

AUDIT, GOVERNANCE AND STANDARDS HEARING PANEL MEETING

Date: Wednesday 20 June 2018
Time: 2.00 p.m.
Venue: Town Hall, High Street, Maidstone

Membership:
Councillors Daley, Harvey and McLoughlin

AGENDA

Page No.

1. Election of Chairman
2. Apologies for Absence
3. Declarations of Interests
4. In the absence of the Subject Member, to consider whether to adjourn or to proceed with the hearing
5. Introduction of those Present
6. To receive representations from the Monitoring Officer and/or Subject Member as to whether any part of the hearing should be held in private and/or whether any documents (or parts thereof) should be withheld from the public/press
7. To determine whether the public/press are to be excluded from any part of the meeting and/or whether any documents (or any parts thereof) should be withheld from the public/press
8. Complaint of Misconduct against a Maidstone Borough Councillor 1 - 64

Issued on Tuesday 12 June 2018

Alison Broom

Alison Broom, Chief Executive

Audit, Governance and Standards Hearing Panel

**Wednesday 20th
June 2018**

Consideration of Complaint M011102

Final Decision-Maker	Audit, Governance and Standards Hearing Panel
Lead Head of Service	Patricia Narebor, Head of Legal Partnership
Lead Officer and Report Author	Christine Nuttall, Senior Lawyer, Corporate Governance (Locum)
Classification	Part 2 matters will be considered in the absence of the public and press for the reasons indicated within the report.
Wards affected	Not applicable.

Executive Summary

The Audit, Governance and Standards Hearing Panel is invited to consider the report of the Investigating Officer and determine what action, if any, to take in respect of complaint numbered M011102.

This report makes the following recommendations to this Hearing Panel:

1. To receive the Investigator's Report and decide on the outcome of the complaint.

Timetable

Meeting	Date
Audit, Governance and Standards Hearing Panel	20 th June 2018

Consideration of Complaint M011102

1. INTRODUCTION AND BACKGROUND

This report is divided into 2 parts. Part 1 is taken in the presence of the public and press. Part 2 items will be considered in the absence of the public and press for the reasons set out below.

PART 1 – MATTERS TO BE CONSIDERED WITH THE PUBLIC AND PRESS PRESENT

2. COMPLAINT

The Monitoring Officer received a complaint under the Councillors' Code of Conduct, reference number M011102. The Monitoring Officer in consultation with the Independent Person decided that the complaint merited formal investigation and appointed an Investigating Officer to undertake the investigation and informed the Parties of the appointment.

The report of the Investigating Officer provides a summary of the business to be transacted in consideration of complaint numbered M011102.

3. EXCLUSION OF THE PRESS AND PUBLIC

The Investigator's Report with Appendices have been withheld from public circulation and deposit pursuant to Section 100(B)(2) of the Local Government Act 1972 on the grounds that the matters may be determined with the press and public excluded.

The Hearing Panel may decide that the press and public be excluded from the meeting during consideration of matters set out in Part 2 pursuant to Section 100(A)4 of the Local Government Act 1972 on the grounds that they involve the likely disclosure of exempt information as defined in Paragraphs 1 and 2 of Part 1 of Schedule 12A to the Local Government Act 1972 and the public interest would not be served in publishing the information.

Paragraphs 1 and 2 of Part 1 of Schedule 12A exempts information relating to any individual and information which is likely to reveal the identity of an individual.

The Subject Member has requested that the hearing be held in private.

If the Hearing Panel declines to pass a resolution that the press and public be excluded from the meeting, the papers listed under Part 2 of this report will be made available to the public at the meeting and will be posted on the Council's website at the conclusion of the meeting.

PART 2 – MATTERS TO BE CONSIDERED WITHOUT THE PUBLIC AND PRESS PRESENT

4. CONSIDERATION OF COMPLAINT MO11102

The Hearing Panel is invited to consider the report of the Investigating Officer and determine what action, if any, to take in respect of the above Complaint.

Issue	Implications	Sign-off
Impact on Corporate Priorities	Maintaining appropriate standards of Member conduct contributes indirectly to all Corporate Priorities.	Monitoring Officer
Risk Management	No risks have been identified for this report.	Head of Legal Partnership
Financial	There are no financial implications arising from this report.	Head of Legal Partnership
Staffing	No staffing issues have been identified in this report.	Head of Legal Partnership
Legal	The Hearing Panel is required to determine all complaints referred to them by the Monitoring Officer where a Member of a Council in the Borough is alleged to have breached their respective Councillors' Code of Conduct under the provisions of the Localism Act 2011.	Monitoring Officer
Privacy and Data Protection	The Hearing will increase the volume of data held by the Council. We will hold that data in line with any requirements of the Localism Act 2011 and the Data Protection legislation.	Head of Legal Partnership
Equalities	There are no equality issues associated with this report.	Head of Legal Partnership
Crime and Disorder	There are no crime and disorder implications associated with this report.	Head of Legal Partnership
Procurement	Not applicable.	Head of Legal Partnership

Appendices:

Appendix 1: Code of Conduct for Councillors

Appendix 2: Computer Use Policy 1.3

Exempt Appendices

By virtue of paragraphs 1 and 2 of Part 1 of Schedule 12A to the Local Government Act 1972 the following Appendices are exempt because they contain information relating to any individual (paragraph 1) and information which is likely to reveal the identity of an individual (paragraph 2) and it is considered that the public interest in maintaining the exemption outweighs the public interest in disclosing the information:

Exempt Appendix 3: Investigating Officer's Report

Exempt Appendix 4: Member Complaint Form

Exempt Appendix 5: Mid Kent Audit Report

Exempt Appendix 6: Subject Member Witness Statement

Exempt Appendix 7: Witness Statement of Head of Mid Kent Audit

Exempt Appendix 8: Witness Statement of Mid Kent Services Director

4.1 COUNCILLORS' CODE OF CONDUCT

Preamble

- (A) The Code of Conduct that follows is adopted under section 27(2) of the Localism Act 2011.
- (B) The Code is based on the Seven Principles of Public Life under section 28(1) of the Localism Act 2011, which are set out in Annex 1.
- (C) This Preamble and Annex 1 do not form part of the Code, but you should have regard to them as they will help you to comply with the Code.
- (D) If you need guidance on any matter under the Code, you should seek it from the Monitoring Officer or your own legal adviser – but it is entirely your responsibility to comply with the provisions of this Code.
- (E) In accordance with section 34 of the Localism Act 2011, where you have a Disclosable Pecuniary Interest it is a criminal offence if, without reasonable excuse, you:
 - (a) Fail to notify the Authority's Monitoring Officer of the interest before the end of 28 days beginning with the day on which you became a Councillor.
 - (b) Fail to disclose the interest at Meetings where the interest is not entered in the Authority's register.
 - (c) Fail to notify the Authority's Monitoring Officer of the interest before the end of 28 days beginning with the date of disclosure at a meeting, if the interest is not entered in the Authority's register and is not the subject of a pending notification.
 - (d) Take part in discussion or votes, or further discussions or votes, at Meetings on matters in which you have the interest which are being considered at the meeting.
 - (e) Fail to notify the Authority's Monitoring Officer of the interest before the end of 28 days beginning with the date when you become aware that you have such an interest in a matter to be dealt with, or being dealt with, by you acting alone in the course of discharging a function of the Authority.
 - (f) Take any step in relation to a matter being dealt with by you acting alone in the course of discharging a function of the Authority, except a step for the purpose of enabling the matter to be dealt with otherwise than by you.
 - (g) Knowingly or recklessly provide false or misleading information in any of the above disclosures or notifications.
- (F) Any written allegation received by the Authority that you have failed to comply with the Code will be dealt with under the arrangements adopted by the Authority for such purposes. If it is found that you have failed to comply with the Code, the Authority may have regard to this failure in deciding whether to take action and, if so, what action to take in relation to you.

