North Ayrshire Council
Comhairle Siorrachd Àir a Tuath

Acceptable Computer Use Policy

Version : 1.3
Date : 20/04/2015
Classification: OFFICIAL

IT Services

Document Control

Prepared By	Cathie Fraser, ICT Security Officer, IT Services
Authorised By	Version 1 - (IT and Customer Services Strategic Management Team, ICT Steering Group, Executive Committee) Version 1.1 - IT Manager
Source Location	Information Security QuickR
Published Location	http://navigate.north-ayrshire.gov.uk/EmployeeInfo/CorpPolicies/CorporateServices/ITCustServices/InformationSecurity/ACUP.pdf
Other documents referenced	See Appendix 1
Related documents	3rd Party Acceptable Computer Use Policy
Acknowledgements	Version 1.0 (IT and Customer Services Strategic Management Team, information and Records Manager, ICT Steering Group)

Document Revision

Version	Date Issued	Author	Update Information
1.0	07/08/2009	Cathie Fraser	Initial issue updated from existing policy with input from; the IT and Customer Services Strategic Management Team, ICT Steering Group, and the Executive Committee.
1.1	25/06/2014	Cathie Fraser	Removed reference to IT and Customer Services, updated logo, replaced GSx with GCSx, moved reference documents to Appendix1, updated sections: Summary 1.11, 1, 2, 3, 4, 5, 7, 14.20, 15, 18, added 14.21
1.2	19/01/2015	Cathie Fraser	Updated sections: 14.2 and 14.14.
1.3	20/04/2015	Cathie Fraser	Updated to reflect the Council's new classifications

Version Awareness

The audience of this document should be aware that a physical copy may not be the latest available version. The latest version, which supersedes all previous versions, is available only at the Published Location stated above. Those to whom this policy applies are responsible for familiarising themselves periodically with the latest version and for complying with policy requirements at all times.

Contents Listing

Policy Summary

1.1 Compliance
Compliance with this policy is mandatory. Any breach of this policy could result in disciplinary action.

1.2 Monitoring and Logs
The use of computing facilities within North Ayrshire Council is monitored and logged. This includes email, Internet and other use of internal and external systems. Backup files may be kept which permanently record this usage.

The Council may review and use these audits with good cause.

You must be aware that computer systems are regularly audited.

This means that employees must not regard either business or personal communications on the Council's facilities as private.

You are responsible for everything done under your login, don't give anyone your password.

1.3 Use of Email
Email is provided for business use only. Personal use is prohibited.

1.4 Use of Internet
Internet is provided primarily for business use. Limited personal use is permitted during authorised times, which can be located on Navigate.

Personal browsing is prohibited between 9:00am and 5:00pm, this includes during lunch time.

Education staff within schools and nurseries are limited to personal use outwith timetabled teaching hours.

1.5 Personal Equipment
It is prohibited to attach personal equipment such as, cameras, USB data storage devices, mobile phones etc. to Council machines and / or Council network facilities.

1.6 Use of Council Equipment
Council equipment can be used on any Council owned machine and / or its network facilities.

Council equipment cannot be used or attached to any non-Council owned machines and / or network facilities. Prior consideration should be given to such circumstances and other transmission methods undertaken. Advice may be sought from IT Services for specific circumstances.

1.7 Council Owned Software
Council owned software cannot be copied or taken home for use. Advice may be sought from IT Services for specific circumstances.

1.8 Personal Owned Software
Personally owned or purchased software cannot be loaded onto Council computers or systems. This includes, but is not limited to:

- games
- applications
- freeware, shareware or trialware without express approval from IT Services
- music files

1.9 Information Security
Data must be handled in accordance with the Council's "Information Classification Guidelines". This includes both paper and electronic files.

Personal, sensitive and Council sensitive electronic files must only be removed from a secure network location with authorisation. Once removed, equipment must be secured to an appropriate level with encryption, passwords or other appropriate controls being taken.

1.10 Equipment Security
Always lock your screen when away from your desk.

Accessing a system or data to which you have no authority is a breach of the Computer Misuse Act 1990 and may result in disciplinary action.

Council systems are not permitted for use by non-Council employees, e.g. family members or unauthorised colleagues from another organisation.

1.11 Disposal
All ICT equipment must be disposed of in line with the Council's ICT Disposal Procedure. Paper files must be disposed of in accordance with their classification and in line with the Council's "Information Classification Guidelines".

