



# Falkirk Council

## Acceptable Use Policy

Version	Date
V4	May 2011

## Contents

Section	Page
Contents	
1. Background	4
2. Objectives	4
3. Review of the Policy	5
4. General Guidelines on Information	5
5. Personal use	6
6. Use of the Internet	6
➤ General Guidelines on Use of the Internet	6
➤ Specific Guidelines of the Use of the Internet	7
➤ Social Media Guidelines	9
➤ Monitoring and Reporting Internet Use	9
7. Use of E-mail	10
➤ General Guidelines for the Use of E-mail	10
➤ Specific Guidelines for the Use of E-mail	10
➤ Monitoring and Reporting E-mail Use	12
8. Laptops and Mobile Storage Equipment	13
9. Telecommunications Equipment	14
➤ Use of Telecommunications Equipment	14
➤ Monitoring	16
➤ Specific Guidance for PDAs	16
10. Home Working/Remote Working	17

11. Misuse	17
Appendix A Legislation	19
Appendix B Agreement Form – Employees and Members	20
Appendix C Agreement Form – all ICT staff	21
Appendix D Agreement Form – ICT Network/Operations Staff	22
Appendix E Social Media Guidance	23

## 1. Background

- 1.1 Falkirk Council provides many and diverse Information and Communications Technology (“**ICT**”) services, tools and equipment to employees and Members (“**users**”) to be used in the course of their work, including computers, laptops, telephones, internet and E-mail.
- 1.2 The Internet has become a fundamental tool which the Council uses for research and education purposes. Internally, the Council has also developed an Intranet site to aid the dissemination of relevant information amongst employees.
- 1.3 The Council supports information and communications resources which will enhance the business and service environment. However, with access to computers and people all over the world via ICT comes the availability of material that may not be considered of value in the context of the Council setting. Additionally, as with any resource, there is the possibility of misuse. Accordingly, the Council requires to set guidelines for the use of ICT and, where appropriate, to monitor its use known as the Acceptable Use Policy (“**AUP**”).
- 1.4 However, even with the AUP, the Council cannot prevent the possibility that some users may access material, even inadvertently, that is not consistent with the policies of the Council or in line with the normal duties and responsibilities of the user.

## 2. Objectives

- 2.1 This Policy sets out the rules by which Falkirk Council expects users to employ the ICT services and equipment provided to them by the Council in order to carry out their duties in a sensible, professional and lawful manner in accordance with law and with the Council’s Code of Conduct for Officers, Employees and Members.
- 2.2 The AUP aims to set out the Council’s Policy on the use and monitoring of ICT and seeks to strike a balance between a users’ right to privacy and the Council’s responsibility to ensure appropriate use of ICT.
- 2.3 Failure to comply with the AUP by employees of the Council may be viewed as a disciplinary matter and may, therefore, be subject to the Council’s agreed Disciplinary Policy and Procedure. Failure to comply may result in access to the Council’s IT systems being restricted or withheld
- 2.4 All Officers and Members should read this Policy carefully before signing the Agreement Form - Appendix B. If the AUP is not signed then access to the Council’s IT systems maybe restricted or withheld.
- 2.5 Any queries in respect of the AUP should be logged through the ICT Service Desk.

### **3. Review of the Policy**

- 3.1 From time to time, as required by changes to legislation, technology or Council Policy, the AUP will be revised. Any changes will be agreed by both the Trades Unions and Members and the changes communicated to the users who have signed the original Policy. In any case, this Policy will be reviewed on a 3 yearly basis.

### **4. General Guidelines on Information**

- 4.1 All information, whether electronic or paper based, relating to our customers, suppliers and business operations should be treated in line with

- (a) The Council's Code of Conduct for Members and Officers
- (b) Relevant policies and
- (c) Relevant legislation, and in particular:

#### **Policies**

Data Protection Policy  
Information Security Policy  
Software Security and Licensing Policy

- 4.2 These documents are available on the Falkirk Council Intranet site.

#### **Legislation**

- 4.3 Users are bound by all relevant legislation. See Appendix A for details.

#### **4.4 E-mail Disclaimer**

- 4.5 All e-mail sent via the Council's e-mail services will carry the following disclaimer:

*"The information contained in this e-mail is confidential and is intended only for the named recipient(s). If you are not the intended recipient, you must not copy, distribute or take any action or reliance on it. If you have received this e-mail in error, please notify the sender. Any unauthorised disclosure of the information contained in this e-mail is strictly prohibited.*

*The views and opinions expressed in this e-mail are the sender's own and do not necessarily represent the views and opinions of Falkirk Council."*

#### **Agreement form - ICT Staff**

- 4.6 All operational ICT staff will be required to sign an agreement (Appendix C) which specifically covers the privileged access to systems that ICT staff have when dealing with the support, maintenance and development of systems and software. A further agreement (Appendix D) will require to be signed by ICT staff involved in the monitoring of Internet usage and network maintenance to cover their privileged access to the Internet for work purposes.