THE CODE

1. Interpretation

In this Code:

“Associated Person” means (either in the singular or in the plural):

- (a) a family member or any other person with whom you have a close association, including your spouse, civil partner, or somebody with whom you are living as a husband or wife, or as if you are civil partners; or
- (b) any person or body who employs or has appointed such persons, any firm in which they are a partner, or any company of which they are directors; or
- (c) any person or body in whom such persons have a beneficial interest in a class of securities exceeding the nominal value of £25,000; or
- (d) any body of which you are in a position of general control or management and to which you are appointed or nominated by the Authority; or
- (e) any body in respect of which you are in a position of general control or management:
 - (i) exercising functions of a public nature; or
 - (ii) directed to charitable purposes; or
 - (iii) one of whose principal purposes includes the influence of public opinion or policy (including any political party or trade union).

“Authority” means Maidstone Borough Council.

“Authority Function” means any one or more of the following interests that relate to the functions of the Authority:

- (a) housing - where you are a tenant of the Authority provided that those functions do not relate particularly to your tenancy or lease; or
- (b) school meals or school transport and travelling expenses - where you are a parent or guardian of a child in full time education, or are a parent governor of a school, unless it relates particularly to the school which your child attends;
- (c) statutory sick pay under Part XI of the Social Security Contributions and Benefits Act 1992 - where you are in receipt of, or are entitled to the receipt of, such pay;
- (d) an allowance, payment or indemnity given to Councillors of the Authority;
- (e) any ceremonial honour given to Councillors of the Authority;
- (f) setting council tax or a precept under the Local Government Finance Act 1992.

“Code” means this Code of Conduct.

“Co-opted Member” means a person who is not an elected Councillor of the Authority but who is a member of:

- (a) any Committee or Sub-Committee of the Authority, or

- (b) and represents the Authority on, any joint committee or joint sub-committee of the Authority; and
- (c) who is entitled to vote on any question that falls to be decided at any Meeting.

"Disclosable Pecuniary Interest" means those interests of a description specified in regulations made by the Secretary of State (as amended from time to time) as set out in Annex 2 and where either it is:

- (a) your interest; or
- (b) an interest of your spouse or civil partner, a person with whom you are living as husband and wife, or a person with whom you are living as if you were civil partners and provided you are aware that the other person has the interest.

"Interests" means Disclosable Pecuniary Interests and Other Significant Interests.

"Meeting" means any meeting of:

- (a) the Authority;
- (b) any of the Authority's committees, sub-committees, joint committees and/or joint sub-committees.

"Member" means a person who is an elected Councillor of the Authority and includes a Co-opted Member.

"Other Significant Interest" means an interest (other than a Disclosable Pecuniary Interest or an interest in an Authority Function) in any business of the Authority which:

- (a) may reasonably be regarded as affecting the financial position of yourself and/or an Associated Person to a greater extent than the majority of: -
 - (i) other council tax payers, ratepayers or inhabitants of the electoral division or ward, as the case may be, affected by the decision; or
 - (ii) (in other cases) other council tax payers, ratepayers or inhabitants of the Authority's area; or
- (b) relates to the determination of your application (whether made by you alone or jointly or on your behalf) for any approval, consent, licence, permission or registration or that of an Associated Person;

and where, in either case, a member of the public with knowledge of the relevant facts would reasonably regard the interest as being so significant that it is likely to prejudice your judgement of the public interest.

"Register of Members' Interests" means the Authority's register of Disclosable Pecuniary Interests established and maintained by the Monitoring Officer under section 29 of the Localism Act 2011.

"Sensitive Interest" means information, the details of which, if disclosed, could lead to you or a person connected with you being subject to violence or intimidation.

Scope

2. You must comply with this Code whenever you act in your capacity as a Councillor or Co-opted Member of the Authority.

General obligations

3. (1) You must, when using or authorising the use by others of the resources of the Authority:
- (a) act in accordance with the Authority's reasonable requirements; and
 - (b) ensure that such resources are not used improperly for political purposes (including party political purposes).
- (2) You must not:
- (a) bully any person;
 - (b) intimidate or attempt to intimidate any person who is or is likely to be a complainant, a witness, or involved in the administration of any investigation or proceedings, in relation to an allegation that a Councillor (including yourself) has failed to comply with this Code;
 - (c) do anything that compromises, or is likely to compromise, the impartiality or integrity of those who work for, or on behalf of, the Authority;
 - (d) disclose information given to you in confidence by anyone, or information acquired by you which you believe, or ought reasonably to be aware, is of a confidential nature, except where:
 - (i) you have the written consent of a person authorised to give it; or
 - (ii) you are required by law to do so; or
 - (iii) the disclosure is made to a third party for the purpose of obtaining professional advice provided that the third party agrees not to disclose the information to any other person; or
 - (iv) the disclosure is:
 - reasonable and in the public interest; and
 - made in good faith and in compliance with the reasonable requirements of the Authority;
 - (e) prevent another person from gaining access to information to which that person is entitled by law;
 - (f) conduct yourself in a manner which could reasonably be regarded as bringing your office or the Authority into disrepute;
 - (g) use or attempt to use your position as a Councillor improperly to confer on or secure for yourself or any other person, an advantage or disadvantage.

Registering Disclosable Pecuniary Interests

- 4.(1) You must, before the end of 28 days beginning with the day you become a Councillor or Co-opted Member of the Authority, or before the end of 28 days beginning with the day on which this Code takes effect (whichever is the later), notify the Monitoring Officer of any Disclosable Pecuniary Interest.
- (2) In addition, you must, before the end of 28 days beginning with the day you become aware of any new Disclosable Pecuniary Interest or change to any interest already registered, register details of that new interest or change, by providing written notification to the Monitoring Officer.
- (3) Where you have a Disclosable Pecuniary Interest in any matter to be dealt with, or being dealt with, by you acting alone in the course of discharging a function of the Authority (including making a decision in relation to the matter), then if the interest is not registered in the Register of Members' Interests and is not the subject of a pending notification, you must notify the Monitoring Officer before the end of 28 days beginning with the day you become aware of the existence of the interest.

