Inverclyde council

AGENDA ITEM NO: 12

Report To:	**Policy & Resources Committee**	**Date:**	**15 November 2022**
Report By:	**Head of Legal & Democratic Services**	**Report No:**	**LS/92/22**
Contact Officer:	**Martin Hughes**	**Contact No:**	**01475 712710**
Subject:	**Acceptable Use of Information Systems Policy**		

1.0 PURPOSE AND SUMMARY

1.1 ☒For Decision ☐For Information/Noting

1.2 The purpose of this report is to seek the Committee's approval to an updated version of the Council's Acceptable Use of Information Systems Policy.

1.3 The Council has had this Policy in place for some years. The purpose of the Policy is to seek to mitigate the risks posed to the Council, staff, and others, including service users and partners, from emerging and increased cyber-security and serious and organised crime threats to our operations, data and information. In line with good practice the Policy has been the subject of a recent review to ensure it remains up to date and appropriate.

2.0 RECOMMENDATIONS

2.1 It is recommended that the Committee approves the updated Acceptable Use of Information Systems Policy for the Council.

Alan Puckrin
Interim Director Finance & Corporate Governance

3.0 BACKGROUND AND CONTEXT

3.1 The Council has had the Acceptable Use of Information Systems Policy (the Policy) in place for some years. The purpose of the Policy is to seek to mitigate the risks posed to the Council, staff, and others, including service users and partners, from emerging and increased cyber-security and serious and organised crime threats to our operations, data and information.

3.2 The Council has chosen to update its Policy to reflect the use of new systems and technologies across the Council. An updated Acceptable Use of Information Systems Policy will continue to assist employees and Elected Members to use Council software and devices in a secure manner.

4.0 PROPOSALS

4.1 The Policy applies to all employees of the Council and the Inverclyde Health & Social Care Partnership (IHSCP), as well as Elected Members. It covers the use of the internet, email, social media and audio and video-conferencing via Council ICT systems, whether in Council property or remotely.

The Policy seeks to ensure there is clarity around the following:-

- The understanding of what is and is not acceptable use of ICT systems, especially email, the internet, social media, audio and video-conferencing and mobile phones;
- The awareness that all electronic and voice communications may be recorded and logged;
- The understanding that all files, communications, video and audio recordings may require to be released under the relevant Data Protection and Freedom of Information legislation;
- The understanding of the implications of inappropriate use of ICT systems; and
- That, notwithstanding the above, all employees understand that their rights to privacy will be respected.

4.2 The policy is clear that all information relating to service users and Council/IHSCP operations is confidential. All employees must treat the Council/IHSCP paper-based and electronic information with utmost care. Section 8 provides guidance to employees around the use of ICT systems for remote and home working.

4.3 Whilst ICT systems are provided primarily for business use, the Council/IHSCP will allow a reasonable level of personal use outside working hours, subject to a number of stipulations including that such use does not: -

- Conflict with work or business activities;
- Violate any Council policies or law;
- Involve any inappropriate content (for example as detailed in Section 5 of the policy);
- Involve the use for any business purpose, other than that of the Council/HISCP.

4.4 The Policy sets out the manner in which the use of ICT systems may be monitored by the Council/IHSCP in order to ensure those systems are used in a safe, legal and business-like manner.

4.5 As noted above, the Policy sets out in some detail what is and is not acceptable use of ICT systems, especially email (Section 4), the internet (Section 5), social media (Section 6), mobile phones (Section 9) and audio and video-conferencing (Section 10).

5.0 IMPLICATIONS

5.1 The table below shows whether risks and implications apply if the recommendation(s) is(are) agreed:

SUBJECT	YES	NO	N/A
Financial		X	
Legal/Risk	X		
Human Resources	X		
Strategic (LOIP/Corporate Plan)		X	
Equalities & Fairer Scotland Duty			X
Children & Young People's Rights & Wellbeing			X
Environmental & Sustainability			X
Data Protection	X		

5.2 **Finance**

There are no financial implications directly arising from this report. However, the adoption of the updated Acceptable Use of Information Systems Policy will assist the Council in mitigating against the risk of financial penalties relating to, including fines and compensation from any losses associated with, the Council failing in its information governance duties, including in respect of data protection.

