b) Users must change default passwords, which enable first access, immediately.

(c) Log-on passwords should be a minimum of seven characters in length and must contain three different type of characters from the following sets:
- Upper case
- Lower case
- Numbers
- Punctuation

Passwords must be changed every 42 days and especially

when it is suspected that the password has been disclosed. The last 20 passwords cannot be reused and passwords must not contain any part of a user's first or surname.

(d) Persons intending to leave the employ of the Council who have access to applications systems, must immediately have their access capabilities restricted as appropriate, and removed as soon as possible on leaving the Council, either by the system owners and/or local systems administrators whichever is applicable.

(e) When users are away from their desks a password controlled screen lock must be activated.

7 PURCHASE AND DISPOSAL OF ICT EQUIPMENT AND SOFTWARE

7.1 All ICT equipment and software procurement contracts must be co-ordinated by IT Services and the Corporate Procurement Unit. The process must comply with the Contracts Procedure Rules as set out in the Constitution of the Council.

7.2 Authority to purchase equipment is controlled within departments, and IT Services will only act on authorisation agreed between user departments and IT Services. This must be evidenced in writing or by e-mail. IT Services will only place orders for equipment and software, whether placed by Departments or IT Services, which comply with the Council's ICT Strategy and are appropriate for the users' business needs. IT Services will consult with the user department as appropriate to ensure both these criteria are met.

7.3 Details of all ICT equipment must be kept on the Council's central ICT Asset Register. This is controlled by IT Services: however, the accuracy of the information is a joint responsibility between IT Services and user departments.

7.4 To ensure compliance with the Waste Electrical & Electronic Equipment (WEEE) Directive and ensure that sensitive data is not accidentally released disposal of any ICT and associated equipment must be carried out in consultation with IT Services.

8 PCs AND PORTABLE COMPUTERS

8.1 **Configuration** (Set Up)

(a) This includes PCs, and portable equipment such as laptops and handheld devices.

(b) The configuration (set up) of such equipment must be carried out by IT Services. Systems will be configured to allow users access only to those applications, features and facilities they

require to perform their day to day duties, and, where possible, these configurations will be standard across workgroups and locked to prevent unauthorised changes

(c) An anti-virus solution must be installed on every device that has the capability to run it. The anti-virus solution must be kept up-to-date and maintained appropriately.

8.2 **Approved Software**

Unlicensed or personal software must not be installed on the Council's hardware, or connected in any way to the Council's equipment or systems. If software is deemed to be of use to the Council then the Council in accordance with section 7 should duly acquire it under licence. Random spot checks may be conducted by IT Services or Internal Audit to ensure compliance with these provisions. (See also paragraph 11: Licences)

8.3 **Mobile Media**

Use of the disk drives and USB ports (floppy disks, CDs, DVDs, memory sticks and any other mobile media) on networked PCs is not permitted unless recorded authorisation has been given by departmental management in consultation with IT Services. **Where authorisation has been given to a specific user it is their responsibility to ensure that all mobile media connected do not transmit any viruses onto the Council's network**. Mobile media which has been used on other PCs, networked or otherwise, within or outside the Council, must not in any case be used on PCs connected to the Council's networks, until the media has been checked using appropriate virus checking procedures as agreed with IT Services.

8.4 Members and staff using mobile devices away from the office are bound by the rules outlined in this policy. Detailed guidance on the use of mobile devices is provided in Appendix 3.

8.5 **Unauthorised Equipment**

Users must not connect unauthorised equipment of any kind to the Authority's computer systems or networks.

9 SAVING DATA/ BACKUPS

9.1 Service continuity is a high priority for the Council. It is the joint responsibility of users and IT Services, to ensure that appropriate back up and Disaster Recovery procedures are operated and tested. Some systems are backed up by IT Services, however, others, if not on the network, must be backed up by departmental system administrators.

(a) **IT Services' Responsibility**

- Mainframe Applications
- Unix Applications located in the corporate computer rooms
- Windows NT & Novell Netware Servers located in the corporate computer rooms. (Some responsibilities for scheduling will be shared with Systems Administrators)

(b) **Departmental**

Other Departmental Application servers, PC Networks and Stand Alone PCs

It is the responsibility of the system administrator and user to ensure that appropriate back-up procedures are in place. IT Services should be consulted for further advice on back-up procedures.

10 NEW SYSTEMS DEVELOPMENT

10.1 The Corporate Improvement Group (CIG) must approve all new systems development, however resourced, prior to commencement.

10.2 All new systems will be subject to a Business Case justification and will be considered in the light of existing systems functionality and implementation timetable.