Declaring Interests

5. (1) Whether or not a Disclosable Pecuniary Interest has been entered onto the Register of Members' Interests or is the subject of a pending notification, you must comply with the disclosure procedures set out below.
- (2) Where you are present at a meeting and have a Disclosable Pecuniary Interest or Other Significant Interest in any matter to be considered, or being considered, at the meeting, you must:
- (a) disclose the Interest; and
 - (b) explain the nature of that Interest at the commencement of that consideration or when the Interest becomes apparent (subject to paragraph 6, below); and unless you have been granted a dispensation or are acting under para 5(4):
 - (c) not participate in any discussion of, or vote taken on, the matter at the Meeting; and
 - (d) withdraw from the Meeting room in accordance with the Authority's Procedure Rules whenever it becomes apparent that the business is being considered; and
 - (e) not seek improperly to influence a decision about that business.
- (3) Where you have a Disclosable Pecuniary Interest or Other Significant Interest in any business of the Authority where you are acting alone in the course of discharging a function of the Authority, you must:
- (a) notify the Monitoring Officer of the interest and its nature as soon as it becomes apparent; and

- (b) not take any steps, or any further steps, in relation to the matter except for the purpose of enabling the matter to be dealt with otherwise than by you; and
 - (c) not seek improperly to influence a decision about the matter.
- (4) Where you have an Other Significant Interest in any business of the Authority, you may attend a Meeting but only for the purpose of making representations, answering questions or giving evidence relating to the business, provided that the public are also allowed to attend the Meeting for the same purpose. Having made your representations, given evidence or answered questions you must:
- (a) not participate in any discussion of, or vote taken on, the matter at the Meeting; and
 - (b) withdraw from the Meeting room in accordance with the Authority's Procedure Rules.

Sensitive Interests

6. (1) Where you consider that the information relating to any of your Disclosable Pecuniary Interests is a Sensitive Interest, and the Monitoring Officer agrees, the Monitoring Officer will not include details of the Sensitive Interest on any copies of the Register of Members' Interests which are made available for inspection or any published version of the Register, but may include a statement that you have an interest, the details of which are withheld under this paragraph.
- (2) You must, before the end of 28 days beginning with the day you become aware of any change of circumstances which means that information excluded under paragraph 6(1) is no longer a Sensitive Interest, notify the Monitoring Officer asking that the information be included in the Register of Members' Interests.
- (3) The rules relating to disclosure of Interests in paragraphs 5(2) and (3) will apply, save that you will not be required to disclose the nature of the Sensitive Interest, but merely the fact that you hold an interest in the matter under discussion.

Gifts and Hospitality

7. (1) You must, before the end of 28 days beginning with the day of receipt/acceptance, notify the Monitoring Officer of any gift, benefit or hospitality with an estimated value of £100 or more, or a series of gifts, benefits and hospitality from the same or an associated source, with an estimated cumulative value of £100 or more, which are received and accepted by you (in any one calendar year) in the conduct of the business of the Authority, the business of the office to which you have been elected or appointed or when you are acting as representative of the Authority. You must also register the source of the gift, benefit or hospitality.

- (2) Where any gift, benefit or hospitality you have received or accepted relates to any matter to be considered, or being considered at a Meeting, you must disclose at the commencement of the Meeting or when the interest becomes apparent, the existence and nature of the gift, benefit or hospitality, the person or body who gave it to you and how the business under consideration relates to that person or body. You may participate in the discussion of the matter and in any vote taken on the matter, unless you have an Other Significant Interest, in which case the procedure in paragraph 5 above will apply.
- (3) You must continue to disclose the existence and nature of the gift, benefit or hospitality at a relevant Meeting, for 3 years from the date you first registered the gift, benefit or hospitality.
- (4) The duty to notify the Monitoring Officer does not apply where the gift, benefit or hospitality comes within any description approved by the Authority for this purpose.

Dispensations

- 8.(1) The Monitoring Officer may, on a written request (as appointed Proper Officer for the receipt of applications for dispensation) by a Councillor with an Interest, grant a dispensation relieving the Councillor from either or both of the restrictions on participating in discussions and in voting (referred to in paragraph 5 above).
- (2) A dispensation may be granted only if, after having had regard to all relevant circumstances, the Monitoring Officer considers that:
 - (a) without the dispensation the number of persons prohibited from participating in any particular business would be so great a proportion of the body transacting the business as to impede the transaction of the business; or
 - (b) without the dispensation, the representation of different political groups on the body transacting any particular business would be so upset as to alter the likely outcome of any vote relating to the business; or
 - (c) granting the dispensation is in the interests of persons living in the Authority's area; or
 - (d) it is otherwise appropriate to grant a dispensation.
- (3) A dispensation must specify the period for which it has effect, and the period specified may not exceed four years.
- (4) Paragraph 5 above does not apply in relation to anything done for the purpose of deciding whether to grant a dispensation under this paragraph 8.

ANNEX 1

THE SEVEN PRINCIPLES OF PUBLIC LIFE

In accordance with the Localism Act 2011, and in order to help maintain public confidence in this Authority, you are committed to behaving in a manner that is consistent with the following principles. However, it should be noted that these Principles do not create statutory obligations for Councillors and do not form part of the Code. It follows from this that the Authority cannot accept allegations that they have been breached.

SELFLESSNESS: Holders of public office should act solely in terms of the public interest.

INTEGRITY: Holders of public office must avoid placing themselves under any obligation to people or organisations that might try inappropriately to influence them in their work. They should not act or take decisions in order to gain financial or other material benefits for themselves, their family, or their friends. They must declare and resolve any interests and relationships.

OBJECTIVITY: Holders of public office must act and take decisions impartially, fairly and on merit, using the best evidence and without discrimination or bias.

ACCOUNTABILITY: Holders of public office are accountable to the public for their decisions and actions and must submit themselves to the scrutiny necessary to ensure this.

OPENNESS: Holders of public office should act and take decisions in an open and transparent manner. Information should not be withheld from the public unless there are clear and lawful reasons for so doing.

HONESTY: Holders of public office should be truthful.

LEADERSHIP: Holders of public office should exhibit these principles in their own behaviour. They should actively promote and robustly support the principles and be willing to challenge poor behaviour wherever it occurs.

ANNEX 2

Disclosable Pecuniary Interests, as prescribed by regulations, are as follows:

The descriptions on Disclosable Pecuniary Interests are subject to the following definitions:

“the Act” means the Localism Act 2011

“body in which the relevant person has a beneficial interest” means a firm in which the relevant person is a partner or a body corporate of which the relevant person is a director, or in the securities of which the relevant person has a beneficial interest

“director” includes a member of the committee of management of an industrial and provident society

“land” excludes an easement, servitude, interest or right in or over land which does not carry with it a right for the relevant person (alone or jointly with another) to occupy the land or to receive income

“M” means a councillor of the relevant authority

“member” includes a co-opted member

“relevant authority” means the authority of which M is a councillor

“relevant period” means the period of 12 months ending with the day on which M gives a notification for the purposes of section 30(1), or section 31(7), as the case may be, of the Act

“relevant person” means M or any other person referred to in section 30(3)(b) of the Act (the Member’s spouse, civil partner, or somebody with whom they are living as a husband or wife, or as if they were civil partners).