One off Costs

Cost Centre	Budget Heading	Budget Years	Proposed Spend this Report	Virement From	Other Comments
N/A					

Annually Recurring Costs/ (Savings)

Cost Centre	Budget Heading	With Effect from	Annual Net Impact	Virement From (If Applicable)	Other Comments
N/A					

5.3 **Legal/Risk**

Linked to the above, the adoption of the updated Acceptable Use of Information Systems Policy will assist the Council in mitigating legal and other risks related to the Council failing in its information governance duties, including in respect of data protection.

5.4 **Human Resources**

There are human resource implications as all Council staff and Elected Members will be obliged to comply with the updated Acceptable Use of Information Systems Policy, if adopted. This will be supported by information on the Policy being cascaded to all staff and Elected Members, with a toolbox talk that all managers will be expected to use. The roll out of the Policy will be overseen by the Council's Information Governance Steering Group.

A breach of the Policy by a staff member could result in disciplinary action being taken against them.

5.5 **Strategic**

There are no strategic implications directly arising from this report.

5.6 **Data Protection**

Has a Data Protection Impact Assessment (DPIA) been carried out?

	YES – This report involves data processing which may result in a high risk to the rights and freedoms of individuals.
X	NO – Assessed as not relevant as this report does not involve data processing which may result in a high risk to the rights and freedoms of individuals.

While a DPIA was not necessary for this report, the adoption of the updated Acceptable Use of Information Systems Policy will assist the Council in mitigating risk to the personal data- held and used by the Council/IHSCP in the delivery of their services.

6.0 CONSULTATION

6.1 The Information Governance Steering Group, the Corporate Management Team and the trade unions have been consulted on the updated Acceptable Use of Information Systems Policy.

7.0 BACKGROUND PAPERS

7.1 None.

APPENDIX 1

Information Governance & Management Framework

Acceptable Use of Information Systems

Version 3.0

Produced by:
Information Governance Steering Group

November 2022

INVERCLYDE COUNCIL IS AN EQUAL OPPORTUNITIES EMPLOYER

THIS POLICY BOOKLET IS AVAILABLE ON REQUEST, IN LARGE PRINT, BRAILLE, ON AUDIOTAPE, OR COMPUTER DISC.

DOCUMENT CONTROL

Document Responsibility		
Name	**Title**	**Service**
(Information Governance) Solicitor	Acceptable Use of Information Systems Policy	Legal and Democratic Services

Change History		
Version	**Date**	**Comments**
0.1		
0.2	27/12/2006	RS – changes as per meeting 11/12/06
0.3	10/5/07	RS – laptop physical security measures
0.4	14/5/07	RS – format changes
0.5	29/5/07	RS - Extended para 2 – section 1 + added music/video streaming SW
1.0	25/10/2007	Final version for approval by committee
1.1	20/01/2010	Added Appendix 1 for GSx – Personal Commitment Statement
1.2	19/02/2010	Information added wrt removable storage media
1.3	17/03/2010	Inclusion of consultant with Information Governance & Management Working Group
2.0	March 2017	Updated and use of Social Media added.
3.0	November 2020	Updated to reflect GDPR, mobile phone and hosted/cloud/web services.
4.0	13 September 2022	Updated to reflect. comments from IGSG
4.1	13 October 2022	Updated to submit to CMT

Distribution		
Name/ Title	**Date**	**Comments**
Information Governance Steering Group	13 September 2022	Various
Corporate Management Team	19 October 2022	TBC

Distribution may be made to others on request

Policy Review		
Review Date	**Person Responsible**	**Service**
September 2022	(Information Governance) Solicitor	Legal & Democratic Services

1 GENERAL PRINCIPLES

This policy applies to all Inverclyde Council and Health and Social Care Partnership (HSCP) employees and elected members, and any person using Council information systems when working with or on behalf of the Council/HSCP. The policy covers the use of Internet, email and social media via ICT systems as well as equipment security and working from home on Council/HSCP business.

ICT systems include, but not limited to, Council: laptops; tablets; desktops; and mobile phones.

Information and communications technologies (ICT) are an integral part of the business of the Council and the HSCP. The Council gives access to ICT systems, email and the internet to relevant employees, to enhance their ability to perform their duties. The Council/HSCP will always endeavour to be as flexible as it can be in allowing a reasonable level of personal use of email and the internet and such use by employees should always be outwith working hours. However, should this right be abused, the Council/HSCP reserve the right to withdraw personal use without notice.

