ABERDEEN
CITY COUNCIL

ICT ACCEPTABLE USE POLICY

ISSUE 11 – 19th June 2014

DOCUMENT CONTROL SHEET

Issue / Amendment	Date(s)	New/Amended Pages	Originator
			Approved By
Issue 8 (Approved by Continuous Improvement Committee)	21 April 2009	Front cover, 3-16, 18 and 19	ICT Security
			R Atkinson
Issue 9 – Draft Updated policy as resulting from 2009-2010 Annual Review	15 March 2010	Front cover, 3, 5, 7-8, 10-13, 15 and 16	RT Guild
			S Massey
Issue 9 – to Corporate Policy & Performance Committee (for information)	29 April 2010	Front cover, 3, 5, 7-8, 10-13, 15 and 16	RT Guild
Issue 9 - accepted by Corporate Policy & Performance Committee	29 April 2010	Front cover, 3, 5, 7-8, 10-13, 15 and 16	RT Guild
			R Atkinson
Issue 10 – to Corporate Policy & Performance Committee (for information)	18 April 2013	Front cover, 5-6, 8-12, 14 and 17-19	RT Guild
			S Massey
Issue 10 – accepted by Corporate Policy & Performance Committee	18 April 2013	Front cover, 5-6, 8-12, 14 and 17-19	RT Guild
			S Massey
Issue 11 – to CMT for approval	April 2014	Front cover 5, 7, 8, 9,11 and 12	S Skidmore
			S Massey
Issue 11 – Accepted by Finance, Policy and Performance Committee	19th June 2014	Front cover 5, 7, 8, 9,11 and 12	S Skidmore
			S Massey

Controlled Copy Number:

1 of 1

Document Status:

Final

CONTENTS

Appendices:

1. Introduction

1.1 Aberdeen City Council ('the Council') recognises the benefits of Information and Communications Technology ('ICT') and encourages the use of ICT equipment, systems and services in all aspects of its business. While email, the Zone intranet and the Internet are essential workplace tools, allowing employees unlimited access to these and other systems carries risks for employers so a policy setting out clear principles on ICT use is required to minimise those risks. This helps to ensure that communication resources are not unduly spent on non-work related activities and, thereby, performance/productivity does not suffer.

1.2 It is important that the use of **ICT Resources** is regulated, to ensure that the Council complies with relevant legislation, regulatory codes of practice, its own corporate governance requirements, equal opportunities and anti-discriminatory policies and ICT best practice. The Council has developed this ICT Acceptable Use Policy (ICT AUP) to set standards and provide **Users** with clear instruction and guidance on what constitutes acceptable and unacceptable use. It is important to note that specific systems and/or services, as provided to the Council by various external service providers, have additional policy-compliance requirements associated with them (based on the individual service providers' agreed terms and conditions of use).

1.3 All **Users** of the Council's computer systems and/or services are expected to comply with this policy when making use of the Council's **ICT Resources**. It should be understood that logging on to the Council's data networks and computers is intended to signify acceptance of this policy. A message is displayed at the point prior to actual logging-on to use **ICT Resources**. This message states that prior to any person logging-on and/or using the Council's ICT Resources they must:

- Be authorised to do so (in keeping with the Scope (of applicability) to the ICT AUP);
- Understand and accept the terms & conditions of the ICT AUP;
- Be aware that accessing and/or using **ICT Resources** may be monitored;
- Be aware that unauthorised access to and/or improper usage of Council's **ICT Resources** may result in disciplinary action and/or criminal prosecution.

It is therefore important to state that if individual **Users** have concerns about their ability to comply with this policy, they must not logon or use **ICT Resources** and raise their concerns with their **Line Manager**. All such concerns must be resolved to the Council's satisfaction, with affected **Users** then being prepared to accept the Council's terms and conditions of this policy before proceeding further. Furthermore, the additional policy-compliance requirements described in the attached appendix must also be complied with (as-and-where appropriate) by related **Users**.

2. Review

2.1 This policy is reviewed annually and when otherwise required; and updated as necessary.

3. Scope and Definitions

3.1 This Policy applies to all **Users** who have access to **ICT Resources** provided by the Council, meaning all:

- Employees (except Schools' teaching staff (who have their own policy));
- Agency workers;
- Contractors (subject to any relevant provision in their contracts);
- Employees of Trusts, agencies and companies that use the Council's **ICT Resources**;
- Students and volunteers (where undertaking work experience or similar).