## **Agreement Form – Contractors and Access by Non Staff Members**

- 4.7 In certain instances, to systems and equipment covered by this Policy may require to be accessed by Contractors or non-staff members. Such access will still require the signed acceptance of the AUP by the individual and the authorisation of a Falkirk Council Service Manager. A separate Agreement Form is available for such instances.

## **5. Personal Use**

- 5.1 Any reasonable personal use of the Council ICT services and equipment must comply with the Council Code of Conduct for Officers and Members.
- 5.2 Reasonable personal use of such services and equipment:
- Should only occur with the permission and knowledge of your line manager;
  - Should not interfere with the performance of your duties;
  - Should not take priority over your work responsibilities;
  - Should not result in the Council incurring expense;
  - Should not have a negative impact on the Council; and
  - Should be lawful and in accordance with Council Policy and with this the AUP.
- 5.3 Where reasonable personal use is referred to in this Policy and is undertaken by the user, this section applies. It should be noted that personal use should be incidental to business use.
- 5.4 Reference to personal use of Council ICT systems and equipment in this Policy apply to Elected Members in the same way as employees with appropriate adjustment to reflect the non employee status of Members. Reasonable personal use is authorised by the Council by adoption of the Policy. Members should note the terms of the Code of Conduct for Councillors and in particular paragraph 3.16. Reasonable personal use does not include any party political or political campaigning activity.

## **6. Use of the Internet**

### **General guidelines on use of the internet**

- 6.1 Use of the Internet is available at your line manager's discretion.
- 6.2 In general, users shall only use the Internet for official purposes. Use of information from the Internet should be directly related to the official duties of the user, or the Council as a whole. All information downloaded from the Internet should be related to the duties and tasks of the user. However, reasonable personal use is permitted where the line manager has agreed this in advance.
- 6.3 Access to the Internet by employees must be authorised by the line manager.

- 6.4 Access to the Internet from Council desktop PCs must only be undertaken via the Council's own Internet server. This will be set up for users by ICT staff.
- 6.5 Where there is public access to the Internet provided by the Council and a member of the public misuses this provision, it will not be deemed the responsibility of any employee present at the time. However, the employee should report this incident as a breach of security to the ICT Service Desk.
- 6.6 Any information distributed or released by users by way of the Internet is subject to the Council's guidance on the release of information and shall, prior to such distribution, be approved by the relevant management procedures as put in place by the Communications Unit of the Policy and Performance Review Service of Corporate and Neighbourhood Services.
- 6.7 Any proposed links from the Council Internet site to other Internet sites must be authorised by the Communications Team.
- 6.8 With regards to the Virtual Teacher Centre and school websites, management approval for the distribution of such information will be as per procedures agreed by Education Services.
- 6.9 Users must be aware that the quality and accuracy of information available on the Internet is variable. It is the responsibility of the individual user to judge whether the information obtained is satisfactory for the purpose for which it will be used, and, if appropriate, steps should be taken to verify this information independently.
- 6.10 Where the Internet is being accessed by employees via a laptop or Personal Digital Assistant (PDA) from an internet connection which is not covered by the Council's internet filtering software e.g. where a direct Internet connection is made from an XDA, the AUP still applies. Extra care must also be taken not to visit sites that would be deemed unsuitable.
- 6.11 Users must check with ICT that virus protection software is installed on all Council Computer equipment that has access to the Internet. Care must be taken with PDA's and mobile storage devices to ensure that files stored on these devices do not become infected.
- 6.12 No personally owned ICT equipment may be attached to the Council's network.

### **Specific Guidelines on Use of the Internet**

- 6.13 Software, including MP3 files, must not be downloaded from the Internet by users without the advice of ICT personnel and approval from ICT and their manager.
- 6.14 When participating in newsgroups, online forums or mailing lists, users may offer information and advice to others if it is appropriate to their official duties or tasks

or if the benefit to be gained by the Council represents a reasonable return in terms of the effort involved.