How employees communicate with people reflects on the individual and on the Council/HSCP. The purpose of this policy is to ensure that all employees: -

- Understand what is and is not acceptable use of ICT systems, especially email and the Internet;
- Are aware that all electronic and voice communications may be recorded and logged;
- Understand that all files and communications may require to be released under the Data Protection Legislation (UK General Data Protection Regulation and the Data Protection Act 2018) or the Freedom of Information (Scotland) Act 2002, or the Environmental Information (Scotland) Regulations 2004 and any updates thereto;
- Understand the implications of inappropriate use of ICT systems; and
- Notwithstanding the above, all employees understand that their rights to privacy will be respected.

All information relating to customers and Council/HSCP operations is confidential. All employees ***must*** treat the Council/HSCP paper-based and electronic information with utmost care.

Downloading, copying, possessing and distributing material from the Internet (or any other source) may be an infringement of copyright or other intellectual property rights. Therefore, in general, employees ***must not*** download or copy any material onto Council ICT equipment, unless the information is clearly for business purposes and provided such download or copy does not infringe copyright or other intellectual property rights.

Whilst ICT systems are provided primarily for business use, the Council/HSCP will allow a reasonable level of personal use outwith working hours, provided that this does not: -

- Conflict with work or business activities;
- Violate any Council policies or law;
- Involve any inappropriate content (e.g. as detailed in Section 5);
- Involve the use for any business purpose, other than that of the Council/HSCP.

Employees may be asked to justify the amount of time they have spent on the internet, or the sites they have visited or the level of personal use of email. Failure to provide a satisfactory explanation may result in disciplinary action, under the Council's disciplinary procedures. (see section 2)

The Council/HSCP will respect all employees' rights at all times and also places a level of trust in its staff to at all times use these facilities professionally, in a respectful manner, lawfully, consistently with their duties and with respect for colleagues.

Employees who do not follow the guidelines in this policy may be liable to disciplinary action, under the Council's disciplinary procedures.

In addition to invoking the disciplinary procedure, the Council/HSCP reserve the right to restrict or deny access to email or the Internet to any employee at work without notice and, in such cases, will give reasons for doing so.

Any employee who is unsure about whether something he/she proposes to do might breach this e-mail and internet policy or is proposing to do something not specifically covered in this policy should seek advice from his/her manager and/or the ICT & Customer Service Manager.

2 MONITORING OF COMMUNICATIONS

The Council will exercise the rights and obligations of a data controller under Data Protection Legislation in relation to staff communications.

The Council/HSCP has a responsibility to both its employees and the organisation to ensure that ICT systems, email and internet access are used in a safe, legal and businesslike manner.

In order to ensure the above: -

- all email, MS Teams or Cisco chat/messaging and voice communication, including incoming and outgoing personal email, and Internet access may be recorded and logged automatically by ICT systems;
- all emails are filtered for inappropriate language, content and attachments; and
- ICT systems automatically prevent access to Internet sites that are deemed inappropriate, because of content or because of the security implications of the technology used within the site.

From time to time, there may be circumstances under which it may be necessary for the Council/HSCP insofar as considered possible to retrieve and use this recorded information. Whenever this is the case, the Council/HSCP will endeavour to inform an affected employee when this is to happen and the reasons for it but the Council/HSCP reserves their discretion to decide whether or not to inform the employee.

Examples of circumstances under which it may be necessary to examine this information include the following:-

- If the Council/HSCP suspects that the employee has been viewing or sending offensive or illegal material. (e.g. racist, homophobic, sectarian, pornography etc);

- If the Council/HSCP suspects that an employee has been using the e-mail system to send and receive an excessive number of personal communications or spending an excessive amount of time viewing websites that are not work related;

- If the Council/HSCP suspects that the employee is sending or receiving e-mails that are detrimental to the Council/HSCP.

Where an employee is absent through illness or on annual leave, the Council/HSCP may require to open emails sent to the employee, where it considers necessary and appropriate to do so. The opening of emails in these circumstances ***must*** be authorised by the ICT & Customer Service Manager and the employee's Head of Service in consultation, where appropriate, with the Head of Legal and Democratic Services

Employees using the Council's e-mail system in the performance of authorised Trade Union duties must also follow any obligations set out in their respective Union privacy policy, as well as the provisions of this policy. Trade Union related correspondence transacted on the Council's e-mail system will be governed by the Trade Union's data protection responsibilities and the Trade Union concerned will be the data controller for any personal data exchanged.