10.3 Systems must not be developed or acquired without consulting IT Services. This is to ensure that appropriate software and equipment is used to the standard appropriate for the business needs, and to ensure compliance with the Council's ICT and purchasing policies. Issues which must be taken into account include, but are not limited to:

- development of a system functional specification
- compatibility, if applicable, with other systems
- provision of access by other users, if required and permitted
- adequate security of data
- standard levels of documentation, access control and Audit Trail
- adequate sizing of the systems hardware; connectivity
- sufficient user support, proper maintenance and back-up

11 SOFTWARE LICENCES

11.1 It is the responsibility of IT Services, systems administrators and users as appropriate, to ensure that appropriate software licences are obtained and maintained.

11.2 IT Services, in conjunction with the Information Strategy Group (ISG), will ensure that, if the Policy laid out in this document is followed, the legal requirements of licences will be met. However, it is the responsibility of all departmental managers to ensure that this Policy is followed at all times.

11.3 The Council's Policy for Computer Software Management and Code of Conduct for the Use of Computer Software, included within **Audit Guidelines for ICT Systems**, by Internal Audit, should be followed at all times.

12 ELECTRONIC COMMUNICATION (INCLUDING USE OF INTERNET)

12.1 **Electronic Communication includes**:

- use of E-mail within the Council,
- use of E-mail to and from addresses outside the Council,
- use of the Council's Intranet, and
- general use of the Internet.

12.2 **Authorisation**

Users will be connected to the internet and/ or e-mail only after receipt by IT Services of a completed and suitably authorised INET01 Form.

12.3 Officers must comply with the Council's **Code of Practice** relating to the **Use of Internet and Electronic Mail Facilities** (reproduced at Appendix 4). The following points should be noted:-

- Services will not be used to access, create, transmit or publish any material likely to cause offence.
- The hardware and software, and all messages belong to the Council; messages can be traced to both sender and recipient.
- Authorised staff in IT Services have the right to monitor the content of all e-mails and data which are transmitted to or from the Council's equipment or downloaded to the Council's equipment.
- All Internet sites visited are recorded automatically.
- Current Council personnel policies, including those on equal opportunities and harassment, apply.
- Data Protection legislation applies.
- Failure to comply with Council policies and procedures or legislation may lead to disciplinary and/or legal action.
- All communications sent or received via the Government Connect Secure Extranet (GCSx) or the Government Secure Intranet (GSi) may be intercepted or monitored.
- The automatic forwarding of electronic mail from a Wirral Council email account to another email account in a lower classification domain (ie – an internet email account such as hotmail) is prohibited by Government Connect.

12.4 **Internet and Intranet Access**

Failure to follow this Policy may put the Council's data and networks at risk: therefore non-compliance may lead to disciplinary action.

(a) Access to the Internet and / or Intranet is only permitted on receipt of a properly authorised INET01 form. Control of access within a department is a departmental management issue.

(b) All access must be in a manner approved by and arranged through IT Services.

(c) Any data or information downloaded from the Internet must not be loaded to any other PC, networked or otherwise, until the data has been checked for viruses by a designated systems administrator or by IT Services. It is the user's responsibility to ensure that this is done.

13 PHYSICAL AND ENVIRONMENTAL SECURITY

13.1 Everyone has a duty of care to ensure that equipment:

- is not put at risk of damage or theft, and is used in accordance with safe working practices. For example:

- The location of ICT equipment should be subject to a risk analysis, and should be sited to avoid unauthorised access, damage, theft interference and the effects of environmental or other hazards.
- Equipment in transit must not be left unattended.
- Equipment must not be removed or moved to another location without notification being given to IT Services and the appropriate changes made to the central asset register.
- Eating and drinking should not take place in the immediate vicinity of equipment.

13.2 Responsibility for the physical security of ICT facilities lies with the appropriate Building Manager in consultation with the ICT system owner.

14 HUMAN RESOURCES SECURITY

14.1 Since May 2004 all potential members of staff are subject to the Right to Work in the UK background security check. This involves establishing the identity of a potential employee by providing details of:

1) Identity, proven by visibility of:
   a) Full 10 year passport
   Or:
   b) Birth Certificate, and
   c) An official document issued by a previous employer or Government agency, such as a P45 form

Additionally potential staff must provide details of:

2) Employment history (past 3 years)
3) Nationality and immigration status
4) Criminal Record (unspent convictions only)

14.2 Existing staff employed prior to May 2004 who require access to Government Connect services will also be subject to the Right to Work in the UK background check.