Managers should make staff for whom they have day-to-day line management responsibility aware (via team meetings/briefings) of the ICT Acceptable Use Policy & its obligations and any additional ones which might arise from periodically published ICT Security guidance/advisories.

3.2 For the purposes of this Policy, **ICT Resources** means all elements of the Council's ICT infrastructure, comprising:

- Data network and main computer systems;

- PCs and portable computers (e.g. laptops, notebooks, tablets and mobile / smart devices;

- Peripheral computer equipment (e.g. printers, scanners, digital copiers, external drives and portable media);

- Software and other services (including e-mail and the Internet) accessed through any of the above;

- Data and information assets accessed through any of the above (regardless of where they are located or how they are processed or communicated).

4. General Responsibilities

4.1 **Users** must therefore take all reasonable steps to comply with this Policy and should endeavour to ensure that **ICT Resources** are used effectively, safely and securely and that all reasonable precautions are taken to avoid loss, theft and damage.

4.2 All persons covered by the scope of this policy must recognise that information is one of the Council's most important assets. There could be extremely serious consequences if it were to be lost, stolen, compromised and misused. The methods employed to protect information must always be commensurate with its importance to the Council and any confidentiality or sensitivity associated with it (particularly in respect of people that such information might relate to). It should also be noted that information assets might be irreplaceable and that severe criminal or civil law penalties could result, with such penalties affecting those covered by this policy as well as the Council itself.

4.3 Where **Users** are authorised to access the Council's main email system over the Internet (using non-Council computers and services), they must not:

(a) Access messages or attachments which they know or suspect contain confidential or otherwise sensitive data/information, and nor should they open attachments regardless of the perceived sensitivity of any data/information. All such access should only be done using Council-owned computers and communication services.

(b) Use GSX. Further restrictions on GSX usage are shown below at Appendix 1.

5 Rules of Acceptable Use

5.1 **Users** must familiarise themselves with and observe the following Rules of Acceptable Use, which apply to all **ICT Resources:**

(a) **Users** must not request, create, adapt, access, use, retain or send (whether as plain text, jokes, cartoons, images or any other form):

- Material which is, or might be considered illegal, obscene, indecent or pornographic (including any material which depicts nudity or is otherwise sexually explicit);

- Material which promotes any form of deception, defamation, discrimination, harassment, maliciousness, misrepresentation, racism, victimisation, intolerance or violence;

- Material which might be considered offensive (on grounds of sex, race, disability, religion or belief, sexual orientation, appearance, gender or otherwise).

(b) **Users** must never impersonate others or use another person's login when using **ICT Resources**. However, it may sometimes prove necessary for systems to be accessed by the Council's management, nominated representatives and/or the Police (in particular circumstances), and for the contents of a **User's** ICT accounts to be examined. The Council reserves the right to do this in circumstances such as:

- **Users'** absence through illness, holiday etc. – with someone having to temporarily carry out their duties, with related responsibilities having been assigned beforehand (in the case of instances of absence which can be forecast);

- **Users** having left the Council's employment or having transferred to an unrelated post within the Council;

- The Council involving the Police, for the purposes of the prevention or detection of crime or in the interests of national security.

Furthermore, **Users** must advise their **Line Manager**, prior to leaving their post, of their **User** account details and any important information held in their accounts (in order that such information can be retrieved and the accounts closed).

Should another authorised person require access to **Users'** accounts during periods of absence which couldn't be forecast, they should record the purposes for which they require access, noting the applications accessed, maintaining a log for the period which they required access.

If it does become necessary for **Users'** ICT accounts to be accessed by other than the related **Users**, then a **Senior Manager** within the relevant Service must ensure individual records of all related activities are created. The ICT Helpdesk should then be requested to either delete the account(s) or temporarily change the respective **Users'** password(s) once there is no further need to access such accounts. A **Senior Manager** must also ensure that their related **Users** are made aware of what has happened and that they need to change default passwords to ones of their own choosing.