- 6.15 Employees must not take part in discussions on political matters via the Internet unless this forms part of the legitimate business of their employment or is in furtherance of their role as an accredited Trade Union Representative.
- 6.16 Users must not use their access to the Internet to carry out their own private business purposes.
- 6.17 Use of Anonymous Proxy tools ('anonymisers') is expressly forbidden.
- 6.18 Orders for goods purchased for Council purposes must not be placed by way of the Internet without the employee having first obtained approval from their line manager, having authorised the purchase in the normal departmental manner and having complied with the Council's Contract Standing Orders and Financial Regulations.
- 6.19 Users must not use the Council's Internet facility for gambling.
- 6.20 Users must not break or attempt to break or circumvent any system security controls placed on their Internet Account.
- 6.21 Users must not intentionally access or transmit computer viruses or software programs used to trigger these.
- 6.22 Users must not intentionally access or transmit information which is obscene, sexually explicit, racist or defamatory or which depicts violent or criminal acts or otherwise represents values that are contrary to Council Policy.
- 6.23 Employees must not intentionally access or transmit information of a political nature unless this forms part of the legitimate business of their employment or is in furtherance of their role as an accredited Trade Union Representative.
- 6.24 Employees must not intentionally access and display information of a personal or sensitive nature that could be offensive to those around them.
- 6.25 Users must not do anything that breaks the law.
- 6.26 Access to Social Networking sites is restricted.
- 6.27 When using Social Networking sites at home or at work, consideration should be given to the security of any personal data that you post on such websites. Information relating to your employment with Falkirk Council, comments, or opinions about Falkirk Council or any of your colleagues should not be posted on such sites.
- 6.28 Where users have created content on the Internet as part of their duties, including on any forums or social networking sites, they have a duty to ensure that any content added to these by others is moderated on a daily basis to ensure

that this content is not defamatory or contrary to Council Policy. Any breaches must be reported to their line manager and the content removed.

- 6.29 If an Internet site containing unsuitable material e.g. of an obscene nature is inadvertently accessed by a user, this must be immediately reported to the ICT Service Desk as a security breach.
- 6.30 If material is inadvertently accessed which is believed to contain a computer virus, the user must immediately break the connection to the Internet and contact the ICT Service Desk for advice and assistance.
- 6.31 Users must not copy information originating from others and re-post it without the permission of or acknowledgement to the original source. Users may risk infringement of copyright by failing to do this.

### **Social Media Guidance**

- 6.32 Specific and more detailed social media guidelines for Falkirk Council employees have been developed and are available on the intranet. A copy of these are attached at Appendix E.

### **Monitoring and Reporting Internet Use**

- 6.33 All access to the Internet is automatically logged against an address unique to the PC of the user, is recorded and may be monitored by the Council. This monitoring will be for the prevention and detection of unauthorised use of the Council's communication systems.
- 6.34 Auditable statistics are kept within ICT of all Council Internet access.
- 6.35 Line managers are able to access details of sites visited by employees and the time spent accessing the internet. Such reporting is not provided on a set basis, but will be available to managers in the normal course of an investigation into inappropriate or prolonged use of the Internet by a member of staff.
- 6.36 The Council ICT Service actively monitors access to inappropriate sites via the Internet security software. Any 'irregularities' encountered in this process are reported to the line manager of an employee or to the Director of Corporate and Neighbourhood Services or Head of Service responsible for ICT in the case of a Member in accordance with the Council's Code of Conduct.
- 6.37 In the case of an investigation requiring to be carried out into the use of the internet by a user, the relevant authority will contact Corporate and Neighbourhood Services ICT section who will access the necessary monitored information and provide a report of this to the relevant authority. The relevant authority is the line manager and/or Human Resources in the cases of an employee and the Director of Corporate and Neighbourhood Services or Head of Service responsible for ICT in the case of an Elected Member.
- 6.38 Internet filtering software is used to block access to sites that have been deemed unacceptable. In certain cases, staff in specific posts may be allowed access to

sites normally blocked to users. This may be when information contained on a site is required or helpful in undertaking the duties of the post. In these circumstances, the line manager must contact the ICT Service Desk to request access to this site for the member of staff and confirm their approval for access to be given.

## 7. Use of E-Mail

### General guidelines on use of E-mail.

- 7.1 The Council is increasingly using E-mail as an important and significant channel of communication both within the Council and to communicate with external contacts. The following guidelines outline the Council's Policy and the responsibilities of users in the use of the E-mail system provided by the Council.
- 7.2 In general, users shall use E-mail for official purposes. However, reasonable personal use is permitted.
- 7.3 When using e-mail as a means of communication, it should be kept in mind that:
- E-mails are potentially subject to disclosure under the Freedom of Information (Scotland) Act 2002, including all expressions of fact, intent and opinion.
  - E-mails may be produced in court in the same manner as any other document.
  - E-mail communications, either internally or via the Internet, are neither guaranteed to be private nor to arrive at their destination either on time or at all.
  - Advice given by Email-has the same legal effect as that given in any written format.
  - All E-mail will have the Council's agreed disclaimer attached.