1.12 Communications
You are responsible for the content of all communications from your account(s), and ensuring compliance with Council policy.

It is recommended that you read The Policy in its entirety to ensure your full understanding of the content.

1 Corporate Sponsorship

This policy has been issued with the authority of The Corporate Management Team and The Cabinet of North Ayrshire Council.

The security of information, whether electronic or paper based, is taken very seriously within North Ayrshire Council. It is the responsibility of us all, as Council employees, Elected Members or any other party with access to Council information systems, to ensure compliance is adhered to with regards to securing our Information.

Communication plays an essential role in the conduct of our business. We value your ability to communicate with colleagues, clients and business contacts. North Ayrshire Council invests substantially in Information Technology and Communications systems which enable you to work more efficiently and effectively, and trusts you to use them responsibly.

Compliance with this policy is Mandatory.

2 Policy Purpose

The purpose of this Policy is to protect the information assets and systems owned, and used, by the Council from all threats, whether internal or external.

A further objective is to meet all regulatory and legislative requirements, specifically:

- Data Protection Act 1998
- Computer Misuse Act 1990
- Copyright, Designs & Patents Act 1988
- Telecommunications Act 1984
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Obscene Publications Act 1984
- Freedom of Information (Scotland) Act 2002
- WEEE Directive: Waste Electrical and Electronic Equipment
- Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA)
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- And any other relevant legislation as may be enacted from time to time

This policy forms part of the Council's initiative to act in accordance with ISO27002 Information Security Code of Practice and the HMG Security Policy Framework.

Any breach of this policy could result in potentially harming the good name of the Council and its employees and may result in disciplinary action.

3 Scope of Policy

This policy applies to all Council employees whether permanent, contract or temporary, Elected Members or any other party accessing any computer systems owned, leased or operated by North Ayrshire Council.

Please note that "Systems" refers to both physical hardware and software applications and "information" refers to Council owned information assets irrelevant of format or storage medium therefore including those both electronic and paper based.

This policy extends to the use of all such equipment, systems or information. This applies regardless of where those equipment, systems or information are located. This also applies regardless of the physical location where user access, connections or access to information originate.

Where third (3rd) party access to NAC computer systems has been approved, it is the responsibility of the engaging Service to ensure compliance with the Councils 'Third Party Use of Council Resources Guidelines'; including securing written acceptance of the 3rd party version of this policy and providing notification to IT Services of this acceptance.

4 Clarification of Policy Contents

In the event of an issue arising from an interpretation of this Policy, clarification should be sought in the first instance from the IT Manager.

5 Publication of Policy

This Policy will be published on the Council's Intranet and any amendments or revisions will be notified to all staff, Elected Members and 3rd party users via electronic means where possible.
Services will manage notification for their staff where electronic notification cannot be guaranteed.
Services will manage notification to 3rd parties where

- previous notification of their compliance has not been lodged with the ICT Security Officer
- lodged notifications have expired and not been re-submitted to the ICT Security Officer

All personnel accessing North Ayrshire Council systems or information are required to agree acceptance of this policy at periodic intervals as determined by the Council.
Acceptance indicates full understanding and compliance with the requirements of this policy and others mentioned therein. It should be noted that this policy forms part of the offer of employment to all new employees.
A review will be undertaken on a biennial basis and content will be updated as appropriate.

The Policy

6 Software including Copyright

6.1 Copyright law, which governs the use of intellectual property, including software, is very straightforward – it is illegal to copy a piece of software unless expressly permitted by the copyright holder. Staff therefore may not copy, retrieve, modify, distribute, broadcast or forward copyrighted materials.

6.2 Legitimate copies of software will be provided to all users who require it, subject to the necessary authorisation having been obtained.

6.3 Council employees are not permitted to make copies of any software or any other copyrighted material. Where devices with the ability to record are made available, this is for the express intention for the copying of material on Council business that does not infringe Copyright or any other UK Legislation.

Employees are not permitted to use or install any of the following on Council computer equipment:

- unauthorised software
- unlicensed software
- illegally reproduced software
- software purchased for home use
- games or screensavers
- developed programs or applications of any kind without express approval from IT Services
- freeware, shareware or trialware without express approval from IT Services
- music files without express approval from IT Services

6.4 All software must be purchased through IT Services, unless prior express authorisation has been agreed. Only staff and 3rd parties authorised by IT Services, will be permitted to load programs on relevant computers or servers, including upgrades to existing applications, wherever published. The Service Level Agreement with Education allows Teaching staff and ICT Technicians within schools to load Educational Software, from a secure and trusted source, within the school environment. Teaching staff and ICT Technicians must also comply with copyright legislation.