14.3 In some instances a Criminal Records Bureau check will be required. If a candidate is successful in their application for a post requiring a CRB check, they will be required to authorise the Council to apply for disclosure of information from the Criminal Records Bureau. This authorisation must be given at the time the application is made. No check will be made, however, until an appointment is offered.

14.4 The policy and procedure for checking existing employees was approved by Employment & Appointments Committee on 11 March 2004 (Minute No. 95). In accordance with the CRB Code of Practice and because there is no contractual obligation on the employee, the Council will need to seek the existing employee's consent before completing a CRB check.

Appendix 1

REPORTING AN ICT SECURITY INCIDENT

1. INTRODUCTION

1.1 An ICT incident monitoring system is required to:

i) Ensure all incidents are recognised and managed appropriately;
ii) Enable Wirral Council to identify any patterns of problems and take action to rectify them.

2. DEFINITION

2.1 For Wirral Council's purposes, an ICT security incident refers to any event that may cause loss or damage to Council ICT equipment or information that it holds. This includes the disclosure of information to someone not authorised to see it.

2.2 Although the loss of equipment is significant, the most important aspect of managing an incident is to identify what Council information or data has been affected. The person reporting the incident should record as quickly as possible what information is involved. For example, if a Council PC, tablet or CD/Datastick is lost or stolen, a list of the information held on the device or media should be made. If the files in which the information is held are password protected or encrypted, this should also be recorded.

2.3 ICT security incidents may be caused by accidental or deliberate actions. The Wirral Council ICT Security Policy requires all staff to report possible ICT security incidents so that remedial action can be taken and the chances of similar events occurring again are reduced.

2.4 A reportable incident could include, but not be limited to:

i. Any theft, damage or loss of ICT equipment (eg – theft of PCs or components);
ii. Any unauthorised access, disclosure, deletion or amendment to information held on a computer;
iii. Any unauthorised access, deletion or amendment to software held on a computer;
iv. Any unauthorised personal use of ICT facilities;
v. Any loading and use of unauthorised software (eg – games, shareware, hacking tools);
vi. Any unauthorised copying of software;
vii. Any disclosure of data to an unauthorised member of staff or any other person who is not authorised to see it;
viii. Any occurrence of malicious software such as a virus;
ix. Any unsolicited e-mail which is offensive or appears to be fraudulent;
x. Any suspicious event (eg – computer equipment being moved, suspicion that a user's computer has been tampered with).

xi. Access to inappropriate websites and the downloading or storage of inappropriate images or material;
xii. Connection of unauthorised or personal equipment to Council networks;
xiii. Use of ICT facilities or systems to engage in fraudulent activities.

3. PROCEDURES

3.1 The following procedures should be followed:

i. If any member of staff suspects an incident has occurred, they should contact their Line Manager. Staff should **NOT** attempt to respond to any incident themselves.

ii. The Line Manager should then contact the Department Security Officer (DSO).

iii. The incident should then be reported to the IT Services Helpdesk on ext. 4080

iv. The relevant sections of the ICT Security Incident Form (at Annex 1) completed.

If the incident involves the loss or unauthorised disclosure of any council information classified as 'PROTECT' or 'RESTRICTED' this must be recorded.

v. The incident details will then be recorded on the Helpdesk system and passed to IT Services staff for further action.

vi. IT Services staff will investigate.

vii. The incident will be prioritised in terms of its potential impact and urgency. Services affected by the incident will be identified.

viii. At this point, the Council's Press & Public Relations Office should be informed by the DSO about incidents, particularly theft, internet misuse and any cases where Council information has been compromised. Staff should contact the Press Office on 0151 691 8089 or 8089 to discuss the matter further.

ix. If it is suspected that the incident has involved fraudulent activity, then the Council's Anti-Fraud and Corruption procedures should be followed. Details of Wirral's anti-fraud policy can be found at http://10.107.1.50/Personnel/Forms/Anti-Fraud.doc. The relevant departmental investigating officer should be contacted.

x. If it is suspected that the incident involves misuse of the Council's internet service, the 'Internet Misuse Investigation Process' should be followed. Details of the process can be found at Annex 2. The Director of Finance's secretary should be contacted immediately on 0151 666 3057.

xi. The relevant team in IT Services will take the appropriate action to resolve the incident.

xii. The incident will be logged and any relevant evidence collected and saved. If the incident involves any activity which could constitute misconduct, then the Council's disciplinary procedures should be followed.

xiii. If the incident involves stolen, lost or damaged ICT equipment it may be possible to submit an insurance claim. The Insurance and Risk Management team should be contacted on 0151 666 3413 for further details.

xiv. If the incident involves and information, ICT equipment, system or staff related to Government Connect services, the incident must be reported by IT Services to GovCertUK[1] using the form at Annex 3.

xv. The incident will be reviewed by IT Services and corrective action taken to ensure the likelihood of a similar incident occurring is reduced.

xvi. Incidents that have highlighted weaknesses in the Council's ICT security framework, or have involved fraud or internet misuse, will be reported by IT Services to senior management via the Information Strategy Group (ISG).