### Specific Guidelines for the Use of E-Mail

- 7.4 All E-mail communications must be dealt with in the same manner as a letter, memo or other business communication. Users must not transmit unencrypted confidential, sensitive or personal information via E-mail as this may constitute a breach of security under the terms of the Data Protection Act 1998.
- 7.5 Example for general guidance:

Confidentiality Risk	Messaging protocol to be used
<b>High</b> Social Enquiry reports to Procurator Fiscal	Secure email over GSX (Government Secure Extranet)
<b>Medium</b> Conveying sensitive personal or	Password protected document attached

personnel information	to email message
<b>Low</b> General messages	Email

- 7.6 Where Users require to send confidential, sensitive or personal information via E-mail, advice on encryption methods and software should be sought from Corporate & Neighbourhood Services, ICT Service and the appropriate encryption technique applied.
- 7.7 All guidelines which apply to the use of E-mail apply equally regardless of whether the E-mail is of a business or a personal nature.
- 7.8 Employees must not take part in discussions on political matters via either the Internet or E-mail unless this forms part of the legitimate business of their employment or is in furtherance of their role as an accredited Trade Union Representative.
- 7.9 E-mail may not be used by users to run a business.
- 7.10 Users must not send abusive, insulting, harassing or obscene E-mail messages.
- 7.11 Users must not use E-mail for the purposes of gambling.
- 7.12 Users must not use E-mail to abuse others (known as *'flaming'*).
- 7.13 Users must not participate in the sending of chain or pyramid letters.
- 7.14 Users must not forward material which has been E-mailed to them directly without the permission of the originator, unless the information is forwarded for reasons of normal Council business.
- 7.15 Where the content of an attachment sent by E-mail requires to exist in its original format only, all reasonable steps must be taken by the sender to ensure that the document cannot be changed e.g. use of password protection. This will be dependant on the software used to create the document.
- 7.16 Users must always use their own unique E-mail address when sending E-mails, even when answering e-mails sent to another user. Exceptions would be where employees are required to use generic email addresses established by the Council.
- 7.17 Users should only use generic E-mail addresses i.e. those in a format similar to [housing@falkirk.gov.uk](mailto:housing@falkirk.gov.uk) when responding to business enquiries. These addresses should not be used for sending personal e-mails.
- 7.18 Users must not falsify E-mails to appear as if sent from someone else or to provide false information to any Internet service requiring an E-mail address or other details.
- 7.19 Users should avoid sending large E-mails attachments wherever possible.

- 7.20 Users should not open electronic attachments if the source of such an attachment is unclear without checking with ICT.
- 7.21 Users should retain messages which are necessary for current Council business needs in their mailbox. These should be filed in accordance with the current Falkirk Council Records Retention Policy and in the format agreed by your line manager for the storage and retrieval of information in accordance with the Freedom of Information (Scotland) Act 2002. All unnecessary mail documents – obsolete messages, return receipts and attachments - should be deleted from the system.
- 7.22 Users must not read, delete, copy or modify the contents of the mailbox of another employee or member without the proper authority. This would generally take the form of the authorisation of the line manager of the employee whose mailbox is being accessed. In the case of an Elected Member, this authorisation would come from the Director of Corporate and Neighbourhood Services or Head of Service responsible for ICT.

### **Monitoring and Reporting E-mail Use**

- 7.23 Monitoring is carried out automatically to block inappropriate or malicious material sent and received by E-mail.
- 7.24 In general, the Council respects users' privacy and autonomy in electronic communications. However, the Council reserves the right to access, record or monitor the contents of E-mails both sent and received via the Council Mail system in order to:
- Provide evidence of business transactions;
  - Ensure that Council business and security procedures are adhered to;
  - Monitor standards of service;
  - Provide necessary training;
  - Prevent or detect unauthorised use of the Communications systems;
  - Access communications where necessary in the event of a user's absence from the office; and / or
  - Access communications to and from an ex-user.
- 7.25 In the case of an investigation requiring to be carried out into the use of E-mail by a user, the relevant authority will contact Corporate And Neighbourhood Services ICT section who will access the necessary monitored information and provide a report of this to the relevant authority. This will be the line manager and/or Human Resources in the cases of an employee and the Director of Corporate and Neighbourhood Services or Head of Service responsible for ICT in the case of an Elected Member.

- 7.26 Personal E-mails will generally be excluded from investigation unless there is good reason to suspect that abuse has occurred through the use of personal E-mail.

## **8. Laptops and Mobile Storage Equipment**

- 8.1 Increasingly, laptops and other forms of mobile electronic storage equipment – PDAs, USB storage devices etc – are being used to help conduct the business of the Council.
- 8.2 Users of such equipment must ensure that these devices are stored securely and used legally in accordance with the AUP.
- 8.3 Users must also ensure that data stored on these devices is held as securely as possible. Data held on such devices should be password protected wherever possible and, where personal, sensitive or confidential information is stored, encryption should be applied. Falkirk Council ICT Service can provide advice on appropriate encryption methods.
- 8.4 All devices kept within Council Premises should be stored securely, and away from windows wherever practicable when not in use. Data held on such devices should be password protected wherever possible. Users should only use USB devices provided by Falkirk Council on Council supplied equipment.
- 8.5 All users of such equipment are responsible for the security of the equipment itself and for the data which is stored on it. Protecting the equipment and the data from viruses forms an essential part of that responsibility.
- 8.6 When mobile equipment is used out with the office environment the following applies:
- It should be stored as securely as possible and out of view e.g. locked in a car boot during the course of business or stored in a locked house. Such equipment should not be left locked in a car overnight.
  - It should not be left unattended in a public place – including clients' homes and suppliers' premises.
  - Laptops should have up-to-date virus protection software installed by Council ICT personnel. It is the responsibility of the user to ensure that this software is kept up to date. This can be done by connecting the equipment to the Council network on a regular basis.
  - Equipment should not be connected to a network other than that of the Council without the permission of the line manager and guidance of Council ICT personnel.
  - Files from mobile devices should only be transferred to a computer on the Council network where the computer has virus protection software installed.