6.5 Employees must not give any Council software to anyone out-with the organisation, including clients, customers, 3rd parties and family members, without express authorisation from the IT Manager.

6.6 IT Services will maintain a register of all software procured through them. Services must maintain a register of software that they have procured. All licences and media will be held centrally or in locations approved by IT Services. With agreement from IT Services, manuals may remain with users, and where permitted by the supplier, a copy of media left on site, in the charge of the identified local responsible person.

6.7 Council software or data is not permitted to be taken home and loaded onto any home computer.

6.8 All software, information, databases and programmes developed for and/or on behalf of the Council by employees during the course of their employment remains the property of the Council. Duplication or sale of such software without prior consent of the Council will be an infringement of the Council's copyright and may lead to disciplinary action.

7 Data Protection Act

Council responsibility and registration under the Data Protection Act 1998 is maintained by Democratic & Administration Services. Staff should be aware of their responsibilities when processing personal and sensitive data relating to any living individual (including names, addresses and telephone numbers). Further information can be obtained from the "Guidelines to the Data Protection Act" on Navigate.

8 System and Information Security

8.1 All Council staff and Elected Members are responsible for the reporting of security incidents through the Council's ***Reporting of Security Incidents Policy***.

This policy should be used to report incidents including:

- threats from viruses/worms and malicious code
- any risk, or actual theft of hardware, software and data
- any unauthorised access and/or editing of data
- the loss of data, whether accidental or deliberate
- any unauthorised or incorrect transmission of data in breach of Council policy
- maintenance of system security

8.2 Employees should not disclose any information relating to the Council's IT facilities to other staff or anyone outside the Council, without express permission from IT Services. Any telephone canvassing for information should be passed directly to IT Services.

8.3 Data should be saved on a network drive rather than on a hard disk of a personal computer whenever possible, to ensure inclusion in Council backup procedures for data. Locally stored data is the responsibility of the user; this includes the maintenance of a backup routine and the assurance of all aspects of data security for that information.

Personal, personal sensitive and Council sensitive data should not be stored on any hard disk of a personal computer or external device without it being secured to an appropriate level with encryption, passwords or other appropriate controls being taken. Authorisation from the Data Owner e.g. Head of Service or Senior Management must also be acquired for the data's removal. This type of data should not be copied to, or retained on, external media including USB devices and optical media (cd's, dvd's etc), when this can be avoided. Data removed from a secure network is the responsibility of the user; this includes the device used as well as the protection of the data. Users must be aware that the removal of files from the secured network environment results in the loss of all network applied security.

The Councils 'Information Handling Guidelines' must be adhered to.

8.4 The responsibility for all data on network servers lies with the Systems Administrators, who will ensure that regular backups are performed and stored off site. All servers located at Cunninghame House are administrated by IT Services staff. Services' server administration is the responsibility of departmental system administrators.

8.5 All computer related equipment must be purchased through IT Services, unless prior express authorisation has been agreed. Use of non-Council owned equipment is prohibited, either via attachment to Council equipment by any method, or on the Council network, and should not be used to access any Council data or information.

The use of non-Council owned equipment outwith Council premises to access Council data and information must be authorised by the Head of Service and advice sought from IT Services for instances when this is achievable and any precautions to be taken.

8.6 All information and data records, whether electronic or paper based, should be included within a Service Information Asset Register, taking into account the Council's 'Information Asset Register Guidelines'.

8.7 Where Council data/information is exposed to non-NAC persons, the Service undertaking this sharing is responsible for ensuring that the appropriate data protection and acceptable use contracts have been secured.

8.8 Staff should be aware of retention schedules related to information and data; these should be applied as appropriate and in line with the Council's Records Retention Schedule.

8.9 Staff should be aware of the requirements in managing staff access to information and data. Services should refer to the Councils 'Managing User Accounts' at all times within their systems. After notification of a leaver, unless otherwise indicated, user accounts and data within IT Services' managed systems, e.g. personal network drives and email systems will be permanently deleted after a period of 4 weeks.

9 Password Security

9.1 Employees must not disclose any system Usernames, unless to authorised Council staff for admin work to be undertaken, and/or Passwords to any other person. This includes the format of login account names to external parties.

9.2 Passwords should not be written down except in exceptional circumstances with agreement from the data owner and where effective physical security arrangements prevent disclosure.