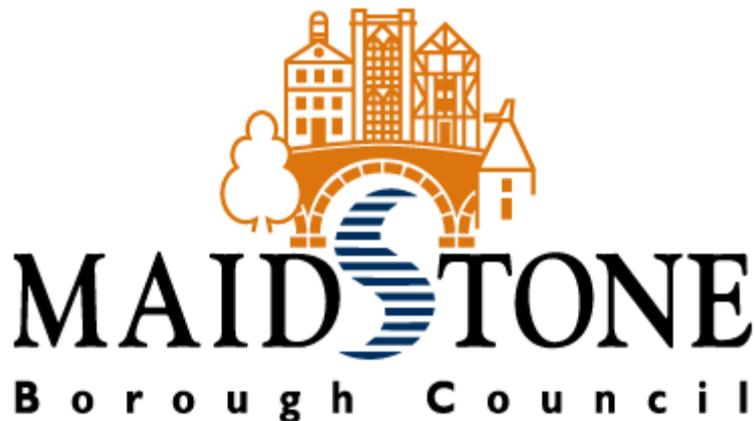
“securities” means shares, debentures, debenture stock, loan stock, bonds, units of a collective investment scheme within the meaning of the Financial Services and Markets Act 2000 and other securities of any description, other than money deposited with a building society

Interest	Description
Employment, office, trade, profession or vacation	Any employment, office, trade, profession or vocation carried on for profit or gain.
Sponsorship	Any payment or provision of any other financial benefit (other than from the relevant authority) made or provided within the relevant period in respect of any expenses incurred by M in carrying out duties as a Councillor, or

APPENDIX 1

	<p>towards the election expenses of M.</p> <p>This includes any payment or financial benefit from a trade union within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992.</p>
Contracts	<p>Any contract which is made between the relevant person (or a body in which the relevant person has a beneficial interest) and the relevant authority:</p> <p>(a) under which goods or services are to be provided or works are to be executed; and</p> <p>(b) which has not been fully discharged.</p>
Land	<p>Any beneficial interest in land which is within the area of the relevant authority.</p>
Licences	<p>Any licence (alone or jointly with others) to occupy land in the area of the relevant authority for a month or longer.</p>
Corporate tenancies	<p>Any tenancy where (to M's knowledge):</p> <p>(a) the landlord is the relevant authority; and</p> <p>(b) the tenant is a body in which the relevant person has a beneficial interest.</p>
Securities	<p>Any beneficial interest in securities of a body where:</p> <p>(a) that body (to M's knowledge) has a place of business or land in the area of the relevant authority; and</p> <p>(b) either</p> <p>(i) the total nominal value of the securities exceeds £25,000 or one hundredth of the total issued share capital of that body; or</p> <p>(ii) if the share capital of that body is of more than one class, the total nominal value of the shares of any one class in which the relevant person has a beneficial interest exceeds one hundredth of the total issued share capital of that class.</p>

MAIDSTONE BOROUGH COUNCIL COMPUTER USE POLICY



Version	Reason	Author	Date
Draft	Government Connect	Dave Lindsay	February 2009
1.0	Security forum amendments	Dave Lindsay	March 2009
1.1	Corporate Information Management Board amendments	Dave Lindsay	May 2010
1.2	Annual review	Dave Lindsay	July 2011
1.3	Audit updates	Dave Lindsay	January 2012

1.	Policy Statement	3
1.1	The need for a computer use policy	3
1.2	The scope of the policy	3
1.3	Management statement	3
1.4	Induction training	3
2.	Asset management	4
2.1	Accountability	4
2.2	Software	4
3.	Information Security	5
3.1	Purpose	5
3.2	Password guidance	5
3.3	Password strategies to avoid	5
3.4	Information classification	6
3.5	Information sharing	7
3.6	Data security	7
3.6.1	Physical security	7
3.6.2	Data storage	8
3.6.3	Removable media	8
3.7	Access to remote systems	9
3.8	Incident management	9
4.	Internet and email usage	11
4.1	Definitions	11
4.2	Conditions of use	11
4.3	Use of the Internet	12
4.4	Use of email	13
5.	Monitoring	16
5.1	Internet monitoring	16
5.2	Email monitoring	16
5.3	Discipline	17
5.4	Legitimate and illegitimate use	17
6.	Disposals policy	19
6.1	Data and document disposal procedure	19
6.2	Equipment disposal procedure	19

1. Policy statement

1.1. The need for a Computer Use policy.

Maidstone Borough Council ("the Council") has made a large investment in the use of information technology. In many areas the use of ICT systems is vital to provide customers with the service they demand and provide good management information that business decisions can be based upon.

It is imperative that all information systems are developed, operated, used and maintained in a safe and secure way. This policy has been written in accordance with the standard *ISO 27000 – Code of Practice for Information Security Management* and it provides a framework of controls for the use and maintenance of secure information systems at the Council.

There are three main objectives of this policy:

- To ensure that all of the Council's assets, staff, data and equipment are adequately protected, on a cost-effective basis, against any action or omission that could adversely affect the ICT services required to conduct Council business?;
- To ensure that staff are aware of and fully comply with all relevant legislation;
- To create and maintain a level of awareness within all sections of the need for IT Security to be an integral part of day to day operations.

1.2. The scope of the policy.

This policy applies to all Councillors and employees, including temporary, casual and contract staff who use the Council's IT facilities (hereafter referred to as 'users') and sets down the standards which users are required to observe in the use of the Council's computer systems and equipment .

1.3. Management Statement.

The Council's computer systems are critical to its ability to function, and to provide services to the public. The Council's Management Team therefore fully endorses the content of this policy, and failure to adhere to the terms of the policy could result in disciplinary action against the transgressor.

This Policy is reviewed annually and approved by the Council's Security Forum. The Council reserves the right to amend this policy at its discretion. In the event of such amendments, all users will be notified appropriately. This policy exists to provide safeguard for the individual and for the Council.

1.4. Induction training.

All staff will be instructed on the requirements of the authority Computer Use Policy within their formal programme of Corporate and departmental induction training .

2. Asset Management.

2.1. Accountability

The IT Section maintains a register of all computer assets, including:

- Servers;
- Network equipment;
- Software and licences;
- Systems documentation;
- Printers;
- Desktop estate, i.e. PCs and laptops.

It is the responsibility of every Business Manager to maintain a Business Continuity Plan which details requirements relating to any incident resulting in the loss of some or all of the equipment (or data) allocated to his or her staff.

2.2. Equipment

It is the responsibility of every user to maintain the IT equipment issued to him or her in a serviceable condition, take reasonable measures to prevent the loss or theft of said equipment, and return all equipment when they leave the Council. Where managers are responsible for protecting the security of network connections and network equipment at remote sites, they should ensure that locks are applied and that key codes changed on a monthly basis.