Annex 4 outlines the above key stages in the incident reporting and response process.

4. ROLES & RESPONSIBILITIES

4.1 Staff

All Wirral Council staff are required to adhere to the ICT Security Policy and the Code of Practice for Use of Internet and Electronic Mail Facilities. If an ICT security incident is suspected users must report it immediately to their line manager. Under no circumstances should staff attempt to respond to an incident themselves.

4.2 Line Manager

When told of an ICT Security Incident a Line Manager they must ensure that any equipment involved remains untouched and that the designated Security Officer for their department is contacted. If the incident involves inappropriate use of the internet the Council's Internet Misuse – Investigation Process must be followed. Details of this are attached at Annex 2.

4.3 Departmental Security Officer (DSO)

When alerted to a suspected ICT Security Incident the DSO must contact the IT Services Helpdesk on x4080 and complete an ICT Security Incident Form. All relevant details must be recorded, including details of any assets and information. If necessary the DSO is responsible for contacting the Press & PR

[1] For more information see http://www.cesg.gov.uk/govcertuk/index.shtml

office; invoking the anti-fraud procedures; and completing and submitting any insurance claim.

4.4 Helpdesk

The Helpdesk will record the details of the incident, log a job and forward it to the relevant officer within IT Services.

4.5 IT Services

IT Services will investigate, diagnose and classify any ICT Security Incident. If necessary they will invoke the relevant procedures if the case involves misuse of the internet. In certain circumstances the case will be forwarded to a specialist team to be dealt with. If the incident is related to the Government Connect programme it will be reported to GovCertUK. Once resolved IT Services will review the incident and implement any necessary corrective actions to reduce the chance of the incident reoccurring in the future.

4.6 A summary report of incidents will be reported annually to ISG.

Annex 1

ICT SECURITY INCIDENT FORM

Security Incident Report Number	*To be completed by ITS Helpdesk* *Will need to cross reference with Helpdesk number*

Date of incident		**Time**	
Staff Name		**Telephone**	
Section		**Department**	
Line Manager			
Location			

Nature of Incident	Brief report outlining the circumstances and details of the incident. Indicate if the incident was accidental or deliberate.
Information/data lost or compromised	*Information Classification – Not Protectively Marked, Protect, Restricted*

Description of Items	
Asset Number	
Asset Description	
Estimated Value of Items	**£**
Insurance Claim	Will a claim be submitted? **Yes** **No** Details, and completed Insurance Form, to be forwarded to Risk and Insurance Management Team *(link to form to be included here)*.

IT Services Actions	
IT Services Officer	
Description of Response	
Asset Register Updated?	
GovCertUK contacted?	If the incident relates to Government Connect services.

Follow Up Actions

Details of any further actions, including processes and procedures, that need to be undertaken to minimise the risk of incident reoccurring.

Annex 2

INTERNET MISUSE – INVESTIGATION PROCESS

IF IMAGES OF A SEXUAL NATURE INVOLVING CHILDREN OR ANIMALS ARE DISCOVERED AT ANY STAGE DURING THIS PROCESS THE INVESTIGATION MUST BE STOPPED, THE EVIDENCE SECURED, THE COMPUTER PLACED IN SECURE STORAGE AND THE POLICE INFORMED.

Line Managers

If it is suspected that a member of staff has been accessing inappropriate Internet sites then line managers should adopt the following procedure.

1. The member of staff should be escorted away from the computer, which should be left switched on, not touched and not left unattended. This will preserve as much evidence as possible.

2. The line manager should report the incident to the Director of Finance's secretary, telephone number (666) 3057, and provide the following information: -
   - Contact name and telephone number
   - Location of the equipment
   - Computer base unit asset reference number

3. If a member of ITS cannot attend site before the end of the working day the computer should be closed down and locked in secure storage. Some evidence may be lost during the close down process.

4. ITS will investigate the incident and report back to the line manager who should initiate the appropriate disciplinary action.

Secretarial

On receipt of a report of suspected misuse Secretarial should carry out the following.