3 USE OF COUNCIL ICT EQUIPMENT

Employees ***must*** take reasonable care of all ICT equipment issued to them. Basic security guidelines for staff using Council owned equipment include:-

- Store laptops or other portable devices out of sight. If a laptop or portable device is used as an office desktop machine, it ***must*** be removed from the desk and stored securely overnight, in a locked drawer or cupboard.

- Rotate storage locations, if possible, of laptops or other portable devices. Changing patterns can make it harder for thieves to prepare for the theft.

- The Council will supply an appropriate carrying case or backpack for transporting the laptop or other portable device safely.

- Keep the laptop or other portable device close at hand. Staff should not leave the laptop or other portable device case unattended, even for a short time. If possible, remain in physical contact with it all times.

- Whilst travelling by car, staff ***must*** ensure that the laptop or other portable device is locked out of sight

in the boot of the car, to prevent opportunistic theft.

Employees ***must not***

- Connect personal digital music/video players to any Council device
- Install or use music or video streaming software, except where express permission has been given by the ICT & Customer Service Manager.
- Store MP3/WMA (or similar) files, AVI/MP4 (or similar) video files on their local or network drives. They may not use the Council network to distribute such files, (Where services require to utilise such files with respect to providing training or other purpose, prior approval from the ICT & Customer Service Manager ***must*** be obtained).
- Download, install or store games, screensavers and/or wallpapers from the internet or from any other source.
- Use Council ICT equipment for any other business purposes, other than those directly related to the Council/HSCP.
- Use these facilities to operate any business and/or service operated by them or a third party.
- Make any attempt to circumvent network security restrictions.
- Take equipment other than authorised, home or move equipment without permission of their line manager.
- Use personal devices for official purposes, e.g. using a private laptop for work related purposes, attending remote or virtual meetings.

4 USE OF ELECTRONIC MAIL

Emails are dealt with in the same manner as a letter, memo or other business communication. Where Employees require to send confidential, sensitive or personal information via email, advice on encryption methods and software should be sought from ICT Services.

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.

Some intended recipients may have rigourous email gateway protocols (or firewalls), which can automatically screen all incoming email for content and source. If this is the case, consider whether this means of communication is appropriate.

Employees ***must not*** **–**

- Send or forward messages which are defamatory, libellious, obscene or otherwise inappropriate. The use of email in this way will be treated as misconduct under the Council's disciplinary procedure. In serious cases this could be regarded as gross misconduct and lead to dismissal.

- Forward any obscene or defamatory email, whether received unwittingly or otherwise and from whatever source, to any other address.
- Impersonate any other person when using email or amend any messages received.
- Open unsolicited email which is clearly not related to Council/HSCP business.
- Open any attachments from unknown senders.
- Respond to or forward any chain emails.
- Forward social emails from friends and colleagues.
- Click on any unknown or suspicious embedded links.
- Use personal accounts for official purposes eg using a private email account for work related purposes.

All email communication is monitored and filtered for inappropriate language, content and attachments. Suspicious emails are quarantined and intended recipients within the Council/HSCP are sent a message detailing the content and ***must*** give approval before the email is released. If the recipient does not wish to receive the message it is automatically deleted. Details of all quarantined messages are retained. Where it cannot be established by ICT that an email or an attachment to an email presents no risk to the Council Network under no circumstances will that email be released.

5 USE OF THE INTERNET

When using an Internet site, employees ***must*** always read and comply with the terms and conditions governing its use.

Employees are ***specifically prohibited*** from downloading and installing software without authorisation from ICT. Any such requests will be judged on whether the software fulfils a business requirement that cannot be provided from the range of software already provided and supported by ICT. ICT will check that the source is safe before allowing installation. ICT is also responsible for keeping a record of the licences for all software used in the Council/HSCP, whether the software was free or paid for. Employees may not download software for non-business related purposes.