- Access to all such equipment should be password protected.
- Files stored on such equipment should be password protected.
- Where data stored on such equipment is of a personal, sensitive or confidential nature, such files should be encrypted as well as password protected.
- Data should only be removed from business premises where absolutely necessary. Where data is removed e.g. on a memory stick this should be password protected and encrypted. It should also be erased from such equipment when it no longer needed in this format.
- Equipment should not be used for personal use without the consent of the line manager.
- Extreme caution should be taken when files containing personal or sensitive information are carried on such equipment. Wherever possible, such files should be password protected. Care should be taken that such personal information cannot be seen in a public place by a third party or accessed by unauthorised persons.
- Where such equipment is used outwith the office environment, it is the responsibility of the user to ensure that all Health and Safety considerations for the operation of such equipment are taken into account, including Display Screen Equipment Regulations, trip hazards etc.
- Where mobile equipment is taken abroad, extreme care must be exercised .Line managers must approve the use of such equipment abroad.
- Any loss of, damage to or unauthorised access of such equipment or data must be reported as soon as reasonably practicable to your line manager. Any stolen property should be notified immediately in accordance with standard Council procedures.

## **9. Telecommunications Equipment**

### **Use of telecommunications equipment**

- 9.1 Falkirk Council provides telephones and mobile telephones to users to carry out the business of the Council.
- 9.2 In general, limited personal use of both is allowed where it has been authorised by the line manager and the user agrees to separately identify and pay for any calls made which are of a personal nature.

- 9.3 All communications carried out by means of telephone should be conducted in a professional manner and not breach the Code of Conduct of Officers and Members.
- 9.4 Calls should not be made to conduct a business other than that of the Council.
- 9.5 When using the speakerphone function, users should always advise those participating in the call that this is being used and that others may hear their conversation.
- 9.6 All mobile telephones should be kept securely and appropriate security measures should be taken to ensure that they, or data held on them, are not subject to loss, damage or unauthorised access.
- 9.7 Any loss or damage to telephony equipment should be notified to both the line manager and the ICT Service Desk as soon as reasonably practicable..
- 9.8 Mobile phones should be used in accordance with the guidelines issued by Human Resources and in particular should not be used
- whilst driving, without hands-free equipment
  - in places where such use is prohibited or restricted
- 9.9 It is a prosecutable offence for a driver to use a handheld mobile phone or other device to send or receive text, data or voice messages whilst their vehicle engine is running. Before making or receiving texts, data or voice messages, Users should be safely parked with the vehicle engine switched off.
- 9.10 Any member of staff in breach of the above during working hours or in a Council vehicle may be subject to disciplinary action.
- 9.11 Dialling premium numbers from mobiles is banned wherever possible. However, users have a responsibility not to contact such numbers and should not be using premium lines or lines which have adult content. Use of such numbers would constitute a breach of the AUP.
- 9.12 Council issued mobile phones can be used abroad. However, such use should be limited and Users should be aware of the increased costs of making calls from abroad and that when answering calls abroad, both the caller and the User will be charged for the call.
- 9.13 Users should be aware that using GPRS technology to access the Internet or e-mail from their phone or XDA will incur charges and use of this should be limited wherever possible.
- 9.14 Users must not use items such as SIM cards, storage cards and other peripherals provided by the Council with a mobile phone other than those provided by the Council without the prior approval of the ICT Service.
- 9.15 Text messages can be sent from Council issued mobile phones. However, users should be aware that all text communications must be dealt with in the same

manner as a letter, memo e-mail or other business communication and that the AUP applies to these.

- 9.16 When a mobile telephone or PDA/XDA is lost, this loss should be reported through the ICT Service Desk as soon as the owner is aware of this. SIM cards will be wiped and disabled as soon as they are reported lost in order to comply with the Data Protection Act 1998.

### **Monitoring**

- 9.17 Details of all calls made from and received by both land lines and mobile phones are recorded including the date, time and duration of the call.
- 9.18 The information gathered on these calls is provided to and may be monitored by line managers.
- 9.19 Content of calls will only be recorded with the explicit knowledge of the user unless this monitoring falls into the terms of the Regulation of Investigatory Powers (Scotland) Act 2000.