The IT Section will apply patches and firmware upgrades to your hardware systems as required and in accordance with the Council's procedures for applying security patches.

2.3. Software

Your computer has been provided to you to for a business purpose. You are not permitted to install or download additional software, even if procured for a business purpose without authorisation from the IT Manager. The IT Section will apply patches to your software systems as required and in accordance with the Council's procedures for applying security patches.

If you wish to purchase additional software, please contact the IT Helpdesk. It is imperative that the IT Section is aware of all software purchases to ensure value for money, compliance with the Council's licensing agreements, and compatibility with Council systems. The Council is periodically audited on its software and licensing records, and failure to produce adequate records could result in financial penalties and loss of reputation.

Discs and licences for software should be forwarded to the IT Section to enable its safe storage, and to assist with licence administration. Please note that most software licensing agreements make it illegal to copy software.

3. Information Security.

3.1. Purpose

The purpose of security in any information system is to preserve an appropriate level of:

<i>Confidentiality</i>	access is confined to those with specified need and authority to view and/or change information
<i>Integrity</i>	the system, installation, network is operating according to specification in the way the user expects it to operate and the information contained on the system is correct
<i>Availability</i>	the system or service is available and the output is delivered to the user who needs it when it is required

Information systems include web-based, financial and non-financial, server-based and PC-run systems.

3.2. Password guidance.

The Council operates a system of complex passwords, this means that:

- The minimum length of any password must be **seven characters**;
- Passwords must be sufficiently complex, i.e. they must include a combination of letters, numbers, and/or symbols;
- Passwords will expire after 90 days, after which you will be required to choose a new password;
- Password history includes your last 20 passwords, **which cannot be re-used**;
- Passwords must be kept confidential, **and on no account shared with other users** – if there is a perceived reason why this is required, please contact the IT helpdesk;
- A paper record of passwords must not be maintained, unless it is stored securely;
- You should avoid easily guessable passwords.

3.3. Password strategies to avoid.

Some common methods used to create passwords are easy to guess by criminals. To avoid weak, easy-to-guess passwords:

- **Avoid sequences or repeated characters.** "12345678," "222222," "abcdefg," or adjacent letters on your keyboard do not help make secure passwords;
- **Avoid using only look-alike substitutions of numbers or symbols.** Criminals and other malicious users who know enough to try and crack your password will not be fooled by common look-alike replacements, such as to replace an 'l' with a '1' or an 'a' with '@' as in "M1cr0\$0ft" or "P@ssw0rd" - but these substitutions can be effective when combined with other measures, such as length, misspellings, or variations in case, to improve the strength of your password;
- **Avoid your login name.** Any part of your name, birthday, national

- insurance number, or similar information for your loved ones constitutes a bad password choice - this is one of the first things criminals will try;
- **Avoid dictionary words in any language.** Criminals use sophisticated tools that can rapidly guess passwords that are based on words in multiple dictionaries, including words spelled backwards, common misspellings, and substitutions - this includes all sorts of profanity and any word you would not say in front of your children;
 - **Use more than one password everywhere.** If any one of the computers or online systems using this password is compromised, all of your other information protected by that password should be considered compromised as well - it is critical to use different passwords for different systems.

3.4. Information classification.

The Council has adopted the Local Government Classification scheme, the purpose of which is to provide a standard framework to help store, share, and dispose of information. Within the scheme there are a variety of types of information which needs to be managed:

- Commercially sensitive e.g. financial data relating to contracts;
- Personal data relating to 'customers';
- Personal data relating to staff e.g. payroll data;
- Property data relating to customers, i.e. spatial or textual;
- Metadata, i.e. data which describes other data.

The responsibility for defining the classification of an item of information rests with the originator or 'owner' of the data.

Any output from ICT systems considered to be of a sensitive or confidential nature must be labelled appropriately. This applies to printed reports, magnetic media, electronic messages, etc.

From 1st April 2009 the Council is required to comply with the Department of Work and Pension's code of connection, and is required to identify data which is deemed 'restricted'. At some point in the future all correspondence with central government will be governed by this data policy. Restricted information is defined as any asset whose compromise would be likely to:

- adversely affect diplomatic relations;
- cause substantial distress to individuals ;
- make it more difficult to maintain the operational effectiveness or security of 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;
- breach 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 the public sector and its operations.

Information security now forms part of the Council's induction process, and all users must signal their formal acceptance of this policy. Moreover staff who are authorised to handle information identified as 'restricted' or 'protected' must be made aware of the impact of the loss of such data, and the actions to be taken in the event of any such loss. The recruitment process of such staff will incorporate security screening to 'Baseline Personnel Security Standard'.

If you are responsible for handling restricted data, you will be notified as such by your Line Manager and will receive additional training on the handling, and the procedures to follow in the case of loss of such data.

3.5. Information sharing.

The Council is required to follow the terms of the Data Protection Act 1998 in how it uses and shares data. The following guidelines generally apply:

- Data collected for Electoral registration or Council Tax purposes cannot be shared, even within the Council;
- Data of a personal or sensitive nature collected for one purpose, cannot be used or shared for another purpose;
- Data of a personal or sensitive nature must be kept secure, and on no account must data of this nature be transferred by non-secure means (see data security below), or transferred to a non-council owned computer or portable storage device.
- It is your responsibility to ensure that the recipient of any data transferred by you is authorised to receive it;
- Data held by the Council on its systems in any format is only to be used for legitimate business purposes.

3.6. Data Security

3.6.1. Physical security.

It is your duty to protect the data and information which the Council collects and owns. The IT Section deploys security systems which protect the Council's systems and data from external attack, whether through theft, virus, spyware or other malware. However, perhaps the greatest risk to 'data-in' is posed by users' failure to follow simple security procedures:

- Do not copy data onto removable storage devices (see 'Removable media' below), such as 'USB keys' unless there is a clear business case to do so – *please contact the IT helpdesk, you may be issued with an encrypted device to enable this*;
 - Never leave a computer device unattended without first invoking the password-protected screen saver;
 - Do not save data onto the C: drive of your PC or laptop unless there is a clear business case to do so (see 'Data sharing' below) – *please contact the IT helpdesk if this is the case, as we may need to encrypt the hard drive of your laptop*
- The Council operates a data retention policy which means that all data has a 'shelf-life'. Electronic documents and records will be automatically destroyed, but data stored on CDs or DVDs is also subject to the same policy and should be destroyed when no longer in use, or it has passed its retention date (see '6. Disposals policy' below).

3.6.2. Data storage.

The manner and location in which you store data is extremely important. Data stored on network drive and server is automatically backed up and stored offsite to aid recovery. Data stored on your PC is not backed up unless you do it, and is therefore at risk should the hard disk fail. For this reason you should not store data on your hard drive unless there is a sound business case for doing so. If this is the case, you may be required to encrypt the data on your hard drive, so please contact the IT Helpdesk.