Employees are expressly prohibited from : -

- Downloading any material that is copyright protected unless authorised to do so by the copyright owner;
- Downloading any images, text or material which are obscene or likely to cause offence (e.g. racist, sectarian, pornography etc);
- Introducing any software which has not been authorised (either from on-line or other sources) by ICT;
- Seeking to gain access to restricted areas of the network without appropriate managerial authorisation;

- Knowingly seeking to access data which they know or ought to know to be confidential unless authorised to do so;
- Introducing any form of computer viruses;
- Carrying out any 'hacking' activities;
- Opening any email via web mail accounts. E.g. Yahoo Mail, Google. etc unless authorised to do so.
- Using unauthorised cloud storage such as DropBox, Google Docs and similar applications for Council data without permission from ICT.

For information, the following activities ***are criminal offences*** under the Computer Misuse Act 1990: -

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

ICT have implemented filtering software that prevents access to sites that are deemed inappropriate because of content or because of the security implications of the technology used within the site. The software monitors and logs all sites visited by council employees and employees are directed to a warning page when a blocked site is accessed.

Where staff are involved in creating, amending or deleting the Council/HSCP web pages or content on the Council/HSCP web sites, such work should be consistent with their responsibilities and be in the Counci/HSCP best interests. Employees ***must*** always ensure that the proper vetting procedures have been complied with and the information is accurate and up-to-date.

6 USE OF SOCIAL MEDIA

The Council and HSCP recognise that social media has become part of everyday life for employees and can be used positively. All Council/HSCP employees should be aware of their conduct and responsibilities when communicating online and using social media sites. The purpose of this guidance, therefore, is to make clear the conduct and behaviours expected of employees of the Council/HSCP who use online communication methods and in particular social media for business and personal use.

When engaged in online activities, including the use of social media, employees are reminded that the Council has a number of policies and procedures which clearly detail the standards of conduct and behaviour expected. These include:

- Code of Conduct for Employees;
- Media and Social Media Protocol;
- Dignity & Respect at Work Policy
- Data Protection Policy;
- Data Protection Breach Protocol;

- Information Sharing Protocol;
- Information Security Guidelines.

Councillors are also reminded of their duties and obligations in the Councillors' Code of Conduct, and related guidance, including the Improvement Service's #FollowMe guide to social media for elected members in Scotland.

Online communications and social media includes software, applications (including those running on mobile devices), emails and websites, which enable users to interact and create and exchange information online. These include, but are not limited to:

- Blogs;
- RSS feeds from other websites;
- Social networking/messaging sites such as Facebook, Twitter, Whatsapp or LinkedIn;
- Photo sharing sites such as Flickr;
- Content sharing or bookmarking sites such as Digg and Delicious;
- Customer feedback sites such as Yelp;
- Video sharintg sites such as YouTube;
- SMS (text) and instant messaging programmes such as, MSN Messenger and BBM.

Employee responsibilities when at work

- Employees permitted to access social media sites such as Facebook and Twitter on the Council network for business purposes must have this access authorised by an appropriate manager who must confirm that there is a legitimate business need for access.

- Employees should be aware that social media can encourage casual and informal dialogue and very often innocent actions can easily be misconstrued or manipulated. Electronic messages are not anonymous and once information is online the author relinquises control of it. Social media sites archive content posted, even when deleted from online profiles.

- Where employees bring their own personal mobile devices into the workplace, they must limit their use of these devices in relation to personal use of social media to official breaks, such as lunch breaks and outwith working hours. Working hours means the period of time that the individual spends at paid work (this is highlighted in the individual employee's contract of employment).

- The expectation of an employee's behaviour when interacting with social media is no different from the expectation of their behaviour when dealing with other methods of communication, such as face-to-face or on the telephone. However, as with all other forms of communication, there may be circumstances where an employee's participation with social media is brought to the attention of the Council/HSCP. Any incidents of unacceptable or inappropriate use of social media will be investigated by the Council/HSCP and could result in disciplinary action, including dismissal.

Employee responsibilities when not at work

- All employees are responsible for any information they make available online whether this was posted during work hours, during breaks or when not at work. The Council/HSCP considers employees to be responsible and accountable for information contained on their social networking page or blog.

Employees need to be aware of what is posted/uploaded to sites they control and that they would be expected to manage any inappropriate material responsibly and appropriately. If an employee comes into contact with any inappropriate material outwith their control, it is expected that this too is managed appropriately.