### **Specific Guidance for PDAs**

- 9.20 The Council is increasingly distributing mobile devices known as Personal Digital Assistants (PDAs) to users. This covers:
- handhelds which run industry standard computer operating systems
  - mobile devices which are standalone
  - devices which have wireless capability including Wi-Fi, Bluetooth and IR
  - Smartphones with PDA functionality
- 9.21 Where a user has been provided with a PDA by the Council, the following applies:
- Any hardware, software or related components should not be added to the PDA without the agreement of the Council's ICT section.
  - PDA's should only be allowed access to the Council's network at the discretion of the Council's ICT section who will require to approve the connection type as secure, protected and supported.
  - As with use of the telephone systems for personal use, connectivity of the PDAs for internet use for personal purposes must be identified and paid for by the user.
  - All PDAs should be password protected wherever technology allows.

## **10. Home Working/Remote Working**

10.1 When using Council systems or equipment (such as laptops) or using your own computer equipment to work on Council business away from Council's premises, the following rules apply:

- All work related to the business of the Council must be password protected.
- All work, in particular that where personal or sensitive information is involved, should be carried out in a position where it cannot be seen by others.
- All reasonable precautions should be taken to safeguard the security of any Council equipment or data regardless of the medium it is stored in – paper, diskette, CD, USB device or laptop.
- Where data to be used at home is of a personal, sensitive or confidential nature such files should be both password protected and encrypted. Advice on encryption methods can be obtained from the ICT service.
- In accordance with principle seven of the Data Protection Act 1998, appropriate measures must be taken to ensure the security of personal data which comes into your possession in the course of your employment to prevent it from theft, loss, destruction or harm either accidental or malicious.
- Any files saved remotely should be transferred to a Falkirk Council System as soon as is practicable.
- Health and Safety consideration around the use of such equipment remotely or at home is the responsibility of the employee. The Council's Home Working Policy will provide guidance on this. This can be found in the HR area of the Intranet.

## **11. Misuse**

11.1 It is the responsibility of every user to use these services and equipment appropriately, legally and in accordance with the AUP and the wider policies of the Council including the Code of Conduct for Officers and Members.

11.2 Furthermore, it is a criminal offence under the Computer Misuse Act 1990 to carry out the following activities:

- Unauthorised access to computer material i.e. hacking
- Unauthorised modification of computer material
- Unauthorised access to computer material with the intent to commit or facilitate the commission of further offences.

- Undertake the harassment of others by electronic means.
- 11.3 The Council reserves the right to withdraw Internet access or E-mail use – or any access to the Council’s computer or communications network – if the user has been found to be in breach of the AUP.
- 11.4 The Council reserves the right to prohibit access to specific newsgroups or Internet sites or other Internet resources or to remove or substitute the hardware or software used to access the Internet at any time for any reason.
- 11.5 Any breach of the AUP will be viewed seriously and may result in action being taken under the Council’s Disciplinary Policy and Procedures.
- 11.6 Additionally, the Council is legally obliged to co-operate with the Police, Inland Revenue and Customs and Excise in the investigation and detection of crime and apprehension of offenders. This may involve allowing such bodies access to the monitoring records of or equipment held by an individual employee or Member.
- 11.7 Where a user has inadvertently accessed inappropriate material or wishes to clarify any points in the AUP or has an incident to report, this should be logged through the ICT Service Desk in the first instance. Service Desk staff will pass this on to the relevant person within ICT or discuss with the line manager of the User if appropriate.

## *Appendix A*

### **Legislation**

**Copyright, Designs and Patents Act 1988** - downloading, copying, processing or distributing information from the Internet may be an infringement of copyright or other intellectual property rights.

**Data Protection Act 1998** - care should be taken in the collection, processing or disclosure of any personal data and all personal data should be processed within the principles of the Act.

**Freedom of Information (Scotland) Act 2002** – all recorded information is potentially liable to disclosure under the Act, including all expressions of fact, intent and opinion. If a request for information is made, the Act prohibits destruction of the information until it is given out in response to the request. Please also see the Council's guidelines on retention of information

**Computer Misuse Act 1990** - makes provision for securing computer material against unauthorised access or modification; and for connected purposes.

**Telecommunications Act 2003** - provides legislation to govern fraudulent and improper uses of telecommunications equipment.

**Regulation of Investigatory Powers (Scotland) Act 2000** - allows the Government and other law enforcing agencies to monitor and access online communications.



Falkirk Council

**Appendix B**  
**Agreement Form – Employees and Members**

I have read and understand Falkirk Council's Guidelines for the Acceptable Use of Information and Communications Technology and agree to comply with these guidelines. I understand that any deliberate breach of these will be viewed seriously and may result in action being taken under the Council's disciplinary procedures which may include the withdrawal of access to either E-mail or Internet facilities or both.

I accept that all access to the Internet is recorded and may be monitored and that any 'irregularities' encountered in this process will be reported to my line manager or the Director of Corporate and Neighbourhood Services or Head of Service responsible for ICT.