5. Contact a member of ITS staff in the following order: -

• Steve Catlow	Group Leader, Distributed Systems	x3046
• Andy Molloy	Principal IT Officer, Distributed Systems	x3099
• John Ellis	Senior IT Officer, Distributed Systems	x3208
• Martin Dewhirst	Principal IT Officer, Distributed Systems	x3100
• Geoff Paterson	Infrastructure Manager	x3029
• John Macmillan	Superstructure Manager	x3074
• John Carruthers	Head of Service	x3106

6. Provide details of the incident and the information given at (2.) above.

ITS

7. On receipt of a report a member of IT Services staff will be requested to investigate.

8. As much investigative work as possible will be carried out and recorded prior to the computer being closed down.

9. The computer will be transported to the IT Services workshop for further investigation, where it will be clearly labelled and securely stored.

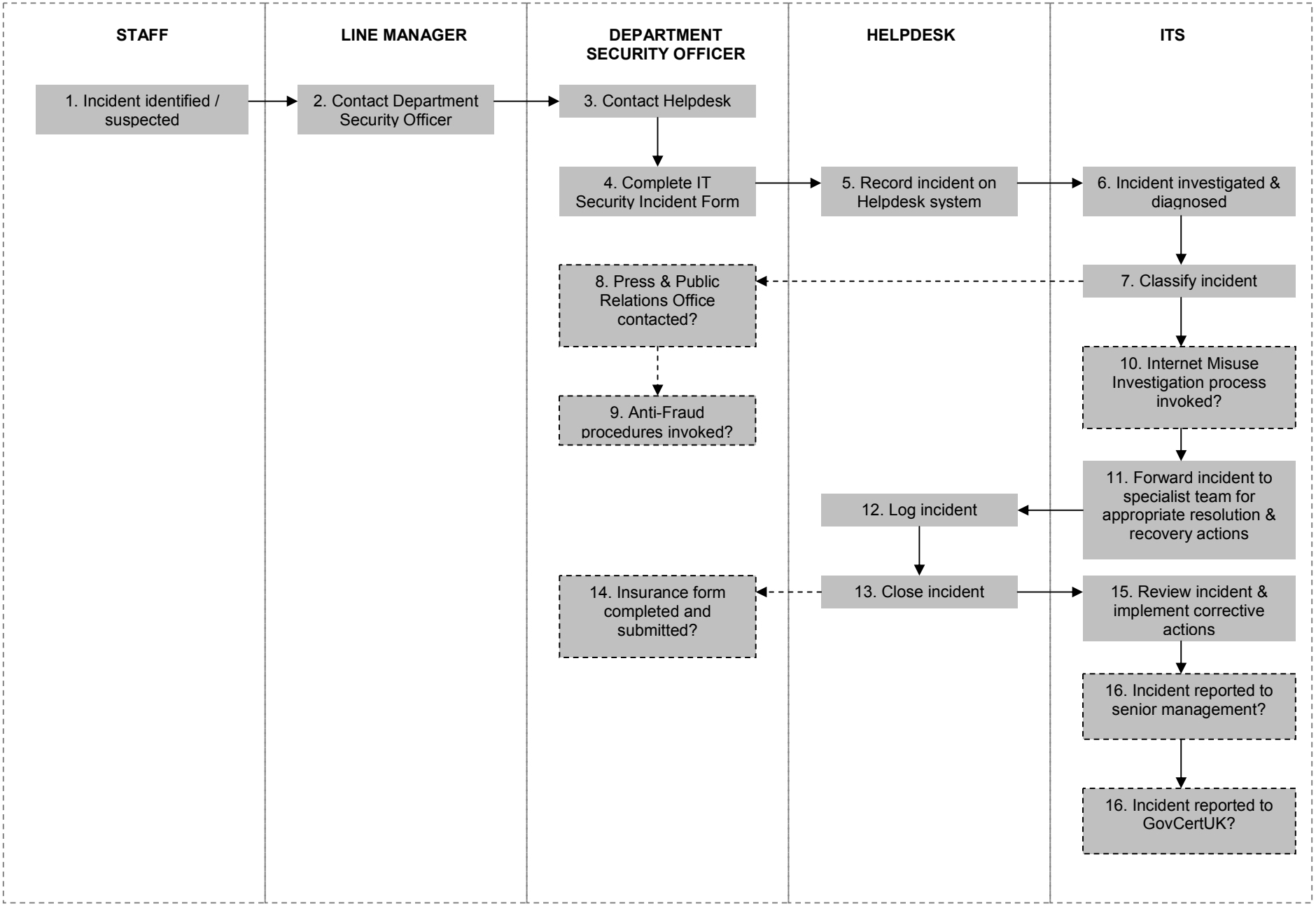
10. IT Services will analyse all firewall logs to determine the dates, times and which sites were accessed.