(c) **Users** must not knowingly or carelessly expose the Council to avoidable risk through the introduction of computer spyware or viruses. These can be introduced in a variety of ways; therefore all smart devices, CDs, DVDs, USB Memory sticks, e-mail messages and attachments must be checked for viruses before being installed, opened or used. Whilst Council's antivirus/antispyware security system will automatically check e-mail for the presence of viruses/spyware, individual **Users** should run the related security software on their PC or portable computer to check smart devices, CDs, DVDs, USB memory sticks etc. prior to making actual use of such portable media (in keeping with Data Protection Act and ICT Security Guidance on Protecting Data on Removable Media, Secure Scanning and Printing (as held on The Zone)). Furthermore, if there is any indication of viruses or spyware being present, or other forms of abnormal activity indicated, then it should be immediately reported to the ICT Helpdesk. The PC or portable computer should not be further used (and left in its existing state) until it has been cleared for use.

(d) **Users** must not breach copyright laws and must not:

- Access, load, run, copy or adapt licensed or unlicensed software other than in accordance with the terms of the relevant licence, where one exists;

- Download, copy or adapt any material from the Internet except that which is allowed by the copyright owner and which is for work related purposes (which includes work-related private study, as supported or sponsored by the Council);

- Load or run any software (including screensavers and wallpaper) which does not have the prior written approval of the relevant ICT Account Manager.

(e) **Users** must not alter the set-up of **ICT Resources** by adding or removing software, hardware or services. The ICT Helpdesk must always be contacted in the first instance (with related requests being subsequently considered for approval by the relevant ICT Account Manager, in order to ensure compliance with this policy).

(f) **Users** must take reasonable steps to protect confidentiality and;

- Must not access, or attempt to access, **ICT Resources** or data which they are not authorised to use;

- Must not allow unauthorised persons to access **ICT Resources** or data;

- Must not disclose any electronic or related hard-copy material, data or information which they are not authorised to;

- Where appropriate, adhere to the Data Protection Act and ICT Security Guidance on Protecting Data on Removable Media, Secure Scanning and Printing (as held on The Zone). The main premise in related respects is that **Users** must never store sensitive person-identifiable information about citizens or employees, or information that is marked RESTRICTED on anything other than Council's main computers, encrypted laptops or 256 AES self-encrypted USB memory sticks.

(g) **Users** must not use **ICT Resources** for unlawful purposes or for any other purpose that could bring the Council into disrepute or damage the effectiveness of its **ICT Resources**. This includes the use of **ICT Resources** to do any of these things by expressing opinion or providing commentary using, primarily, e-mail and the Internet (see in conjunction with 5.1a above).

(h) **Users** must comply with the Council's policies, procedures and guidance in respect of data protection and physical security.

(i) **Users** must not leave computers unattended in such a state as to risk unauthorised access to and disclosure of information. This may entail closing e-mail programs, logging-off from the computer, activating password-protected screensavers, etc.

(j) E-mail needs to be constructed with the same regard for the rules applicable to other forms of business communication, particularly as it can be considered binding in business transactions as well as being admissible evidence in court. The Council (unless negotiations by way of email correspondence are otherwise authorised by the City Solicitor or her office) does not permit it to be used for contractually-binding purposes. Email must not be used for the external communication of confidential or otherwise sensitive information (unless, in the latter case, password-protection is applied to confidential/sensitive content (which must only exist in attachments - not in covering messages)). Unless expressly stated within an e-mail or its attachments, e-mails are not intended to create, form part of or vary any contractual or unilateral obligation.

(k) **Users'** passwords must be no less than 8 characters long, must not be re-used when the need to change them arises, and be comprised of a series of alphanumeric characters (with at least one character being a special character (e.g. an upper case/sign character)).

(l) Where confidential or otherwise sensitive data/information requires to be sent over the Internet, it must be always and only be contained in password-protected attachments – with the intended recipient(s) being advised separately of what the related password(s) is/are. This requirement must always be observed in conjunction with Data Protection procedures (as held on The Zone) where related data/information is person(s) identifiable.

5.2 **Users** who wish to communicate confidential, work-related information to their trades union or relevant Council Service should prefix their e-mail message descriptions with the words 'PRIVATE E-MAIL' and then add subject-specific wording as per the following examples:

- PRIVATE E-MAIL – UNISON;
- PRIVATE E-MAIL – HEALTH MATTER;
- PRIVATE E-MAIL – EMPLOYEE PENSION etc.

This is intended to ensure that the content of such messages is not reported on as part of the Council's electronic monitoring of Users' e-mail.