I agree that if I inadvertently access any Internet site containing unsuitable material, I will report this matter as a security breach through the ICT Service Desk.

Please complete the details on this form and return to **Email Implementation Team, ICT, Corporate & Neighbourhood Services, Municipal Buildings, West Bridge Street, Falkirk FK1 5RS**. For school based employees, these forms should be retained within the school.

Known Name: \_\_\_\_\_ Other Initial(s): \_\_\_\_\_ Surname: \_\_\_\_\_

Job Title: \_\_\_\_\_ Place of Work: \_\_\_\_\_

Service: \_\_\_\_\_ Section: \_\_\_\_\_

Room No: \_\_\_\_\_ Work Tel. No: \_\_\_\_\_ Work Fax No: \_\_\_\_\_

Login Id: \_\_\_\_\_ Server Name (if known): \_\_\_\_\_

Signature: \_\_\_\_\_

Manager's Signature: \_\_\_\_\_

Internet Use - business   
Internet Use - personal

E-mail Use - business   
E-mail use - personal

**Appendix C**

**Agreement Form – ICT Staff**

I have read and understand Falkirk Council's Guidelines for the Acceptable Use of Information and Communications Technology and agree to comply with these guidelines. I understand that any deliberate breach of these will be viewed seriously and may result in action being taken under the Council's disciplinary procedures which may include the withdrawal of access to either E-mail or Internet facilities or both.

I accept that all access to the Internet is recorded and may be monitored and that any 'irregularities' encountered in this process will be reported to my line manager or the Director of Corporate and Neighbourhood Services or Head of Service responsible for ICT. I also agree not to disclose or otherwise distribute any information which I may come across in the course of my duties.

I agree that if I inadvertently access any Internet site containing unsuitable material, I will report this matter as a security breach through the ICT Service Desk.



**Falkirk Council**

Please complete the details on this form and return to **Email Implementation Team, ICT, Corporate & Neighbourhood Services, Municipal Buildings, West Bridge Street, Falkirk FK1 5RS**. For school based employees, these forms should be retained within the school.

Known Name: \_\_\_\_\_ Other Initial(s): \_\_\_\_\_ Surname: \_\_\_\_\_

Job Title: \_\_\_\_\_ Service -: C&NS -ICT

Signature: \_\_\_\_\_

The above named member of staff is involved in the support and maintenance of the Council's ICT systems and of the equipment used to provide the ICT Service. As such, they may require, as part of these duties, access records and information which are not their own and may be of a confidential nature e.g. accessing the e-mail account of another member of staff.

Signature of Line Manager .....

Print Name of Line Manager .....

Date .....



*Appendix D*

**Agreement Form – ICT Network & Operations Staff**

I have read and understand Falkirk Council's Guidelines for the Acceptable Use of Information and Communications Technology and agree to comply with these guidelines. I understand that any deliberate breach of these will be viewed seriously and may result in action being taken under the Council's disciplinary procedures which may include the withdrawal of access to either E-mail or Internet facilities or both.

I accept that all access to the Internet is recorded and may be monitored and that any 'irregularities' encountered in this process will be reported to my line manager or the Director of Corporate and Neighbourhood Services or Head of Service responsible for ICT.

I agree that if I inadvertently access any Internet site containing unsuitable material, I will report this matter as a security breach through the ICT Service Desk.



**Falkirk Council**

Please complete the details on this form and return to **Email Implementation Team, ICT, Corporate & Neighbourhood Services, Municipal Buildings, West Bridge Street, Falkirk FK1 5RS**. For school based employees, these forms should be retained within the school.

Known Name: \_\_\_\_\_ Other Initial(s): \_\_\_\_\_ Surname: \_\_\_\_\_

Job Title: \_\_\_\_\_ Service -: C&NS -ICT

Signature: \_\_\_\_\_

The above named member of staff is involved in the support and maintenance of the Council's network and of the equipment used to provide the network services. As such, they may require, as part of these duties, to undertake investigative and diagnostic work at the discretion of the Head of Service responsible for ICT which may depart from the actions specified in the policy.

Signature of Line Manager .....

Print Name of Line Manager .....

Date .....

## ***Appendix E***

### **Social media guidelines for Falkirk Council Employees**

#### **Background**

Guidelines for the use of the Council's systems and resources including the Internet and email are clearly set out in the Council's Acceptable Use Policy (AUP), which can be found on the intranet. The Acceptable Use Policy sets out the rules the Council expects users to employ when using the ICT services and equipment provided to them by the Council, in order to carry out their duties in a sensible, professional and lawful manner in accordance with the law, the Council's Policies and the Council's Code of Conduct for Members and officers.

The guidance in the AUP sets out the Council's policy on the use and monitoring of ICT and seeks to strike a balance between a user's right to privacy and the Council's responsibility to ensure appropriate use of ICT.

#### **Social Media**

These guidelines have been produced to help employees and managers understand their responsibilities when using social media.