Safer use of social media

Using online communication and social media can be a great way of keeping in touch with family, friends, and work/professional colleagues. To avoid any conflict between your personal use of social media and your employment with the Council/HSCP, you should:

- Think twice before posting anything about the Council/HSCP, your job or your colleagues;
- Not, or not appear to, promote, encourage or express any personal or political views/opinions which may bring the Council/HSCP into disrepute or harm the Council/HSCP reputation, or breach any of the Council's other policies. If in doubt, don't post it;
- Manage your privacy settings and keep them under review;
- Regularly review your settings to ensure you know who has access to your information;
- Do not use the Council/HSCP logo or branding materials in personal social networking accounts;
- Share information in accordance with the Council's Information Sharing Protocol.
- Comply with copyright and data protection laws, as defamation/libel and data protection laws still apply online.

Employees should speak to their manager if they believe they are being targeted online or believe that personal information may be used in a manner that might compromise their professional status.

Unacceptable use of social media

Examples of unacceptable and inappropriate online activity and use of social media, whether made during working hours or otherwise, are:

- Offensive comments in relation to any employee including management or colleagues or service users of the Council/HSCP;
- Using photographs or video footage of an employee or service user of the Council/HSCP without their permission;
- Disclosure of personal, sensitive or confidential information gained during the course of your employment without authorisation. Unauthorised disclosure could constitute misconduct/gross-misconduct in accordance with the Council's disciplinary procedures;
- Posting comments, content, media or information that could bring the Council/HSCP into disrepute.

Legitimate concerns about the Council/HSCP employees should be addressed through the appropriate human resources policies and procedures, such as the Council's grievance procedure or the Dignity & Respect at Work Policy. Where, through investigation, it is found that the use of social media has been unacceptable, this may lead to disciplinary action being taken and could lead to dismissal.

Inappropriate online behaviour can result in criminal action or in some instances civil action brought by others. Employees should also be aware that in circumstances where their behaviour is unlawful i.e., a hate crime incident such as sectarianism, racism or homophobia, the Council/HSCP will report this to Police Scotland.

7 ICT SYSTEMS SECURITY

Employees ***must*: -**

- Not use ICT systems in any way that may damage, overload or affect the performance of the system or the internal or external network.

- Ensure that all confidential information is secure and used only for the purposes intended and is not disclosed to any unauthorised third party.

- Keep their user names and passwords confidential at all times.

- Ensure that they lock their computer whenever they move away from it for any length of time (press 'Ctrl-Alt-Delete' simultaneously then click lock computer. This will ensure that the machine can only be unlocked with the original password.)

8 REMOTE, HOME WORKING AND USE OF USB MEMORY DEVICES

This section applies to the use of Council laptops or other portable devices and PCs when accessing Council/HSCP systems from outwith Council/HSCP premises e.g. home access.

Where employees have been given the facility to access the Council network from home, or any other remote location, they will be provided with a Council owned laptop or other portable device or desktop PC. Employees must not use their own equipment or devices for Council/HSCP work purposes.

No employees should seek to take a Council ICT system, including laptop or other portable device, to a country outside of the United Kingdom, save with the prior written consent of their Head of Service and the ICT & Customer Service Manager, and only after first agreeing to comply with any reasonable conditions their Head of Service and the ICT & Customer Service Manager impose in respect of the same.

Where a temporary requirement for a USB memory device is identified, the ICT service desk will issue a device from a centrally held stock. It will be issued for a fixed period of time and only for the purposes identified in the request. The Individual will be fully responsible for the safe use and management of this device and the consequence of any data loss should be understood and acknowledge.

Use of Council owned laptops or other portable devices and PCs is covered by Display Screen Equipment Regulations 1993. A display screen equipment (DSE) assessment is required and in some instances a home

visit may be carried out by the Council's health and safety officer to ensure home workstations comply with the requirements of the regulations.

All employees ***must:***

- Password protect any work which relates to Council/HSCP business, where the work in question could reasonably be considered to be of such a sensitive or confidential nature that such protection is sensible;
- Position themselves so that work cannot be overlooked by any other person;
- take reasonable precautions to safeguard all passwords and the security of any computer equipment on which they do Council/HSCP business;
- apply an appropriate level of security to any personal data which comes into their knowledge, possession or control through their employment with the Council/HSCP, so that the personal data is protected from theft, loss, destruction or damage and unauthorised access and use;
- inform the police and ICT as soon as possible, if a laptop or other portable device in their possession or any computer equipment on which they do the Council/HSCP work has been stolen;
- ensure that any work which they do remotely is saved on the Council's network or transferred to the Council's network as soon as reasonably practicable.