Every user has a secure personal drive on which to store personal data, your Y: drive. This data is backed up on a daily basis and should be used to store business data relating to your role.

You may also have a shared drive which all your colleagues have access to for storing information which you all require access to. This data is also backed up on a daily basis.

3.6.3. Removable media.

Removable media by the terms of this policy refers to storage media which can be removed from its reader device, conferring portability on the data it carries. These devices present a risk in their capability to facilitate data theft, and as a medium for introducing viruses and other malware to the Council's network.

This includes:

- USB flash drives (sometimes called USB keys, or USB sticks);
- Secure digital (SD) card and micro SD card: these cards are widely used in cameras, mobile phones, PDAs, and media players;
- CDs and DVDs.

It is the Council's policy to prohibit the use of all removable media devices. The use of removable media devices will only be approved if a valid business case for its use is presented. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Requests for access to, and use of, removable media devices must be made to the IT helpdesk. Approval for their use must be given by a Director or Head of Service.

Should access to, and use of, removable media devices be approved the following sections apply and must be adhered to at all times. All removable media devices and any associated equipment and software must only be purchased and installed by the IT Section. Non-council owned removable media devices **must not** be used to store any information used to conduct official Council business, and **must not** be used with any Council owned or leased IT equipment.

The only equipment and media that should be used to connect to Council equipment or the Council network is equipment and media that has been purchased by the Council and approved by the IT Manager.

3.7. Remote access to systems

Work is now recognised as an activity, not a place and therefore the locations in which work is carried out can be many and varied. The nature of local government services means that “work” has always been carried out away from the office, particularly if the role involves dealing with the public at their business or residential premises. There are a wide range of staff that already spend a considerable amount of time working remotely from other members of the team.

The Council’s flexible working policy sets out the criteria and arrangements for flexible working:

<http://vindex/HR/Documents/Home%20and%20Mobile%20Working%20Policy.pdf>

Requests for remote access to the established will be assessed using a consistent set of criteria regardless of the remote location:

- Physical security of site;
- Provision of firewall, or firewall router/modem;
- Suitability of ISP – this is of particular relevance if remote site is outside of UK.

3.8. Connecting to the Council’s network

This policy defines how the Council’s IT Team manages access to its LAN for both employees and third parties. This policy is designed to provide a reasonable level of security whilst still enabling everyone to work effectively. It outlines the Council’s policy on the usage of not only traditional workstations and notebooks but also the increasingly popular more esoteric portable devices commonly referred to as PDA’s ‘smartphones’, USB memory sticks, MP3 players etc

- Firstly, only authorised devices are permitted to connect to Maidstone Borough Council’s network and its resources. This policy is equally applicable to interactive and remote sessions and applies at all times and to any Council access point.
- Authorisation must be obtained in writing from an authorised source. Authorised sources include the IT Manager, Technical Support Team Leader and Network and Security Officers. No other party is permitted to grant access under any circumstances.
- Non council employees including visitors and third party consultants are strictly forbidden from connecting PC’s, notebooks or any other devices to any Council network point or wireless access point without prior written authority.
- The Council does not lock down individual network cards to specific switch ports however it does configure WLAN access to MAC addresses.
- No employee or third party is permitted to connect an unauthorised PDA, smartphone, portable network capable or storage device to any Council network point or device without prior authorisation. This specifically includes but is not restricted to any devices that connect using USB, serial, Infra red, firewire or device cradles & blue-tooth.

3.8.1 Third-party access

- Suppliers and contractors requiring remote access to systems within the Council must connect using an approved Virtual Private Network (VPN) client.
- The Council does not permit (unless there are exceptional circumstances agreed in advance) any connection to its systems via directly attached analogue or ISDN modems. All connections must be made through the Council perimeter firewall via a monitored and securely encrypted VPN tunnel
- Non-Council devices connecting via this method must be agreed in advance and a full disclosure of its configuration must be made.
- Non-Council equipment connecting through a VPN tunnel must adhere to a minimum standard of protection agreed in advance. This will include for example the requirement that all connected equipment be running up-to-date anti-virus software. It must be free of malware (worms etc) and comply with any configuration requirements asked of it by the Council. Failure to comply with this requirement will result in disconnection.
- For site-to-site VPN tunnels workstations must be on an isolated segment and must not allow bridging to the third party internal network (split tunnelling)
- Third parties are expected to protect any Council supplied accounts and passwords and only issue them to nominated individuals.
- VPN accounts will be disabled by default and only re-enabled by request. The requester will be required to confirm their credentials and will be a named party. Once the account is enabled it will be configured to expire within an appropriate time (usually 24 hours).
- Login passwords on clients must not be saved or cached but entered by the operator with each use.
- Passwords will be set to expire as per the Council's standard security policy (currently thirty days).
- Connectivity to Council systems must only be made for the purpose of conducting Council business or technical support (including maintenance and system upgrades) and only during agreed hours.
- Third parties must agree to access only those systems deemed necessary to complete their work. Any attempt to access other systems for any reason whatsoever will place that organisation and individual in breach of this policy and be liable to immediate termination of connection.
- Third party accounts will be issued with the appropriate rights and permissions necessary to complete their task. Occasionally, local administrative rights and permissions will be required. Third parties are expected to respect the privileges and trust they have been granted and ensure that any reconfigurations, installations, upgrades or changes of any kind are notified to Technical Support PRIOR to them being applied. Due diligence must be taken at all times whilst connected to Council systems and any mishaps immediately reported.
- Under no circumstances will Domain Administration rights and permissions be granted.
- The configuration and establishment of the initial VPN tunnel, i.e the authentication method, encryption and tunnel type must be appropriate to the task. Requests to permit unrestricted access to multiple clients using DHCP for example will be refused. MAC addresses and static IP's must be provided where appropriate to enable traceability and accountability.

Internet and email use.

The purpose of this element of the policy is to ensure the proper use of email and the Internet and make users aware of what Maidstone Borough Council deems as acceptable and unacceptable use of these information and communication tools.

In using the e-mail and internet facilities every user has a responsibility to maintain and enhance the council's public image and to use these facilities in a professional manner.

3.9. Definitions.

The council now permits more extensive use of the internet and e-mail facilities in order to benefit users and to enhance the working environment. Users are advised that external e-mails are formal communications from the council and will be treated as such by recipients. Every care should therefore be taken in writing them with the same importance being attached to them as to a formal letter. For the purposes of this policy, the term 'access to the internet' means access to the internet:

- from any of the council's premises and property;
- from any remote site, e.g. from a private house;
- from any premises not deemed council premises, where access is via the council's internet service provider (ISP);
- via any council provided ISP;
- via any council owned equipment;
- via any personal equipment where access is via the council's or council provided Internet Service Provider (ISP).

Risks associated with the internet and e-mail usage include:

- access to or use of inappropriate or illegal sites or material;
- security of the council's network and associated systems;
- waste of computer and staff resources;
- breach of copyright;
- actions for defamation, unlawful use of data, breaches of confidentiality etc;
- adverse impact on the provision of services to our customers;
- damage to the council's reputation.