Social media is a term used to refer to online technologies and practices that are used to share opinions and information, promote discussion and build relationships. Social media services and tools involve a combination of technology, telecommunications and some kind of social interaction. They can use a variety of different formats, for example text, pictures, video and audio.

Social media includes online tools, websites and services that people use to share content, profiles, opinions, insights, experiences, perspectives and media itself. These tools include social networks, blogs, message boards, podcasts, microblogs, livestreams, social bookmarking, wikis, and vlogs.

The feature that all these tools, websites and services have in common is that they facilitate conversations and online interactions between groups of people.

Well-known examples of popular social media applications are Wikipedia (wiki), MySpace and Facebook (social networking), Twitter (microblog), YouTube (video sharing), Flickr (image sharing) and del.icio.us (bookmarking).

The Council currently restricts access to social networking sites on work-based PCs unless this is required as part of an employee's job. The Council will monitor the use of social networking sites to ensure that any use by employees complies with its internet policy, as detailed in the AUP.

## **Personal Use of Social Media**

This document is designed to provide guidance on the use of social media tools by Council officers in a personal capacity. For example, this includes a personal profile on Facebook or use of Twitter in a personal capacity by Council officers and includes personal use at home.

It is not our role as an employer to discourage you from using these sites in their own time on your own PCs. These guidelines are not meant to deter you from using these communications methods but are necessary to help protect employees and prevent them from bringing the Council into disrepute either inadvertently or intentionally. They also set out the potential consequences of doing so.

In addition, care does, however, need to be taken to protect your personal identity. You should be aware that some sites allow you to display your name, photograph and personal details to potentially thousands, if not millions, of users. You can set privacy settings which limit the number of people who can view your information. If you don't do this, you never know who's looking at your profile.

If you do use such sites:

- Think carefully about whether it is appropriate to share the information on your profile with potentially millions of users;
- Think about whether someone could steal your identity and how you could change your profile to avoid this happening;
- Make sure you set privacy settings and seek guidance if you're not sure how to do this;
- Think about whether your profile could be used with other information on the internet to identify where you live and other things about you – you may want to change your information if this is a risk;
- On personal networking sites, don't display information which identifies Falkirk Council as your employer, e.g., a photograph in which you're wearing an identity badge or staff uniform – this could allow someone to find out information on you, as well as raising conflict with your role as an employee which could lead to questions about your conduct;
- Think about the information you're posting on the site and any interactions you have – some of which could damage relationships with individuals and cause difficulties for you;
- Review your profile regularly; especially if you have changed jobs to make sure contacts don't conflict with your new role;
- Teachers, social workers and related professionals working with children, young people and vulnerable adults should take extra care when using social networking or photo-sharing sites. They should not accept current pupils, clients or vulnerable adults as "Contacts" or "Friends".

## Employee Code of Conduct

When using social media, you should respect your audience. As a general rule, you should be mindful of any detrimental comments made about colleagues whilst using social media. Any conduct which breaches Council policies or the Employee Code of Conduct, such as failing to show dignity at work (harassment), discriminatory language, personal insults, obscenity, or disclosure of confidential information, etc, could be considered a disciplinary matter.

You should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory – such as politics and religion.

You should be aware of your association with Falkirk Council when using social media, including professional networking. If you identify yourself as a Falkirk Council employee (e.g. on Linked In) you should ensure that your profile and any related content are consistent with how you would wish to present yourself to colleagues and professional contacts.

Even if you do not directly identify yourself as a Falkirk Council employee when using social media for personal purposes, you should be aware that content you post on social media websites could still be construed as relevant to your employment at Falkirk Council.

For example, you should not write or report on conversations, meetings or matters that are meant to be private or internal to Falkirk Council. Unauthorised disclosure of confidential information could constitute misconduct/gross-misconduct in accordance with the Council's disciplinary policy.

Using the Internet to make negative or defamatory comments about Falkirk Council, its agreed decisions or policies, or its officers or Members could also result in disciplinary action and potentially legal action on a collective or individual basis. The Council will not accept liability for any actions arising out of your personal use of social networking sites.

- You should remember that you are personally responsible for the content you publish on blogs, wikis or any other form of user-generated media;
- You should be mindful that anything you publish will be public for a long time and can't be retracted once it is published.

Some people also have personal blogs. This is entirely a matter of personal choice. Blogs should however, only detail personal matters and not in anyway associate personal views expressed on a blog with the Council. Equally, blogs should not reveal confidential information about the Council.

Whether it is the use of a social networking site, or development of your own blog, think about protecting your personal identity.

You should also not be using such sites to:

- Attack, abuse or 'gossip' about your work colleagues or clients/customers;
- Bring the Council as your employer into disrepute;
- Post derogatory or offensive comments on the Internet.
- Such use may require to be formally investigated by the Council.

If you are in any doubt about what you're doing on such sites, ask for help.