5.3 **Users** should be aware that improper e-mail messages might be interpreted as reflecting adversely on both the Council and the sender. It is therefore important that all e-mails are written with the same due care and consideration as would apply to other business correspondence, by applying appropriate standards of protocol, language and style. The content of emails must comply with the Council's equal opportunities and anti-harassment policies. The distribution of chain emails or jokes is prohibited. The Council, as a public body, is subject to a high level of scrutiny and damaging e-mail messages might ultimately have to be disclosed for the Council's Managing Discipline Policy and Procedure, criminal or civil law investigations/evidence-gathering purposes. **Users** should read the Outlook Guidelines on the Zone for further advice and guidance.

6 Use of the Internet

6.1 Internet access is permitted for Council business use by all **users**, subject to the restrictions on personal use detailed under para 7.1 below, but will be controlled and monitored for excessive or improper use, use of some services, e.g. webmail and social media will be controlled and generally blocked by the Council's Internet security systems for reasons of limiting bandwidth usage and mitigating threats posed by malicious software and a warning message from our web filtering software will be displayed to the effect that the site is only available to those that are authorised. Where a business use of such websites is identified and supported by a business case then it may be permissible to gain access to these sites. In this event it is necessary to fill in a Restricted Internet Access Form, which is posted on the Zone. It needs to be completed by your Line Manager and must be countersigned by a Head of Service (this may also be a Head of Establishment in the case of schools and Community Education Centres) and submitted to the ICT Security Team, Customer Service and Performance, Corporate Governance Service. Improper or excessive use reports will be raised and issued to Managers as and when required and can be requested by managers who want to check Internet access by their Teams.

6.2 Furthermore, the Council requires that all of its employees comply with its Employee Code of Conduct and in particular the Social Media Guidance for Employees both of which can be found on the HR pages of the Zone. **Users** should also note that:

- It is unacceptable for employees to make, publish or post defamatory or generally unacceptable comments, views or information about the Council, its employees, clients or customers (including school pupils) in any medium, including Internet social networking sites.

- It is further unacceptable for employees to publish any photographs of clients or customers in/on social networking sites without first obtaining formal permission.

7 Personal Use

7.1 Personal use of **ICT Resources** is permitted with **Users** trusted to use the Internet properly and in line with the above Rules of Acceptable Use and subject to the following conditions:

- Personal use should only be undertaken in a **User's** own time so that it does not interfere with work responsibilities and effective service delivery.
- Personal use of e-mail is unrestricted, providing it is undertaken in a **User's** own time.

- Only the words '**PERSONAL E-MAIL**' should appear in the subject field of an e-mail.
- Only basic messages are permitted to be sent (i.e. attachments are not permitted).

Any **User** who abuses this trust may be dealt with under the disciplinary procedure.

7.2 Permitted personal use of **ICT Resources** does not extend to:

- Using personal Internet e-mail accounts (e.g. hotmail, gmail, yahoo);
- Retaining any personal document or file for more than 1 week (except information recorded in electronic diaries);
- Sending personal e-mail attachments;
- Subscribing to web-site services, if such subscription generates further, multiple, communications;
- Using instant messaging services or chat rooms;
- Using any application software other than that which officially exists on **ICT Resources**.

8 Monitoring

8.1 It is important that **Users** comply with the provisions of the ICT AUP. To help verify compliance, the Council monitors usage of its **ICT Resources** in keeping with the requirements of its approved Electronic Monitoring of Use Impact Assessment. Users should therefore familiarise themselves with the contents of both documents.

9 Breaches and Incidents Reporting

9.1 Where any person covered by the Scope of this policy suspects or knows that an incident has taken place, there is potential for the policy's requirements to have been breached. They should report the matter immediately to their **Line Manager** who should then report the incident in the first instance to the ICT Helpdesk in order to:

- Register the incident;

- Request additional support/information from the ICT Security Team to verify that the incident has occurred and assess any technical implications for ICT Operations

Once the incident has been verified, the **Line Manager** should further advise the ICT Helpdesk in order that the ICT Security Team can determine and implement any necessary technical and non-technical corrective & preventive action measures.

9.2 Where the incident results in Council supplied equipment, software, data or information being mislaid, lost, stolen, misappropriated or damaged, it is essential that the **Line Manager** establishes the cause as well as the consequences of any data or information being compromised or irrecoverable. The implications of such data or information being compromised could be considerable and far reaching, particularly in respect to any which relate to individual persons or groups (e.g. people at risk). The implications of data or information being misused could also extend to the Council and its Services – with the possibility of the Council being exposed to litigation as well as adverse publicity. Where data or information is involved in such incidents, the **Line Manager** must inform the relevant data or information owner.