3.10. Conditions of use.

Access to the internet is permitted using only the facilities provided for this purpose, and using the designated ISP. Any unapproved connection to the internet will be deemed a breach of the internet policy and IT security policy and may lead to disciplinary action being taken. Users must comply with all the relevant legislation and the code of conduct which is published on the Intranet.

- Users must not use any 'chat' facilities or breach the copyrights of material or deliberately propagate any virus;
- Users must ensure that PCs are locked when left unattended, and a password-protected screen saver activated whenever a PC is left unattended - any misuse by a third party will be attributed to the

username and password of the 'logged on' user and any disciplinary action may include action against that user;

- Users must not allow others access to the internet and e-mail via their user ID and password;
- Under no circumstances should individuals divulge their passwords to anyone else. Passwords should not be written down in case they are read and possibly used by someone else. If a user ID or password is disclosed the password must be changed immediately.

Users must remember that access to the internet and external e-mail facilities during working time is solely to assist users in performing their duties at work. **Private use is only permitted in an user's own time**, and is still subject to the terms of this policy.

It will be the responsibility of each individual to ensure that the use of internet facilities:

- within their work time, is relevant to and appropriate to the council's business, and is within the context of the user's responsibilities;
- within their own time, is subject to the rules contained within this document.

In case of any doubt about the permitted use of the internet, users should seek further guidance from the IT Helpdesk. **Any misuse of the internet or e-mail may be subject to disciplinary action.**

3.11. Use of the internet.

All users are authorised to use the internet for the purposes of their work and will be allowed access to the internet at work (or at home for those people working at or from home), in their own time subject to the overriding requirement that the council's service to the public must not be compromised.

The following basic rules must be observed. Usage must be appropriate, i.e. not excessive and not of a nature that might cause offence or bring the council into disrepute. The following are examples of inappropriate usage. However, this is not an exhaustive list. Further examples are given at the end of the document.

- a. Users must not use the council's network or computing resources to access, acquire, store, transmit, edit, display, view or download material that may be deemed to be:
 - sexually explicit, obscene or pornographic;
 - racial or discriminatory;
 - libellous or defamatory;
 - hateful, inciting or depicting violence;
 - illegal or may lead to a criminal prosecution of any person;
 - otherwise objectionable material.
- b. Users must not download **any** software. This may be done by the IT Section on behalf of users by contacting the IT Helpdesk. All requests must conform to the ICT strategy. Contact the IT Section for further details.

- c. Users must not use the council's internet facilities to download entertainment software, e.g. games, video, music or screensavers, or to play games against other opponents over the internet.
- d. Users must not use the council's internet facilities to take part in online gambling.
- e. Users must not use the facility for their own business purposes, or private commercial activity.
- f. Users are not permitted to visit social networking sites (such as Facebook and Bebo) during office hours.

NB: Users who are required for council purposes to undertake any access which is generally deemed inappropriate must have the **express** prior written permission of their line manager to do so.

Where organisations accept orders for goods and services via the internet the facility may be utilised for the council's business purposes providing it complies fully with the council's contract and financial procedure rules. Before committing the authority users must have the necessary appropriate authorisation from their line manager.

It will be the responsibility of each user and manager/supervisor/team leader to ensure that:

- time is not wasted on unproductive access to the internet;
- time spent browsing the web is not excessive;
- inappropriate websites are not visited; and
- Personal use only occurs in the user's own time.

3.12. Use of email.

E-mail communication using the council's network or computing resources becomes the property of the council, and could also be the subject of Freedom of Information search requests. The use of the council's resources for personal gain or for any purpose that is illegal, contrary to the council's policies for general conduct or which is known to be contrary to the council's interest is prohibited, and may lead to disciplinary action and in extreme cases to dismissal.

Access to e-mail must be via the council's chosen e-mail application. E-mails should be concise and not have lengthy or large attachments. They are formal pieces of correspondence from the council and should be treated as such.

All users should be aware that financial and contract procedure rules and all rules of the council apply to all business transactions conducted by e-mail. Before committing the authority, users must have the necessary appropriate authorisation.

Communications will be monitored for a variety of reasons as explained below. Users should not assume electronic communications are totally private. Users should communicate confidential data in other ways.

The e-mail facility must not be used for inappropriate purposes, i.e. of a nature that might cause offence to others or bring the council into disrepute. The following are examples of inappropriate use. However this is not an exhaustive list. E-mails should not:

- be used for transmitting, retrieving or storing any communications of a discriminatory, harassing, obscene or pornographic nature, or for advertising such materials;
- have contents which may be considered by the recipient as derogatory or inflammatory in relation to race, age, disability, religion, ethnic origin, physical attributes or sexual preference;
- contain material that may be classed as harassment, e.g. material of an aggressive, abusive, bullying, offensive, libellous, derogatory or anti-social nature, or may reasonably be considered in bad taste;
- be used to communicate extreme views which could be to the detriment of the council or its reputation;
- be open to misinterpretation;
- be used to respond angrily or defensively to perceived criticism or derogation;
- contain any information/data that contravenes the Data Protection Act 1998;
- contain anything that may bring the council, its members or officers into disrepute;
- be used to participate in chain or pyramid letters or other such schemes.

If e-mails that are received contain the following, or similar requests, such requests must be adhered to. Permission to do otherwise must be obtained from the originator:

- This e-mail and any file or link transmitted with it is confidential, subject to copyright and intended solely for the use of the individual or entity to which it is addressed. It may contain privileged information. Any unauthorised review, use, disclosure, distribution or publication is prohibited.
- If you have received the e-mail in error please contact the sender by reply e-mail and destroy and delete the message and all copies from your computer.

When sending an e-mail consider the recipient and ensure they will be able to read the format you are sending. Users should avoid conversational e-mail. They are not a substitute for the telephone; the general rule is that if you can use the telephone, do so.

E-mail should not be relied on to provide a permanent record, unless they are saved into the Council's document management system.

Users are allowed reasonable use of the Council's e-mail facility for personal use, in their own time, if they observe the rules set out in this section. These rules apply equally if the facility is used on council premises, or remotely, e.g. from a private house or other premises. Such use is subject to the requirements of the service, and at the discretion of the user's line manager.

Some users may receive unsolicited email (SPAM). The Council has in place software which attempts to limit the impact of SPAM; however it is not 100% effective. If users receive SPAM email, they should forward the email onto Spamwatch@maidstone.gov.uk and immediately delete the email.

The Council has implemented an email archiving facility to reduce the amount of email storage required. If you wish to have access to your archived emails, contact the IT Helpdesk.

4. Monitoring.

The council has a number of specific and general duties to monitor how the organisation operates and how its individual users perform while at work. Individuals also have a right to privacy.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 apply to the use of the internet and e-mails. The Information Commissioner has also issued a code of practice on the carrying out of lawful monitoring of internet access and e-mail use at work, taking account of the provisions of the Human Rights Act 1998, the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000. The council will adhere to this guidance and the relevant rules and regulations while ensuring that the council's interests are safeguarded.