9.3 Passwords should be hard to guess while taking into account the Council's 'Password Guidelines'.

9.4 Passwords should be changed at regular intervals whenever possible. Systems should be configured to force password changes every 30 days.

10 Physical Security

10.1 Computers must never be left unattended while signed-on. Users must log out or ensure use of the Windows lock screen saver by using the Ctrl, Alt and Del keys or by using the windows key and L.

10.2 You must not deliberately attempt to access a system or data to which you have no authority. This is a breach of the Computer Misuse Act 1990 and may result in disciplinary action.

10.3 Equipment should not be left unattended in **any** location outwith secure Council offices, and never left in plain sight in unsecured office areas, cars, at home, public areas, public transport or hotels.

10.4 Council systems are not permitted for use by non-Council employees, e.g. family members or unauthorised colleagues from another organisation. Systems may not be used for any purpose other than Council business without the express permission of the Corporate Director or Head of Service, and IT Services after a security review of the purpose. Where personnel from other organisations require access to NAC systems this must be authorised and not permitted until the applicable contracts are in place. Refer to the Councils 3rd Party Access to Council Resources Guidelines.

10.5 Only members of IT Services, staff and 3rd parties authorised by IT Services, are permitted to move any IT equipment connected to a network, whether internally within an office or to another location. Managers must ensure that inventories are updated in accordance with the Council's Financial Regulations.

10.6 Council owned and supplied peripherals, e.g. USB devices of any kind (memory sticks, digital cameras, PDA's, USB drives etc.) may be used within any Council owned computing or network environment. Where the use of such a peripheral or device involves the moving of Personal, personal sensitive or Council sensitive data the device must be secured to an appropriate level with encryption, passwords or other appropriate controls being taken. Advice may be sought from IT Services.

Encryption solutions must be approved and supplied by IT Services. Staff must be aware that encryption provides security to data in transit from unauthorised access; it does not provide virus protection to the device.

Council owned and supplied peripherals may not be used outwith Council computing or network environments. Prior consideration should be given to such circumstances and other transmission methods undertaken, e.g. email. Advice may be sought from IT Services for specific circumstances.

Under no circumstances are the following environments acceptable for the use of Council owned peripherals:

- the home environment
- non-Council teaching establishments such as colleges, universities etc.

Any connected devices, including USB devices, where applicable, should be fully virus checked prior to being used within any Council systems.

Non-Council owned peripherals or USB devices are not permitted to be installed, used or configured on any Council computer or network. Prior consideration should be given to such circumstances and other transmission methods undertaken, e.g. email. Advice may be sought from IT Services for specific circumstances.

Under no circumstances are the following peripherals or equipment acceptable for use within the Council computing or network environments:

- personally owned equipment;
- equipment owned by non-Council teaching establishments such as colleges, universities etc.

Advice may be sought from IT Services for specific circumstances.

USB devices, as with all computer equipment for use on Council systems, must be procured through IT Services to allow a log of authorised equipment to be maintained and to ensure standards are maintained.

10.7 No wireless device may be installed or attached to Council equipment and/or network(s), except in instances authorised by IT Services and where the work is undertaken by IT Services staff or authorised parties.

11 Information Classification

Information should be classified in accordance with the Council's Information Classification guidelines, which aim to ensure the confidentiality, availability and integrity of Council data. Methods used for transmitting information should be adhered to as set out within the guidelines. Transmitting, removal and storage of information must also comply with this policy and any other applicable Council policy.

12 Disposal

Calls must be logged with the IT Service desk for the disposal of all Council computer related equipment and devices with the ability to store information. Service asset register updates and the removal of any locally stored data on computing equipment is the responsibility of the Service making a disposal request. Services should ensure staff are aware of their responsibilities with regards to IT waste and are aware of the Councils ICT Disposal Procedure.

Disposal of IT equipment is managed by IT Services taking into account legal and environmental issues, including copyright and data destruction while further ensuring that the appropriate corporate hardware and software registers are updated. The Councils 'ICT Disposal Procedure' must be adhered to.

13 Communications

13.1 Each employee is responsible for the content of all text, sound files or images he or she places on or sends over the Council's network, email/Internet system. No email or other electronic communication may be sent over the Council's systems which hides the identity of the sender or represents the sender as someone else or someone from another organisation.

13.2 Employees should remember that electronic communications have the same significance as other written communications and employees should exercise the same level of care whenever they are writing in this way. For additional guidance please refer to the "E-mail etiquette Hints & Tips" document on Navigate.