11. A report of findings will be sent to the originating line manager for action.

Annex 3

GOVCERTUK INCIDENT REPORT FORM

General Information	
Reported By:	**Date/Time Detected:**
Department:	**Date/Time Reported:**
Title:	**Mobile:**
Phone:	**Fax:**
Email Address:	**Additional Information:**
Postal Address:	
Incident Details	
Type of Incident:	
Status of the Department:	**Classification of affected System:**
Incident Details:	
Site Details:	**Site Point of Contact:**
Actions Taken: For further information go to: http://www.cesg.gov.uk/govcertuk/index.shtml	



ICT SECURITY INCIDENT PROCESS

Actions with a dotted border must always be considered but executing them will depend on the individual incident.

Annex 4

Appendix 2

GOVERNMENT PROTECTIVE MARKING SCHEME (GPMS)

1. DEFINITIONS

1.1 The national Government Protective Marking System provides a framework for people handling public sector information to recognize the security required for the information being held, processed or transmitted. Each protective marking is allocated an appropriate Impact Level (IL). The IL value is used in order to determine how much protection these assets should be given. To recognise the appropriate security required, the person handling the information must consider the impact of it being released outside its normal channels, or the impact of its loss or destruction. The GPMS has 7 impact levels – see below.

Protective Marking	e-Government Impact Level
TOP SECRET	6
SECRET	5
CONFIDENTIAL	4
RESTRICTED	**3**
PROTECT	**2** **1**
Not Protectively Marked	**0**

1.2 A description of Top Secret and Secret is not given here. Anyone holding information that may have a higher IL than CONFIDENTIAL should contact the IT Services Helpdesk.

1.3 The compromise of assets marked “CONFIDENTIAL” would be likely to:

- Materially damage diplomatic relations, that is, cause formal protest or other sanctions
- Prejudice individual security or liberty
- Cause serious damage to the operational effectiveness of security or UK or allied forces
- Cause serious damage to the continuing effectiveness of highly valuable security or intelligence operations
- Work substantially against national finances or economic and commercial interests
- Impede the investigation or facilitate the commission of serious crime
- Seriously impede the development or operation of major government policies
- Shut down or otherwise substantially disrupt significant national operations

1.4 Compromise of assets marked “RESTRICTED” would be likely to:

- Adversely affect diplomatic relations
- Cause substantial distress to individuals
- Make it more difficult to maintain the operational effectiveness of security or UK or allied forces
- Cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies
- Prejudice the investigation or facilitate the commission of crime
- Beach proper undertakings to maintain the confidence of information provided by third parties
- Impede the effective development or operation of government policies
- Breach statutory restrictions on the disclosure of information (except the Data Protection Act – which can be addressed by other impact statements and/or the e-Government Security Framework)
- Disadvantage government in commercial or policy negotiations with others
- Undermine the proper management of public sector and its operations

1.5 The compromise of assets marked “PROTECT” would be likely to:

- Cause substantial distress to individuals
- Breach proper undertakings to maintain the confidence of information provided by third parties
- Breach statutory restrictions on the disclosure of information (except the Data Protection Act – which can be addressed by other impact statements and or/the e-government Security Framework).

2. DISTINCTIONS

1.1 At a working level within Wirral the baseline security objectives for PROTECT will be the same as for RESTRICTED, which are:

- Handle, use and transmit with care.
- Take basic precautions against accidental compromise (eg – unprotected data held on a datastick) or opportunist attack (eg – a laptop containing Council information being left on public transport).

1.2 Depending on the severity of the circumstances either RESTRICTED or PROTECT may apply where compromise would be likely to:

- Cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies.
- Prejudice the investigation or facilitate the commission of crime.
- Disadvantage government in commercial or policy negotiations with others.

1.3 Care should be taken when using and describing information with the CONFIDENTIAL protective marking. Within the UK Government CONFIDENTIAL is an explicit marking with clearly defined handling requirements. Sometimes, within Wirral ‘Confidential’ is used as a marking to indicate that information has a requirement for protection. Care should be taken to ensure that information protectively marked with the national CONFIDENTIAL marking should be handled accordingly.

1.4 Wirral staff must also consider the affect of the aggregation of information. For example, an individual instance of a personnel file may be marked as PROTECT. However, if a number of personnel files all marked as PROTECT are stored on a database then the aggregated affect of holding the information together may increase the classification of the data as a whole. Consequently the collective marking would rise to RESTRICTED. If you are in doubt of the aggregation affect of the information you hold you should consult the system owner or the ITS Helpdesk.