9.3 Furthermore, the loss of ICT assets must also be reported, by the affected **User**, to the ICT Helpdesk, in order that appropriate action and escalation takes place as soon as possible following receipt of the report. Where ICT assets contain person identifiable data/information, affected **Users** should also comply with the Data Protection Breach Reporting Procedure (as held on The Zone).

Amplifying Note: ICT Security breaches and incidents are defined as follows:

- ICT Security Breaches: these are events or circumstances involving the wilful or negligent contravention of this policy which may lead to disciplinary and, as appropriate, legal action being taken against offenders.

- ICT Security Incidents: these are events or circumstances which may appear not to contravene the Councils ICT security policies, but will still require investigation in order to determine if breaches of policy have taken place and/or if other action(s) need to be taken to improve ICT security measures/countermeasures.

10 Disciplinary Action

10.1 Breaches of this policy will not be tolerated and those responsible for those breaches will be subject to the procedures set out in the Managing Discipline Policy and

Procedure. This could result in disciplinary action being taken. Serious breaches of this policy could be construed as gross misconduct resulting in dismissal without notice e.g. deliberately accessing or otherwise using pornographic or other indecent or obscene material, or participating in any form of e-mail harassment.

10.2 Advice and guidance on the application of the Council's Managing Discipline Policy and Procedure is available from Human Resources. Legal and ICT Security support is respectively provided by Legal and Democratic Services and ICT Security Team, Customer Service and Performance.

10.3 In certain circumstances, breaches of this Policy may also be a criminal offence. In these cases, the Council is required to report the matter to the police.

11 Legal Compliance

11.1 **Users** are to also ensure that they comply with all related legal/regulatory requirements - with particular emphasis on the following (as a minimum) and any amendments thereof:

Local Government (Access to Information) Act 1985. This places a duty on local authorities to actively publish certain information, although there are categories of information which are exempt. It is also of note that some information which was previously categorised as confidential at the time the Act was published may now have to be disclosed under the Freedom of Information (Scotland) Act 2002 as the sensitivity of certain subjects can reduce dramatically over time.

Copyright, Designs and Patents Act 1988. This deals with copyright and intellectual property rights and what constitutes their contravention.

Computer Misuse Act 1990. This deals with unauthorised access to and modification of computer material (with such practices being criminal offences, particularly in respect of electronic information). The Act also deals with the need to securely dispose of such computer material when it is no longer required for its intended purpose(s) by those who are/were authorised to have access to it.

Copyright and Rights in Databases Regulations 1997. Essentially as per Copyright, Design and Patents Act legislation, but including non-authorised modification to databases (which are also subject to copyright and intellectual property rights' ownership).

Data Protection Act 1998. This relates to implementing measures that will ensure the relevance, need for retention, accuracy, integrity and control over the use, handling and disclosure of personal information (although there is other legislation which can take precedence over the disclosing of personal information).

Human Rights Act 1998. This, from an ICT Security perspective, is essentially to do with the following employees' rights:

- Respect for their private correspondence (Article 8).
- Their freedom of thought, conscience and religion (Article 9).
- Their freedom of expression (Article 10).

- Their right of association and Trade Union membership (Article 11).

- Prohibition of discrimination in their enjoyment of Convention rights (Article 14).

Regulation of Investigatory Powers Act 2000. This relates to surveillance or covert monitoring that has taken place, in support of specifically authorised investigations only (as might be initiated by criminal/civil law agencies). An application to undertake a covert surveillance operation requires consideration and an assessment of any potential human rights implications prior to it being authorised.

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. This permits an employer to monitor and intercept communications for specific business purposes, such as; compliance with internal procedures, establishing facts or to ascertain that acceptable standards are being achieved. This policy informs **Users** how ICT systems are being monitored.

Freedom of Information (Scotland) Act 2002. This is to do with providing non-personal public recorded information on request, subject to specific exemptions.

Local Government in Scotland Act 2003. This, in the context of ICT Security, is essentially to do with Best Value and the need for continuous improvement.

Civil Contingencies Act 2004 and Contingency Planning (Scotland) Regulations 2005. This is to do with having Business Continuity and Disaster Recovery plans in place.