13.3 Any messages or information sent by an employee to another individual outside the Council are statements that reflect the Council. Notwithstanding personal "disclaimers" in electronic communications, there is still an affiliation to the Council, and all communications sent by employees via the Council's network, email/Internet system must recognise this and generally should not disclose any confidential or proprietary Council information.

Offical-Sensitive (Classified) information may not be sent via email to either internal or external addresses, without it being secured to an appropriate level with passwords, encryption or other controls in place such as communicating within the GCSx framework. Refer to the Councils Information Classification Guidelines for further advice. Such information should not be transmitted over the Internet without proper security measures in place. If clarification is required contact IT Services in the first instance.

13.4 Council information and/or data may not be removed from any Council premises without express permission from Senior Management. The individual removing the data must be aware of their legal responsibilities for maintaining the confidentiality, security and integrity of this information and must always comply with the Data Protection Act and other applicable legislation or Council policy. Information must be secured to an appropriate level with encryption, passwords or other appropriate controls being taken.

14 Email and Internet

14.1 The Council provides internal and external e-mail, and Internet access to assist employees in the performance of their jobs and its use should be limited to official Council business. Corporate network users are provided with Internet and Email access as standard. All Education Services School staff requiring access to external mail and Internet facilities must complete the ***Internet Access*** and/or ***Email Access*** authorisation forms and have them authorised by their line manager who must be at Grade 10 level or above.

14.2 Internet and Email use conforms to controls as applied by the Council such as mailbox size, malicious code scanning, permitted attachment types and web site filtering. Any non-receipt of expected communications should be discussed with IT Services.

14.3 Limited personal use of the Internet is permitted at certain times for authorised users. These times are published on Navigate for non-educational staff. All education staff within schools and nurseries are limited to personal use outwith timetabled teaching hours.

14.4 The user logged into an account will be responsible for the secure access to that account. It is the responsibility of the account owner to log out or lock access to the computer while away from the desk. Under no circumstances should you send email or access the Internet from an account that you are not authorised to use.

14.5 Email addresses should not be disclosed unnecessarily. If you give your address when completing surveys or other questionnaires you will be at risk of receiving unwanted junk messages.

14.6 Any Council email account authorised for your use, i.e. *name@north-ayrshire.gov.uk, name@north-ayrshire.gcsx.gov.uk* is for business related purposes only.

14.7 Internal Council e-mail and other internal materials should not be forwarded to destinations outside the Council, unless you have authority to do so by your manager or supervisor. In all instances the Council's Information Classification guidelines must be adhered to. Under no circumstances can Council email be automatically forwarded to a personal owned email account such as Hotmail etc.

14.8 The forwarding of chain mail is strictly forbidden. This includes those purporting to be for Charity or other good causes as well as those promising wealth or other personal gain.

14.9 You should not knowingly engage in any illegal activities using the Internet or email.

14.10 The Internet or email must not be used for personal financial gain.

14.11 In all messages, it should be remembered that e-mail is not a secure form of communication. External email messages that you send will be passed over networks owned by other companies. If the content of the message could cause problems for the Council or result in financial loss, should the contents become known, a more secure method should be used. Reference should be made to the Councils 'Information Handling Guidelines'.

14.12 You should only subscribe to e-mail lists that are appropriate for Council business. The volumes of messages that can be generated are high and you have no control over the content, which may bring you into conflict with other conditions of Council policy.

14.13 E-Mail should not be used to send large attached files, unless very urgent. Many e-mail systems will not accept large files and are therefore returned, possibly resulting in overloading the Council's own e-mail system. Exceptions to this should be discussed with IT Services.

In all instances of data being placed onto removable media the Council's Information Classification Guidelines and the Information Handling Guidelines should be followed. All media must be secured to an appropriate level in line with Council policy and legislation.

14.14 Do not open attachments to e-mail messages from untrusted or unknown sources. Do not connect to any URL embedded link within emails unless from a trusted, known and authenticated source. Where images are excluded from email communications these should only be activated where absolutely necessary.

14.15 No messages should be posted on any Internet message board, Blog or other similar Web based service that would bring the Council into disrepute, or which a reasonable person would consider to be offensive or abusive.

14.16 Users should be aware that certain Internet sites and services require you to leave your name and possibly other identification. Automatic collation of information, including your computer address and network may be logged allowing others to locate the Council that you work for, and the particular computer used to post a message. As part of the Council's routine security measures, all sites visited are centrally logged.