	PROTECT	RESTRICTED
Description	Compromise of information would be likely to affect individuals in an adverse manner.	Compromise of information would be likely to affect the national interests in an adverse manner.
Guidelines	• Cause substantial distress to individuals. • Breach proper undertakings to maintain the confidence of information provided by third parties. • Breach statutory restrictions on the disclosure of information.	• Affect diplomatic relations adversely. • Hinder the operational effectiveness or security of the UK or friendly forces. • Affect the internal stability or economic well-being of the UK or friendly countries adversely.
Principles and Clearance Levels	• Information classified as PROTECT should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. • Only staff cleared by the department to access PROTECT level or above are authorised to handle the information. This includes all staff involved with transmission, storage and disposal.	• Information classified as RESTRICTED should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. • Only staff cleared by the department to access RESTRICTED level or above are authorised to handle the information. This includes all staff involved with transmission, storage and disposal.
Electronic Transmission (e-mail)	All PROTECT information may be transmitted across public networks within the UK or across any networks overseas i.e. across the internet.	All RESTRICTED information transmitted across public networks within the UK or across any networks overseas must be encrypted using an approved system.
Electronic Transmission (Fax)	All PROTECT information may be transmitted across the PSTN using a fax.	All RESTRICTED information may not be transmitted by fax at any time.
Electronic Storage	Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: a. User challenge and authentication (username/password or digital ID/Certificate).	Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: a. User challenge and authentication (username/password or digital ID/Certificate).

	PROTECT	RESTRICTED
	b. Logging use at level of individual. c. Firewalls and intrusion-detection systems and procedures; server authentication. d. OS-specific/application-specific security measures.	b. Logging use at level of individual. c. Firewalls and intrusion-detection systems and procedures; server authentication. d. OS-specific/application-specific security measures.
Electronic Disposal	Electronic files should be disposed of in a way that makes reconstruction highly unlikely.	Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
Voice Telephone Conversation	Information protectively marked with PROTECT can be spoken about over the telephone.	Departments should already be aware from S(E)N 06-10 issued on 22 September 2006 that telecommunications made at RESTRICTED (Confidentially IL 3) level can no longer be guaranteed as secure. Appropriate secure communications should be used.
Manual Transmission	• Within a single physical location. As determined by the ITSM or equivalent. • Transfer between establishments within or outside UK: a. May be carried by ordinary postal service or commercial courier firms, provided the envelope/package3 is closed and the word PROTECT is not visible. b. The outer envelope must clearly show a return address in case delivery is unsuccessful. d. In some cases due to the nature of the contents, identifying the originating department may be inappropriate and a return PO Box alone should be used.	• Within a single physical location. As determined by the ITSM or equivalent. • Transfer between establishments within or outside UK: a. May be carried by ordinary postal service or commercial courier firms, provided the envelope/package3 is closed and the word RESTRICTED is not visible. b. The outer envelope should be addressed to an individual by name and title. RESTRICTED mail for/from overseas posts should be carried by diplomatic airfreight. c. The outer envelope must clearly show a return address in case delivery is unsuccessful. d. In some cases due to the nature of the contents, identifying the originating department may be inappropriate and a return PO Box alone should be used.
Manual Storage	• In an office environment, PROTECT material should be held in a lockable storage area or cabinet. • In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment.	• In an office environment, RESTRICTED material should be held in a lockable storage area or cabinet. • In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment.
Manual Disposal	Disposed of or destroyed in a way that makes reconstruction highly	Disposed of or destroyed in a way that makes reconstruction highly unlikely.

	PROTECT	RESTRICTED
	unlikely.	

3. EXAMPLES OF USE OF PROTECT AND RESTRICTED IN WIRRAL COUNCIL

3.1 PROTECT refers to information relating to an individual. For example, information concerning parents who have registered for free school meals should be labelled PROTECT when dealing with an individual case. In instances where this information is viewed collectively, such as a database report showing all Wirral parents who claim free school meals, then the labelling will change to RESTRICTED.

3.2 Information that is personal and sensitive should be labelled RESTRICTED, even if it relates to one record of an individual files. This may include Social Services case files.

3.3 If you wish to discuss the classification of specific information contact the ITS Helpdesk.

Appendix 3

USE OF MOBILE DEVICES

1. WHAT IS THE DEFINITION OF A MOBILE DEVICE?

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

2. PURPOSE OF PROVIDING MOBILE DEVICES

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

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

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

3. PERSONAL USE OF COUNCIL SUPPLIED MOBILE DEVICES

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

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

4. THINGS YOU MUST NOT DO

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

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

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

5. MONITORING THE USE OF MOBILE DEVICES

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

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

5.3 A summary of personal usage above the accepted minimum and the associated costs will be provided to individuals. These costs will be reclaimed by the Council.