9 MOBILE PHONE USE

Employees are expected to exercise due care when making telephone calls and using mobile messaging, to ensure that they maintain the standards of professionalism the Council expects of their position.

The Council reserves the right to monitor and record/log individuals' use of Council owned mobile device systems for its lawful business purposes. The Council's employees must not expect privacy whilst using Council equipment for the purposes of communicating. The Council may be required to disclose voice recordings to third parties for legal reasons, which may include requests made under the Data Protection Legislation or Freedom of Information (Scotand) Act 2002.

Employees *must: -*

- Use the phone in connection with normal business

Employees *must not*: -

- Allow the use of Council phones by unauthorised person(s);
- Download Apps without the approval of ICT Services;

- Incur international roaming costs unless pre-authorised by your manager;
- Use phones in a manner that could bring the Council into disrepute;
- Send SMS or MMS messages that could contain discriminatory, abusive, racist, homophobic, pornographic, obscene, illegal, offensive, potentially libellous or defamatory content;
- Send personal and/or sensitive data using SMS or MMS messages without verifying that the Council has the legal powers or explicit consent to do so;
- Use a Council number to promote any external private business;
- Use a Council phone to contact premium rate numbers;
- Remove the Council SIM card for any purpose (unless explicitly told to do so by a member of the ICT Service Desk as part of fault diagnosis/repair);
- Transfer the SIM Card to any personal device;
- Use personal laptops, personal mobile phones, personal email addresses; Facebook Messenger or WhatsApp Groups to send personal information. Please note that this list is not exhaustive.

10 VIDEO AND AUDIOCONFERENCING

Employees should note that this Policy also applies to any use of video and audioconferencing such as use of Microsoft Teams, Webex, Cisco Jabber etc. Please note the following in relation to use of video and audioconferencing:-

- Council provided facilities for video and audio conferencing should be used primarily for business purposes, however there is discretion for personal use where appropriate and necessary to do so, for example in emergency circumstances, as provided for under Section 1 above in relation to the use of ICT systems.
- When organising a video or audio conference, care must be taken to ensure that you only invite the correct parties to attend. Please take particular care when inviting external parties.
- Please do not proceed with a video or audio call if an unauthorised attendee is present.

For all use of video and audioconferencing, regardless of being provided by the Council or a Third Party, professional standards of behaviours are expected of our users at all times, and any Council approved protocols for use of the same must also be adhered to.

Employees must:-

- Make all participants aware prior to the start of the call if the video or audio conference is to be recorded for subsequent broadcast.
- Be mindful of their surroundings and who else is around them if discussing details about service users, other staff and/or other sensitive material.
- Ensure there is nothing visible in the background of your call that may be damaging to the reputation or professional image of the Council.
- Be aware that both video and audio recordings plus the content of online chat discussions may be regarded as Council records and may have to be released under Freedom of Information and Data Protection legislation.
- Use their Council user account to register, organise and invite attendees.

Employees must not:-

- During calls, download files from untrusted sources.

11 DATA PROTECTION

On occasion, Council/HSCP employees may possess or control personal data. If you are collecting or sharing personal data on behalf of the Council then please note the following Council Policies/Procedures on handling information:-

- Data Protection Breach Management Protocol
- Data Protection Policy
- Code of Conduct for Employees
- Information Sharing Protocol
- Policy for the Retention and Disposal of Documents and Records Paper and Electronic

When in possession of such personal data, employees ***must: -***

- Keep the data confidential and not disclose any information to any other person unless authorised to do so by the Council/HSCP.

- Familiarise themselves with the provisions of the Data Protection Legislation and comply with its provisions.

- Process personal data strictly in accordance with the Data Protection Legislation and other policies and procedures issued by the Council.

- Not make personal or other inappropriate remarks about clients or colleagues on manual files, computer records or any other communication, since the subject of such remarks has a right to see information the Council/HSCP holds on that individual.

Inverclyde Council and the HSCP views any breach of the Data Protection Legislation and its data protection policy as potentially gross misconduct which may lead to summary dismissal under its disciplinary procedures.

If an employee makes or encourages another person to make an unauthorised disclosure knowingly or recklessly, they may be held criminally liable.