14.17 No web hosting of any kind is permitted on Council equipment without express permission.

14.18 You must not visit Web sites that display material of a pornographic nature, or which contain material that may be considered offensive.

14.19 You should not download any files from the Internet, or capture any images that are displayed unless business related and authorised to do so. You must ensure that copyright is adhered to with regards to the use of images and other material derived from any Internet or external source.

14.20 Council authorised peer-to-peer Internet sites must be used in line with Council policy and such use must not infringe Copyright or any other UK Legislation. Staff must seek guidance from Legal Services if required.
The use of unauthorised peer-to-peer Internet sites is not permitted without express permission. Initial guidance may be sought from IT Services.

14.21 Council Official-Protect information assets are not permitted to be shared on unauthorised Internet file sharing sites or peer-to-peer sites. Sharing of Official Classified information assets must be authorised by senior management.

14.22 The Council logs all Internet and email usage by individuals and reserves the right to access and report on this information.

15 Remote Connectivity

Remote connectivity to Council owned systems is only permitted with appropriate authorisation. This is applicable for both Council employees and non-Council employed persons.

Adherence to Council connectivity policies is mandatory. Advice can be sought from IT Services and should be sought prior to Services entering into any agreements for connectivity by other parties.

16 Permitted Personal use of Equipment

Where the Service has given permission for personal use of business equipment; this use must be appropriate to the device in question and used for business purposes within the remit of Council policy. Any personal use should be appropriate e.g. it would not be seen as appropriate for a Council mobile phone to be used for adult chat line usage.

17 Discrimination

Council systems must be used in a professional manner and may not be used for transmitting, retrieving or storing of any materials or communications of a discriminatory or harassing nature or that are obscene, pornographic or adult orientated. Discrimination of any kind is prohibited. No messages with derogatory remarks about an individuals race, age, disability, religion, national origin, physical attributes, sexual preference or any type of inflammatory remarks shall be transmitted. No abusive or offensive language is to be transmitted using the Council's systems.

This type of abuse may be deemed as gross misconduct resulting in summary dismissal. Please refer to the Council's Equal Opportunities Policy for further information.

18 Monitoring

The Council, and its service providers, log and audit usage of computers and systems. This includes email, Internet and other use of internal and external systems. Backup files may be kept which permanently record this usage. With good cause, the Council may monitor, record and report on the contents of computer systems and applications, computer files, Internet use and email messages sent, received and stored. This means that employees must not regard either business or personal communications on the Council's facilities as private.

Council computers are regularly audited as part of the conditions required for:

- achieving and maintaining certain accreditations
- complying with security requirements for processing of data within areas of Council operations
- compliance with security standards such as ISO17799/ISO27001

Staff should be aware that unauthorised attempts to access systems or data could be a criminal act under the Computer Misuse Act 1990 and are investigated.

19 Purpose of Monitoring

The purposes of monitoring, logging, auditing and recording are to:

- Ensure the effective operation of the Council's systems and to maintain system security
- Detect and investigate unauthorised use of the systems in breach of Council policies, such as excessive personal use or distribution of inappropriate material
- Monitor standards of performance
- Ensure business operates during employee absence and other business requirements
- Investigate allegations of misconduct, breach of contract, a criminal offence or fraud by the user or any third party

20 Breaches of Policy

Any employee who determines that there may be a misuse of software or breach of this policy within the Council should notify their line manager or Information Technology Service Desk immediately and follow the 'Reporting of Security Incidents' procedure and where appropriate, the Council's Public Interest Disclosure procedures.
Any actual or suspected breach of this Policy will be investigated by Information Technology Services, a Senior Manager from the service involved, and may also include Internal Audit. Any resultant action against an employee will be in accordance with the Council's disciplinary procedures and does not preclude prosecution through a court of law.

Appendix 1 – Referenced Documents

ICT Security Policy Framework

Education Service Level Agreement

E-Mail Etiquette Hints and Tips

Equal Opportunities Policy

Guidelines to the Data Protection Act

ICT Disposal Guidelines

Information Asset Register Guidelines

Information Classification Guidelines

Information Handling Guidelines

Internet and Email Access Control Policy

Password Guidelines

Records Retention Schedule

Reporting of Security Incidents Policy

Third Party use of Council Resources Guidelines

Checking the version of virus software

Public Interest Disclosure procedures

ICT Disposal Procedure – Corporate and Schools