Any other relevant UK laws or directives (particularly as they apply to Council Services – individually or collectively)

Any specific security requirements stipulated by Council customers and organisations which provide electronic services to the Council.

Users should take advice from their **Line Manager** as to which of the above are applicable to their role and responsibilities.

Appendix 1 - ICT Security Requirements for other Government Systems/Services

The following policy-compliance requirements are additional to the ones shown above. **Users** should consult their **Line Manager** about these, and also be aware that access to the Council’s systems and/or services might be withdrawn if they are not complied with. Furthermore, the referred systems and/or services are only to be used for work-related purposes.

All **Users** must understand and comply with Aberdeen City Council’s (ACC’s) security rules. For the avoidance of doubt in the following’s respects, the security rules relating to Public Services Network (PSN) - i.e. Government Connect Secure Extranet (GCSX) secure e-mail and IT systems usage/non-usage which must also be taken into consideration include:

- Knowing that that the use of the PSN may be monitored and/or recorded for lawful purposes;
- Accepting responsibility for using PSN unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address;
- Must not use a colleague's credentials to access the PSN and will equally ensure that their unique credentials are not shared and are protected against misuse;
- Must protect their credentials at least to the same level of Classification/Protective Marking as the information they may be used to access (and will not write down or share their credentials other than for the purposes of placing a secured copy in a secure location – as and if required by ACC line management);
- Must not attempt to access any computer system that they have not been given express authorisation to access;
- Must not attempt to access the PSN other than from IT systems and locations which they have been expressly authorised for;
- Must not transmit information via the PSN which they know, suspect or have been advised of is of a higher level of sensitivity than their PSN domain is designed to carry;
- Must not make false claims or denials relating to their use of the PSN (e.g. falsely deny that email had been sent or received);
- Protect any material - whatever its sensitivity or protective marking (as sent, received,

stored or processed by themselves - via the PSN), to the same level as they would do with paper copies or similar material/media;

- Must not send information marked RESTRICTED or above over public networks such as the Internet unless approved encryption has been applied to it;

- Always check that the recipients of email messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain;

- Must disclose information received via the PSN only on a 'need to know' basis;

- Do not forward or otherwise disclose any sensitive or protectively marked material received via the PSN unless the recipient(s) can be trusted to handle the material securely according to its degree of sensitivity, and forwarding it via a suitably secure communication channel;

- Strive to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via the PSN (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc.) and by carefully checking the distribution list for any material to be transmitted;

- Securely store or destroy any printed material when no longer required;

- Must not leave their computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the PSN (this might be by closing the e-mail program, logging-off from the computer, activating a password-protected screensaver, etc., so as to require a user logon for activation); and where the Council has implemented other measures to prevent unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), and not attempting to disable such protection;

- Make themselves familiar with the security policies, procedures and any special instructions that relate to the PSN;

- Inform their line manager immediately if they detect, suspect or witness an incident that may be a breach of security;

- Do not knowingly attempt to bypass or subvert system security controls or to use them for any purpose other than that intended;

- Do not remove equipment or information from Council's premises without appropriate approval;

- Take precautions to protect all computer media and portable electronic devices when carrying them outside of the Council's premises (e.g. not leaving a laptop unattended or on display in a car such that it would encourage opportunist theft);

- Must not knowingly introduce viruses, spyware or other malware into the system or PSN;

- Must not disable anti-virus, anti-spyware or other malware protection provided on their computer;

- Comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that the Council informs them are relevant; and;

- Where about to leave the Council's employment, they must inform their line manager prior to departure of any important information held in their computer accounts.

Appendix 2 - Categories of Websites Blocked by the Council's Internet Security System

Adult/Sexually Explicit
Spyware
Advertisements and Popups
Web-based Email
Illegal Drugs
Chat
Criminal Activity
Gambling
Games
Hacking
Intolerance and Hate
Peer to Peer
Personals and Dating
Phishing and Fraud
Ringtones/Mobile Phone Downloads
Skype (Internet Telephony)
Social Networking sites
Spam URLs
Tasteless and Offensive
Video Sharing Sites
Violence
Weapons
Web Proxies and Translators

Important Note: Users must not use ‘anonymising’ proxy servers (sometimes called web proxy servers), in an attempt to hide web surfing activities. This type of activity is wholly contrary to Council policy and is subject to continuous monitoring (by the Internet Security System).