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

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

6. MOBILE DEVICES AND THE LAW

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

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

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

6.4 The law (Road Vehicles (Construction and Use) (Amendment) (No. 4) Regulations 2003) prohibits drivers from using a hand-held mobile phone, or similar device, while driving. Employees must never use a phone while driving and ensure that their phone is switched off when driving. Further information on the use of mobile phones in cars is available on the Health Unit's pages of the intranet here.

7. YOUR RESPONSIBILITIES AS A MOBILE DEVICE USER

7.1 It is your responsibility to:

- Familiarise yourself with this guidance before using a council supplied mobile device.
- Assess the risks associated with using your mobile device
- Keep your mobile device secure at all times. Advice on protecting your mobile device and using your mobile device in a public place is given below.

8. THREATS TO MOBILE DEVICES

8.1 Staff should be aware of the threats associated with using a mobile device. These include, but are not limited to:

- Theft
- Loss
- Damage
- Compromise of information
- Malicious attack (eg – viruses)

9. USING YOUR MOBILE DEVICE IN A PUBLIC PLACE – A QUICK GUIDE

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

9.2 **Be vigilant and don't invite crime:**

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

9.3 **Do your housekeeping:**

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

Appendix 4

USE OF INTERNET AND ELECTRONIC MAIL FACILITIES

CODE OF PRACTICE - EMPLOYEES

This document outlines the policy adopted by the Council for the acceptable use of computer network facilities, including electronic mail and the Internet.

Anyone authorised to use such facilities is required to abide by the conditions laid down in this policy. Any breach of these conditions could result in disciplinary action or in some cases a criminal prosecution.

All users are expected to demonstrate a responsible approach in the use of resources available to them, and to show consideration for other users, both those using the Council's facilities and those with whom they may come into contact on the Internet. Users are expected to behave in a legal, moral and ethical fashion that is consistent with Council policies and standards.

It must be recognised that any view communicated over the Internet will be deemed to be the view of the Council, and will in most cases be treated as equivalent to correspondence sent by traditional formal routes. Normal rules for authorising correspondence and statements should therefore be applied to electronic communication.

Access to the Internet by personal computers (including portables) provided by the Council must use only the approved service providers. (Downloading "free" browsers etc. may significantly change the way in which the PC is organised, which may in turn give rise to support problems.)

Users must not load unauthorised software, including games, on personal computers provided by the Council.

Users should print only essential material, and should check the length of a document before printing.

Use of the facilities provided will be routinely monitored and any unauthorised or unacceptable use could result in disciplinary measures.

All communications sent or received via the Government Connect Secure Extranet (GCSx) or the Government Secure Intranet (GSi) may be intercepted or monitored.

The automatic forwarding of electronic mail from a Wirral Council email account to another email account in a lower classification domain (ie – an internet email account such as hotmail) is prohibited.

Unacceptable Deliberate Use

The following activities, whilst not an exhaustive list, are unacceptable:

1. The access to or creation, transmission or publication of any offensive, discriminatory, pornographic, obscene or indecent images, sounds, data or other material.

2. The access to or creation, transmission or publication of any data capable of being displayed or converted to such offensive, pornographic, obscene or indecent images, sounds, data or other material.

3. The creation, transmission or publication of any material which is designed or likely to cause offence, inconvenience or needless anxiety, or which may intimidate or create an atmosphere of harassment.

4. The creation, transmission or publication of defamatory material.

5. The receipt or transmission of material that infringes the copyright of another person.

6. The creation, transmission or publication of any material in violation of Data Protection legislation or of any UK or International laws or regulations. Such activity may constitute a criminal offence.

7. The transmission of unsolicited commercial or advertising material to other users of the Council's network or users of the Internet.

8. The deliberate unauthorised access to facilities, services, data or resources within the Council or any other network or service accessible via the Internet, or attempts to gain such access.

9. Unauthorised access to the electronic mail of another individual.

10. Deliberate activities with any of the following characteristics or that by their nature could result in:

    - wasting staff or other users' efforts or network resources
    - corrupting or destroying other users' data
    - violating the privacy of other users
    - disrupting the work of other users
    - using the internet in a way that denies service to other users (for example by overloading the connection to the network by unnecessarily, excessively and thoughtlessly downloading large files)
    - continuing to use any item of software or to access any material after being requested to cease its use because of disruption caused to the functioning of the Council's network or the Internet (for example utilities designed to broadcast network-wide messages)
    - the introduction or propagation of viruses

11. Where the Internet is being used to access another network, any abuse of the acceptable use policy of that network.

12. Any use of the Internet or other facilities that could damage the reputation of the Council.