Lawful monitoring is undertaken to safeguard users as well as protect the interests of the council and of our customers. It is also undertaken so that managers can ensure the smooth running of their section/departments, and to enable the management of resources and the council's gateway. Monitoring of e-mails (both incoming and outgoing), and the use of the internet, will be undertaken so that the council can plan and manage its resources properly. Monitoring will also ensure that users act only in accordance with policies and procedures such that standards are maintained, to prevent and detect crime, and to investigate unauthorised use.

4.1. Internet monitoring.

All internet usage is recorded via an automatic logging system; this system logs the time of access, the length of time the internet was accessed and the name or IP address of each site visited. The system also logs attempts to access those sites which are blocked.

Reports will be available to managers identifying the length of time spent by their staff browsing the internet, and the categories of sites visited. Where required by managers more detailed reports can be provided by the IT Section by contacting the IT Helpdesk. Where there is suspicion of misuse/abuse of the internet or resources, further investigation will be undertaken in accordance with the code of practice.

4.2. Email monitoring.

All users who use external e-mail must be aware that external e-mails received or sent are copied and stored in order to safeguard the interests of the individuals and the council should any allegations be made against the council or its staff.

There is no systematic or continuous monitoring of such e-mails and they are not accessed/read unless absolutely necessary during the course of an investigation or complaint. Access can only be gained with the express permission of a director or assistant director, and all such access will be carried out lawfully and in accordance with the legislation outlined above.

4.3. Discipline.

Users should take note that breaches of this policy may result in disciplinary action being taken, and in extreme cases, dismissal. All disciplinary action will be undertaken in accordance with the council's disciplinary procedures which are published on the Intranet.

The procedure gives examples of acts which would ordinarily constitute gross misconduct. This list is not exhaustive. The following are those which could relate to breaches of this policy, and which could result in instant dismissal:

- Conduct which results in a serious breach of confidence in the user;
- Action which brings the council into serious disrepute;
- Sexual or racial abuse or harassment;
- Viewing/forwarding/storing images or content which could be considered pornographic, obscene or offensive;
- Corruption, fraud, falsification of records, e.g. abuse of the Computer Misuse Act 1990;
- Misuse of the council's property or name.

4.4. Legitimate and illegitimate use.

E-mail and the internet enable users to have more ready access to information and colleagues. It can transform the way in which jobs are done and can enrich the working environment. It is therefore to be welcomed and used wherever and whenever possible to streamline communication. The following system has been produced to help users make effective use of the medium.

4.4.1. Legitimate use:

- Communicating on behalf of the council or as an aid to pursuing tasks within your job description or remit.
- Conducting research into work related matters.
- Personal research of the internet or sending personal e-mails in own time.
- Personal purchases of goods and services via the internet in own time e.g. booking personal holidays, flights etc.

4.4.2. Do not engage in these activities:

- Use e-mail for gossip, or to libel others or other organisations.
- Visit social networking sites.
- Make statements purporting to represent the council when they are personal views.
- Make derogatory remarks or express derogatory opinions regarding the council, its officers or members.
- Knowingly infringe copyright or intellectual property rights.
- Knowingly send or receive anything that is illegal or fraudulent.

- Knowingly send or receive anything that is obscene, sexually explicit, defamatory, racist or homophobic in nature, or any material which is intended to cause the receiver or anyone who sees the material harassment, alarm or distress.
- Use the facility to pursue personal business interests/commercial activity.
- Allow anyone else to use your user ID or password to gain access to your internet or e-mail account.
- Knowingly engage in any activity that threatens the integrity or availability of the council's systems.
- Attempt to break (hack) into any area, whether inside or outside the council.
- Engage in any online gambling or play games with other opponents over the internet.
- Download any entertainment software, games, music, videos, screensavers or any software/applications.

5. Disposals policy.

It is the policy of the Council to ensure that any data of either a personal nature (as defined by the Data Protection Act) or confidential nature that is no longer required is dealt with in a secure manner before the equipment or data is relocated within or disposed of by the Council. In order to achieve this objective all data stored in digital form must be disposed of in accordance with this procedure.

IT equipment disposals should, where possible, ensure that best value is obtained and also address Local Agenda 21 issues, and WEEE standards to minimise any environmental impact resulting from the disposal of equipment (for example from toxic and contaminating materials such as lithium and lead which are present within computer equipment). For further information on WEEE:

<http://www.dti.gov.uk/sustainability/weee/>

The policy applies to all computer hardware, including printers, VDUs, etc.

5.1. Data and document disposal procedure.

Information selected for disposal must be redundant or have been copied for use elsewhere, for example on a network drive accessible by members of the section which originated the data.

The information must no longer be required for operational, accounting, functional, legal, training, security or contractual reasons. Please refer to local 'data owner' data retention and disposal policy guidance.

Data on fixed or removable hard drives should be destroyed centrally by the IT Section by use of an appropriate utility program. Data on tape, cartridge, DLT or DAT tapes should be overwritten by appropriate software or the item cut into sections before disposal. Alternatively the items may be sent for secure disposal via the IT Section. Floppy disks and CD ROMS/DVDs should be cut into quarters before disposal.

Documents containing personal data or confidential information should be shredded or placed in confidential waste sacks.

5.2. Equipment disposal procedure.

The reasons for disposal of each item must be identified, justified, documented and authorised by the relevant Section Manager. These will be noted on the equipment inventories where appropriate. All disposals must be notified to the IT Manager and the asset register must be updated accordingly by the IT Section.

For items which are in working order or are repairable, depending on the nature and estimated value of the item, an external purchaser should be considered in accordance with tendering and contract procedures under the provisions of Standing Orders.

Where items are deemed to have some intrinsic value, and there is no potential for donation to the voluntary sector, consideration may be given to selling items on the internet, for example on eBay. This is only suitable for items where there are no software licensing issues and no implications for Council data being compromised – an example might be networking equipment.

Where there is judged to be no market interest, the items should be disposed of by other means eg internal sale, donation to other organisations (eg charitable or educational), or scrapped. Where items are to be sold internally, notices inviting sealed bids should be placed on notice boards and advertised using email.

All equipment must have an electrical check carried out prior to sale.

Any equipment is 'sold as seen' and no IT support will be offered after sale.

Any software provided by the Council on equipment being disposed of must be removed in accordance with the software licence.

Defective items (which cannot be wiped) and judged to be beyond economic repair must have any fixed disks removed and rendered unusable (for example by physical damage). Environmental considerations, and the advice of the Recycling Officer, must be taken into account when deciding on the manner of disposal. The Recycling Officer should be contacted for the latest recommendations from the DTI concerning re-use and refurbishment companies, and county wide arrangements for scrap via Local Agenda 21 networks and WEEE compliance.

Document is Restricted

By virtue of paragraph(s) 1, 2 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

By virtue of paragraph(s) 1, 2 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

Document is Restricted

Document is Restricted

By virtue of paragraph(s) 1, 2 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted