Argyll Bute COUNCIL

ARGYLL AND BUTE COUNCIL

ICT Acceptable Use Policy

Date of Issue: September 2021

Contents

SECTION 1 INTRODUCTION

1.1 Information is one of the Council's most important assets. The objective of Information Security is to ensure the confidentiality, integrity, availability and legal compliance of all the Council's information assets, including hard copy documents as well as electronically stored information. This policy details the principles, guidelines and requirements of the Council's ICT (Information and Communications Technology) Acceptable Use Policy.

1.2 This policy has been created to promote the integrity, security, reliability and privacy of the Council's information systems, electronic communications and networks, and the networks to which they connect. This includes but is not limited to, servers, PCs, Laptops, Tablets, PDAs, communications, networks and other organisations networks, printers, software, mobile phones, pagers, scanners, data storage devices, computer-processing services and electronically held data.

1.3 This policy applies to all employees (including home based, flexible and agile workers), elected members, contractors, consultants, temporary staff and other workers at the Council, employees of Live Argyll and partner organisations including the Health and Social Care Partnership.

1.4 The Council retains the right, in consultation with Trades Unions, to modify the policy at any time and any such modification shall be notified to all existing users.

1.5 **It is important that you read this policy carefully.** If there is anything that you do not understand, it is your responsibility to ask your line manager or ICT Systems Administrator to explain. Formal acceptance of this policy is a condition of being granted access to the Councils ICT resources and the provision of an internet/email account.

SECTION 2 GENERAL

2.1 Background

2.1.1 Violation of this policy including inappropriate use of the Internet, Council Intranet, email services, or other communications media may result in an investigation being conducted, with disciplinary action being taken if necessary against any of the individuals involved, up to, and including dismissal. In instances where disciplinary procedures are invoked, the individuals will be given the opportunity to see, explain or challenge the results of any investigation.

2.1.2 Access to any of the Council's computer systems is only granted where there is demonstrable business need, and to those facilities that are specifically authorised. There is also a personnel verification process explained in section 2.7.

2.1.3 Access to the Internet and email is provided to make information available in support of business, for research and education purposes and to improve the efficiency of the Council's communication system, business operations and service delivery.

2.2 Security

2.2.1 The Council's successful delivery of services increasingly depends on the effective performance of ICT systems. Employees must report immediately any unusual events, occurrences, emails or issues, to the IT Service Desk on extension 4060.

2.2.2 Any attempt to disable or circumvent security procedures is prohibited. Employees must ensure that you have the correct authorisation before attempting to gain access to Council systems.

2.2.3 The Internet is a public domain; therefore all confidential corporate information must be dealt with appropriately. Anyone found disclosing confidential organisational material deliberately or inadvertently may be subject to disciplinary action. If you are unsure as to whether data is confidential, consult your line manager.

2.2.4 Under no circumstances must any employee or elected member connect a Council owned computer to any non-Council owned computing device or network, e.g. connection to an Internet Service Provider or personal device without prior approval from the ICT and Digital Manager - that can be sought via the ICT Service Desk on extension 4060.

2.2.5 Laptops and other mobile equipment, such as mobile phones or tablets are vulnerable to the unauthorised disclosure of information. Mobile equipment should be kept in a safe place when outside Council premises.

2.3 Virus. Malware or Ransomware Attack

2.3.1 All incoming and outgoing media, DVDs or USB memory devices (including connecting mobile phones) and email attachments must be virus checked. If you suspect a virus is present, if you receive a suspicious email or your PC behaves in an unusual manner, stop using it and contact the IT Service Desk on extension 4060. The anti-virus software, which is installed on your equipment must not be disabled at any time.

2.3.2 All computers, laptops, tablets or mobile phones should have a virus checker in place. If you believe that your equipment does not have a virus checker, please notify the Service desk immediately.

2.4 Right to Privacy and Monitoring of Electronic Communications

All user activity on the Council's ICT network is logged. In accordance with the Data Protection Act 2018 and GDPR, a privacy notice is available in Appendix 1 which describes the Councils responsibilities for the information collected.

2.4.1 Electronic communications are an essential business tool. They take many forms, but include the use of the internet, email and other use of systems and applications. Monitoring is undertaken to protect the Council from potential misuse of these electronic communications, and to assist ICT staff in the delivery of service. The nature and extent of the monitoring that takes place is set out below. The Council regularly reviews its monitoring procedures to ensure that internet and email monitoring does not become intrusive.

2.4.2 The Council will respect individual's right to privacy and comply with data protection legislation.

2.4.3 The Council will carry out periodic, random baseline data audits that consist of date, time and address of the computer using Internet Protocol (IP), address of the Web page and the name of any file accessed or downloaded.

2.4.4 The Council reserves the right to access the contents of employee or elected members' email or internet usage if it has reasonable grounds to do so. This would include, but not be limited to, unlawful acts, breach of Council policies and procedures, suspicions about defamation, copyright infringement and harassment.

2.4.5 System access, internet and email traffic including attachments and usage of facilities are logged. This will include any personal usage. Monitoring is largely automated (i.e. conducted by automated ICT systems such as virus scanners, firewalls and content checking software to block offensive and inappropriate material). Intervention is carried out on an exception basis and targets the areas of greatest risk, to protect information technology systems and assets. In instances where specific monitoring takes place of individuals, the authorisation of the individual's Executive Director or Head of Service will be obtained. Where the Executive Director or Head of Service authorisation has not or cannot be obtained, such authorisation shall be sought from the Executive Director of Customer Services who may give such authorisation.

2.4.6 Union representatives have the right to use existing Council email facilities for trade union purposes.

2.4.7 Employees have the right to use existing Council email facilities to communicate with union representatives.

2.4.8 Where employees are involved in a high volume of message interaction directly with the public as a core duty, the content of messages received or sent may be accessed for quality control purposes. In these circumstances the employee would be made fully aware in advance of that necessity and the intention to perform monitoring

2.4.9 Where the Council holds monitoring information from which individuals can be identified, this will be registered under the Data Protection Act 2018 and General Data Protection Regulations (GDPR) 2018. aAny data subject has the right of access to their information.

2.5 Protection of Copyright Material

2.5.1 The penalties for using unlicensed software are significant. Therefore only software provided by the Council must be used. The ICT service representatives are responsible for loading all computer hardware and software. Unauthorised staff must not, under any circumstances, install software; or install, remove or swap items of hardware. You must not take copies of any Council supplied software, nor load any software not provided by the Council.

2.5.2 The ICT Helpdesk must approve any software prior to installation. In the event of any contention the final approval or denial will be decided by the Executive Director of Customer Services.

2.6 Software Removal

2.6.1 Unlicensed, redundant or unused software will be removed by ICT service representatives. End users should not attempt to delete software or software components from their systems as you may inadvertently remove key operating files.

2.7 Public Services Network (PSN)

2.7.1 The Councils computer systems form part of a wider connected community called the Public Services Network (PSN). To access the Council's computer systems and wider PSN services it is necessary to carry out personnel security checks in line with a HM Government policy known as the Baseline Personnel Security Standard (BPSS). BPSS comprises verification of the following four main elements, which are described below:

- Identity
- Nationality and Immigration Status (including an entitlement to undertake the work in question)
- Employment history (past 3 years)
- Criminal record (unspent convictions only)

Additionally, prospective employees are required to give a reasonable account of any significant periods (6 months or more in the past 3 years) of time spent abroad.

2.7.2 The PSN provides secure connection and communications (including secure email) with other UK Public Sector bodies. Membership of the PSN community allows Council email users to receive potentially sensitive information by email from other public bodies through a secure channel - there is therefore a requirement that Council email users control the subsequent treatment of such incoming emails. The Council abides by the PSN Code of Conduct (CoCo) though adoption of compliant security management processes and procedures. All users having access to the Councils systems are potential users of the PSN and the requirements of the CoCo are hereby incorporated into this Acceptable Use Policy.

2.7.3 Access to the PSN must not be attempted other than from ICT systems and locations that have been explicitly authorised for that purpose. Information must not be transmitted via PSN that is :

a) Known or suspected to be unacceptable within the context and purpose for which it is being communicated.

b) Known or suspected or have been advised is of a higher level of sensitivity than the PSN is designed to carry.

SECTION 3 NETWORK ACCESS - PASSWORDS

3.1 POLICY

3.1.1 All employees (including home based, flexible and agile workers), elected members, contractors, consultants, temporary staff and other workers at the Council, employees of Live Argyll and partner organisations including the Health and Social Care Partnership, must have a unique user name and confidential password to access Council computer systems. It is the responsibility of each employee and elected member to maintain the confidentiality and integrity of their logon and passwords.

3.1.2 Good password selection and non-disclosure is paramount and each user is accountable for actions linked to their user-id, therefore passwords must never be disclosed or shared.

3.2 GUIDANCE

a) DO use at least fourteen mixed alphabetic and numeric characters.
b) DO use a phrase with spaces between words
c) DO NOT repeat characters (111 or AAA) and avoid obvious sequences (123… or ABC…)
d) DO NOT use names, dates, user-id, or words associated with yourself.
e) DO NOT re-use your passwords.
f) DO NOT write your password down.
g) LOG OFF the computer at the end of each day.
h) Always use the PC screen lock to protect sessions during brief departures.

SECTION 4 EMAIL, CHAT AND INSTANT MESSAGING

4.1 POLICY

4.1.1 Email, Skype for Business (SfB) and MS365 messaging facilities are provided within the Council to assist employees, members, contractors and consultants in the performance of their jobs. All such communication must conform to the same standards as written documents.

4.1.2 Personal use is discouraged; however occasional and reasonable personal use is permitted provided that it does not interfere with the performance of your contract/duties, nor does it compromise the Council.

4.1.3 It is important to remember that electronic communications can be used as evidence in a court of law and may also be disclosed under certain provisions of the Data Protection Act 2018 and General Data Protection Regulations (GDPR) 2018.

4.1.4 A manager with the authority to sign an AUP may also request a member of staff be given access to a mailbox in circumstances where you are not available for a significant period and there is a concern that important business emails may not be handled in a timely manner.

4.1.5 Email and instant messages should be treated as formal means of communication. You should not send messages that could be deemed to be discriminatory in terms of the protected characteristics set out in the Equality Act 2010 which are age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation. This includes forwarding any received e-Mail for example: chain letters, sexually explicit messages, images, cartoons, or jokes. Users should not communicate anything on e-mail that they would not want read by a third party or attributed to the Council.

4.1.6 Abuse of email and instant messaging may result in an investigation being conducted, with disciplinary action being taken against any of the individuals involved if necessary, up to, and including dismissal. In instances where disciplinary procedures are invoked, the individuals will be given the opportunity to see, explain or challenge the results of any investigation.

4.1.7 Any other private messaging platform (including but not limited to WhatsApp, Signal, Telegram etc.) should never be used to transmit personal or sensitive information and council business should not be conducted on these platforms. It is acceptable to check in and stay in touch only.

4.1.8 Users must ensure they are familiar with the current guidance and approved use, and have undertaken any required training, for any standard corporate applications, such as Outlook, Teams, Sharepoint, Planner, OneDrive, and any other applications in use. Guidance will set out the type of use approved for each application, and will provide guidelines in relation to data protection and information management.

4.2 *GUIDANCE*

4.2.1 Acceptable Use

DO

a) Follow the Email management guidance for staff – move emails which need to be kept as formal records to an appropriate repository in accordance with information management guidance, and delete emails which do not need to be kept.
b) Remember that using CAPITAL letters is sometimes viewed as shouting.
c) Disable the email option to 'display a message when a new mail message arrives' as the sender cannot be verified if the 'YES' option is enabled. This will prevent the use of "autorun" messages that could be used to either place a virus on a PC or run a program that could cause damage to data stored on a PC.
d) Use personal and professional courtesy and consideration when using email.
e) Only use the 'reply all' function if it is necessary for all recipients to see your message.

4.2.2 Unacceptable Use

DO NOT

a) Do not apply an email rule, process or setting that automatically or routinely forwards incoming emails to external or private email accounts.
b) Do not send protectively marked information over the public internet.
c) Do not say, send or write anything you would not say in a letter or on headed paper.
d) Do not use or access another employee or elected members' email without authorisation.
e) Claim to represent the views of the Council, unless authorised to do so.
f) Open a suspected chain email or any suspicious email that cannot be authenticated;
g) Forge a message to make it appear to have originated from another person;
h) Violate the Council's policy prohibiting personal harassment. This includes, but is not limited to, forwarding chain letters and deliberately flooding a user's mailbox with automatically generated mail and sending mail that is deliberately designed to interfere with mail delivery;
i) Do not make jokes or use sarcasm as it can be misinterpreted when using email. Be very careful about the tone of emails.
j) Do not send strictly confidential or commercially sensitive information externally.
k) Do not enter into contractual commitment via email without legal advice.

SECTION 5 INTERNET

5.1 Business Internet Use

5.1.1 POLICY

a) Should you wish to make personal use of Council ICT Internet facilities, the appropriate options must be selected on your application and approved by your 3rd tier Manager.

b) When using the Internet you must not engage in activities that are illegal, harm the organisation's reputation or violate other Council policies. Examples of acceptable and unacceptable use are given below:

5.1.2 GUIDANCE

Acceptable Business Use

DO

a) Use the internet to support communications between the organisation and its partners/suppliers
b) Use the internet for legitimate research purposes
c) Ensure that your use is in support of business and service needs and consistent with departmental and Council policy;
d) Report immediately to your line manager any accidental access of an inappropriate web site.

Unacceptable Business Use

DO NOT

a) Make unauthorised attempts to gain access to company systems.
b) Violate the privacy of users and their personal data.
c) Download, display, use or send any defamatory, discriminatory, obscene, abusive or otherwise material that would be in breach of any legislation or legal obligation placed on the Council;
d) Use or copy material that is protected by copyright law;
e) Facilitate the conduct of any personal contractual obligation;
f) Enter into any contractual obligations unless authorised to do so;
g) Gamble, deal shares, arrange auctions or sell goods online or any other business transactions not related to Council business.
h) Engage in any activity that is illegal in national or international law.

5.2 Personal Internet Use

5.2.1 POLICY

a) The Council's information systems including the internet are provided primarily for business use. The Internet means the accessing of ‘pages’ on the World Wide Web (www) or using services provided by the Internet. The section of the application form relating to personal use of the Internet use MUST be completed and authorised by your 3rd tier Manager. If access is allowed, employees and members must not abuse the privilege by wasting Council resources, including their work time.

b) In addition to the statements contained for business use of the Councils ICT assets - the following sets out what is and what is not acceptable personal use.

5.2.2 GUIDANCE

Acceptable Personal Use

a) Use for legitimate research purposes
b) Use that is consistent with departmental and Council policy
c) Use good password practice to deter potential intruders
d) Report immediately to your line manager or, in the case of elected members, Member Services, any accidental access of inappropriate web content

Unacceptable Personal Use

a) Excessive use of system and system resources that interferes with the performance of your duties or potentially adversely affects the availability of system resources for legitimate Council business
b) Unauthorised attempts to gain access to any company system. Access attempts of this nature will be dealt with under the disciplinary procedures or in the case of members, may be deemed to be in violation of the Code of Conduct.
c) Under no circumstances must any employee or elected member connect to or from a Council owned computer to any non-Council owned, or personal computing device, using any connections or wireless technology without prior approval from the ICT Head of Service.
d) Use for commercial or electoral canvassing purposes

DO NOT

e) Post statements that are defamatory, misleading or false about the Council, its partners, or any other organisation or product.
f) Post or disseminate the Councils confidential information of any type outside the business including to a home address via email.
g) Let others use your Internet account for personal use. The intended user is responsible and accountable for any searches or actions that are carried out with their account and under their name.

SECTION 6 MOBILE AND OTHER COUNCIL SUPPLIED PHONES

6.1 Introduction

This policy defines the responsibilities of employees and elected members and the Council in managing the use of mobile phones. This applies also to personal PCs that are enabled for making or receiving telephone calls, and to personal calls made on other council supplied phones including via Skype for Business.

6.2 Responsibilities

Certain employees and elected members are issued with a Council mobile phone for the performance of their duties. The phone remains the property of the Council and may be withdrawn at any time.

6.3 Use of Council supplied Phones

a) Council mobile phones will be normally allocated to named employees and elected members who will remain responsible for their use. Departments issuing pool phones will keep a record of all employees who are issued the phone.

b) Employees and elected members must pay for all personal (that is, non-work) calls/texts billed to the mobile held in their name and also for personal calls made on other council supplied phones. Where the Council requires the employee at short notice to work additional hours, or otherwise for health and safety reasons to make contact, then an essential call in this respect that might otherwise be deemed to be non-work, shall be deemed to be work related. This can be done in several ways dependant on the procedures within each department.

c) Failure to declare personal use of Council mobile phones may result in disciplinary action.

d) Employees and elected members are advised not to let others use their allocated Council mobile phone unless it is for Council business or an emergency.

6.4 Health and Safety

Employees and elected members must abide by all the Council’s Health and Safety guidelines.

6.5 Security

a) Employees and elected members should take due care of the mobile phone at all times so that it is kept in good working condition and safe at all times. Any loss, damage or theft must be reported to the ICT Service Desk as soon as is practicable and must also be reported in accordance with the Council’s Data Breach procedure.

b) Employees or elected members may not insert a personal SIM card into a Council mobile phone.

c) The phone must be PIN code protected and kept locked at all times to minimise security risks, particularly if the phone is stolen.

6.6 Modifications and Use of Mobile Phones

a) Employees and elected members may change their phone covers (at their own expense) or use any of the modifications available on the mobile phone's menus, providing that such changes are not offensive or bring the Council into disrepute.

b) Employees and elected members will be held liable for any unacceptable phone calls or text messages sent from, or stored on, the mobile phone allocated to them. Such actions may be regarded as gross misconduct under the Council's Disciplinary Policy.

6.7 Courteous Use of Mobile Phones

Mobile phones should be switched off during meetings, lectures, seminars, training course etc. except in very exceptional circumstances where it is vital to make or receive an urgent call. In such circumstances you should adjust the phone to 'silent' mode and alert colleagues to the fact an urgent call needs to be made or is expected.

SECTION 7 SOCIAL MEDIA

7.1 POLICY

7.1.1 Access to Social Media sites such as Twitter, Facebook, YouTube etc. using Council resources is permitted to assist identified employees in the performance of their duties, and to assist elected members to support the communities that they are elected to represent where they deem this to be required by them. Such use where authorised must solely be under the terms of the Council's Social Media Policy.

7.1.2 Personal use is discouraged, however occasional and reasonable personal incidental use is permitted provided that it does not interfere with the performance of staff contract/duties, nor compromise the Council.

7.1.3 There should be no use by elected members to promote any political parties or political agenda on Council social media channels. Members should remember that the use of Council supplied resources in support of any party political or associated campaigning purposes, as defined by the Standards Commission, is not permitted and is governed by the Councillors Code of Conduct.

7.1.4 Access to Social Media sites for employees is governed by the Employees Code of Conduct. Abuse of access to Social Media sites may result in disciplinary action being taken under the terms of the Council's Code of Disciplinary Procedures.

7.1.5 It is important to remember that views and opinions expressed on Social Media sites can be used as evidence in a court of law and may also be disclosed under certain provisions of the Data Protection Act 2018 and GDPR 2018.

7.2 GUIDANCE

7.2.1 Full guidance on the use of Social media is set out in the Council's Social Media Policy. This policy sets out the type of situations when access should be granted to employees. The main reason for granting this access should be set out on the AUP form when requesting this access. The guidance also describes the principles to be followed for various different types of use of social media sites.

APPENDIX 1 ICT INFRASTRUCTURE PRIVACY NOTICE

ICT Infrastructure Services

Your Personal Data

What Information do we need?

Argyll and Bute Council will act as the 'Data Controller' for the personal data you provide to us. The Data Protection Officer, who is responsible for ensuring personal data is managed in accordance with data protection legislation, can be contacted as follows:

Address: Governance, Risk and Safety Manager, Argyll and Bute Council, Legal and Regulatory Support, Kilmory, Lochgilphead PA31 8RT.

Email: data.protection@argyll-bute.gov.uk

Telephone: 01546 605522

We will only collect personal data about you which does not include any *special categories* of personal information about you (also known as '*sensitive personal data'*). Specifically:

- Network activity logs (includes VPN and Server logins)
- IP addresses records linked to user accounts and devices
- Telephone (incl. mobile) call logs
- Skype for Business activity and diagnostic logs
- Internet activity including websites visited
- Database Activity / Audit
- E-mails (3 years + current year)

Why do we need this information?

You have chosen to connect to Argyll and Bute Council's ICT network and use the Council's IT equipment. The information collected will be required to monitor data activity on the network to ensure security and legal compliance. Monitoring is undertaken to protect the Council from potential misuse of these electronic communications, and to assist IT staff in the delivery of service. The Council regularly reviews its monitoring procedures to ensure that internet and email monitoring does not become intrusive.

The legal basis for collecting your information in these circumstances is Article 6 (1) (b) of the General Data Protection Regulation. This processing is necessary for the performance of a contract to which you are a party, i.e. your employment contract. The processing is necessary for the protection of data and network integrity and the prevention of misuse of computer equipment. (*See also* [1] *Ref: Privacy Notice for Staff / Members*)

[1] *Available from HROD/ Member Services*

What we will do with your information?

Where required, your information will be processed by the Council ICT service which includes the provision of reports to managers regarding inappropriate use.

Your data will be stored on servers located within the United Kingdom and EU. We will take all reasonable steps to ensure that your data is kept secure, and more information on how we do this can be provided by contacting the Data Protection Officer (contact details can be found above).

How long will we keep your information?

General user activity data will be kept for a maximum of 1 year, then it will be disposed of securely. Email is archived for 3 years (plus current year). If your correspondence becomes part of a file in relation to a service or disciplinary issue, legal action etc., it may be kept for longer – this will depend on the nature of the issue. ([1] *Ref*: *Privacy Notice for Staff / Members*)

More information on our retention policy and relevant privacy notice can be obtained from the Data Protection Officer.

Automated Decision Making

No automated decision making will take place.

Your Rights

When you provide information to the Council, you will have the following rights:

- to withdraw consent at any time, where the legal basis specified above is consent (not applicable)
- to lodge a complaint with the Information Commissioner's Office – see below for details
- to request access to your personal data – please contact the Data Protection Officer if you wish to submit a request.
- to data portability, where the Legal basis specified above is i) consent or ii) performance of a contract (not applicable)
- to request rectification or erasure of your personal data, as far as the legislation permits – please contact the Data Protection Officer and provide details of what data you wish to be rectified or erased.

You can find out more about your rights in relation to data protection here: www.argyll-bute.gov.uk/data-protection or from the Data Protection Officer by telephone or in writing, as detailed above.

Information Commissioner's Office
The ICO is the UK's independent body set up to uphold information rights.

> Information Commissioner's Office
> Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
> Telephone: 0303 123 1113
> Email: casework@ico.org.uk

The Information Commissioner's Office – Scotland

45 Melville Street, Edinburgh, EH3 7HL
Telephone: 0303 123 1115
Email: Scotland@ico.org.uk
Note

This Privacy Notice applies to information provided to the Council by individuals within our general correspondence systems. If your enquiry is progressed by a particular service and the content of this Notice is not applicable, then another, service specific, Privacy Notice will be provided to you.

APPENDIX 2 ACCEPTABLE USE APPLICATION FORM

Registration for staff Business and Personal Use of the Network, E-Mail, MS SkypefB, Internet, MS365, Council Mobile Phone and access to Social Media sites

Return completed and authorised forms to the ICT Service Desk, Kilmory.
Fields marked * must be completed before processing

NAME*			
POST*			
DEPARTMENT*			
SERVICE			
SECTION*			
LOCATION*		**Telephone No***	
Access Required* Yes or No should be ticked for **all** services as required. If neither box is ticked for any service, ICT staff will return the form to you for completion.	1. Business use of the Network ☐ Yes **Business Use of the Network is mandatory prior to registration for email or internet use** VPN access ☐ No **VPN access will be given by default but if it is not required, tick the box**		
	2. Use of the Email system ☐ Yes ☐ No (includes business and personal use)		
	3. Use of MS Skype for Business (SfB) ☐ Yes ☐ No (includes business and personal use)		
	Ledger code for external calls		
	If a specific telephone number is required, please indicate the number.		
	4. Use of MS365 (including MSTeams and MS365 apps) ☐ Yes ☐ No (includes business and personal use)		
	5. Business use of the Internet ☐ Yes ☐ No		
	6. Business use of a Council mobile phone ☐ Yes ☐ No		
	Mobile Phone Number if known		
	Is this a shared phone?	☐ Yes ☐ No	
	7. Personal use of the Internet ☐ Yes ☐ No Reason :		
	8. Personal use of a Council mobile phone ☐ Yes ☐ No If you are given approval for personal use of a Council phone, you must use the Vodafone Split Billing software to identify personal usage and pay for all personal calls and texts via salary deduction. If you are applying for personal use, the following additional information is required :		

	Employee Number	
	Pay run	
	9. Access to Social Media Sites ☐ Yes ☐ No Reason:	
Reason for Registration*	☐ New User (√ appropriate) ☐ Re-Registration of Existing User	
Post status	Is this a seasonal/casual/temporary post? ☐ Yes ☐ No If Yes, what is the expected length of employment: ________________	

Only equipment that has been supplied or approved by ICT for use on the Council Network may be connected to any terminal or Council PC/laptop/tablet or phone.

The Council provides access to the Internet to make information available in support of its business, for research and education purposes, and to improve the efficiency of the Council's communications. The advantages provided come with a significantly greater element of risk to the confidentiality and integrity of information. Although the Council and its partners do everything within their powers to reduce security risks, the very nature of the Internet means that it is inherently insecure. All users should, therefore, be aware of the risks involved when using the internet. The following terms and conditions apply to Internet usage:

- ICT will determine the most appropriate Internet access method.
- No onward connection will be allowed from the Council's network system.
- The applicant must read and agree to abide by Argyll and Bute Council's ICT Acceptable Use Policy.
- It remains at the Council's discretion to withdraw these facilities at any time.
- The Council reserves the right to prohibit access to certain specific newsgroups, web pages and other Internet resources.

Any violation of the ICT Acceptable Use Policy may result in disciplinary procedures being initiated. Some violations may also constitute a criminal offence and may result in legal action.

To be completed by the member of staff	
I have read and understand Argyll and Bute Council's ICT Acceptable Use Policy and agree to comply with the policy including the terms and conditions contained in this registration. I have retained a copy of the policy for future reference.	
Signed*	**Date***

To be completed by Executive Director/Head of Service/ 3rd Tier Manager, Education Manager or Head Teacher	
Approval is granted to the above named member of staff to have access to the Council network and, as indicated above E-Mail, MS Skype for Business, Internet, Council mobile phone and access to Social Media sites. This may also include personal use of the Internet and of a council mobile phone. All such use is subject to the terms and conditions of the ICT Acceptable Use Policy	
Signed* **Print Name:**	Date*
Job Title:	

For ICT use only

Form correctly completed and Paper Copy Filed	**Name of Service Desk Operator**		**Date**	
Heat Database updated	**Name of Service Desk Operator**		**Log Number**	
Individual Informed by E-Mail of the outcome of this application	**Name of Service Desk Operator**		**Date**	