Pembrokeshire Council
Cyngor Sir Penfro

IT SECTION

# IT Security, Internet, Email, Skype for Business and Telephony Policy

## Document Revision History

| Version No | Comments | Author | Date of Issue | Status |
|---|---|---|---|---|
| 3.0 | | Hylton Davies | 01 February 2009 | Complete |
| 3.1 | | John Roberts | 01 September 2010 | Complete |
| 4.0 | Review with updates for Skype for Business, Smarter Working and Telephony. | Lee McSparron | November 2016 | Complete |
| 4.1 | GDPR additions. | Matthew James | January 2019 | Complete |

## Contents

## 1.0 Introduction

1.1 The following document applies to everyone who makes use of The Council's Corporate Network. This includes all employees and staff including Heads of Service employed in schools, and those who utilise the network e.g. business managers, school administrators. This policy also applies to all individuals who may use the Corporate network for their work; including Heads of Service seconded from other organisations, working within a SLA agreement between agencies and it includes individuals on work experience, apprentice schemes and volunteering.

1.2 The Council attaches great importance to ensuring the confidentiality, security and accurate processing of information held in computer systems and the physical security of equipment itself.

1.3 The rules and procedures set out in this document are designed to ensure that computer equipment (hardware), software, systems and data are maintained in a secure and controlled environment.

1.4 Computer equipment includes Personal Computers (PC's), Laptop Computers, tablet computers, mobile phones, smart phones, Personal Digital Assistants (PDA's) storage devices, printers and other peripherals in all directorates of the Council.

1.5 This document should be read in conjunction with the Council's Disciplinary Procedure and Code of Conduct a copy of which are available on the Council's intranet.

## 2.0 Computer Equipment (Hardware)

2.1 The Directors and Heads of Service are responsible for computer equipment under their control to ensure its proper use. Please refer to the Council's Financial Regulations (117-119) regarding acquisitions etc. The IT Section maintains a corporate database of computer equipment for support purposes, and any new acquisitions should be notified to them without delay. Once a device has been replaced the IT Section will be responsible for maintenance and make decisions on the disposal / re-use of all IT equipment including obsolete equipment and devices.

2.2 The use of equipment for purposes not directly connected with Council business is forbidden except with the express permission of a Director or appropriate Head of Service. Any permission for use must be in accordance with this policy.

2.3 Only persons authorised by the Director, appropriate Head of Service or an officer delegated to do so may operate computer equipment. In order for access to be granted, the "Network User Request" form must be completed and

forwarded to the IT helpdesk. The Head of Service authorising a User access are responsible for ensuring Users are made fully aware of this and other related Council policies.

2.4 Network Attached Computer Systems not supplied by I.T. are **NOT** to be connected to the Council's Wide Area Network, except on the authority of the IT Infrastructure Manager.

2.5 No telecommunication, whether dedicated or otherwise, is to be made between any computer equipment within the Council and any computer equipment outside the Council, except on the written authority of the IT Infrastructure Manager. i.e. Users must not set up any remote access facilities to any Council computer system without written authority.

## 3.0 Computer Software Systems and Data

3.1 All computer software, systems and data developed for the Council are to be used only for the purposes of the Council, unless permission is expressly given by the Head of IT.

3.2 Where software is to be produced specially for the Council (i.e. bespoke), members of staff involved in negotiating the contract must ensure in conjunction with the Head of IT that, where possible, copyright will be vested in the Council.

3.3 All databases and spreadsheets (or other computer systems) generated within Directorates must be done using approved Software Packages and Users are responsible for ensuring that if they record personal information it complies with the Data Protection Act 2018.

3.4 Council data must be stored on council hardware. No Council data should be copied to privately owned computers including devices such as personal removable memory sticks or private cloud storage such as Sky Drive.

3.5 Council data must not reside on local devices for longer than is necessary. Where data is captured on a local device it must be transferred to Central Storage as soon as practically possible.

3.6 The IT section under instruction by a Director or Head of Service or other authorised manager reserve the right to inspect any and all files stored in private areas of our network and other storage media/devices in order to assure compliance with this policy.

3.7 Only Software authorised by a Director or Head of Service in conjunction with the Head of IT, or an officer acting on his behalf, may be installed and used.

3.8 Deliberate unauthorised attempts at gaining access to, copying of, destruction of, alteration to or interference with Computer Programs or Data is forbidden.

3.9 Unauthorised disclosure of information from computer input or output is forbidden. Sensitive and Confidential output **MUST** be shredded.

3.10 Personal Identifiable Information must not be stored on any removable storage device.

3.11 Personal Identifiable Information may only be stored on local storage when the device has been encrypted and it is for a short time period Data should be uploaded to the central storage and deleted from the local device as soon as is practical.

For further information of Information Governance and Data Protection Policies please refer to the Intranet:

http://intranet.pembrokeshire.gov.uk/en-gb/ChiefExec/audit-risk-info/Pages/default.aspx

## 4.0 User Access and Passwords

4.1 Users are responsible for managing their own credentials for access to the network and applications.

4.2 Users should **never** share passwords with other users.

4.3 Computers must never be left unattended when signed on to any system, users should always utilise the 'lock workstation' facility.

4.4 Computers must be signed off completely when not in use and computers and monitors physically switched off at the end of the working day.

4.5 After allocation of their first password by the I.T. Section, all persons are required to enter their own complex personal password. This personal password will be known only to the employee or authorised user, the password must be 8 characters and contain a mixture of alpha and numeric characters.

4.6 Certain computer applications require a further password (application password).These passwords **must** only be obtained from the application administrator to which the application applies, or in his/her absence an officer acting on their behalf.

4.7 User Accounts that have been inactive for a period of 30 days will be disabled on the network. User Accounts that have been disabled for a period of 90 days will be removed from the system.

**4.8 The disclosure of passwords, directly or indirectly (such as written down and not secure) or use of any password but your own, is forbidden, this includes the use of a computer which has been signed on by another user, in which case both parties will have been deemed to be in breach of this policy.**

**4.9 In the case of a user of the Corporate network leaving the authority unexpectedly and or on long term sick. Where access to the individuals area is critical to business delivery, complaint investigation etc access to their area must be requested by a Director and/or Head of Service.**

## 5.0 Reporting of Security Incidents

5.1 Users are required to report information security weaknesses and events immediately to the IT Helpdesk and complete the "IT Security Incident" form. Examples of security incidents are phishing, chain mails, virus alerts, loss of data and Ransomware; IT staff will also log incidents and breaches they determine and escalate as necessary.

## 6.0 General

6.1 Any persons leaving the employment of the Council must return, on or before his/her last working day, all data, manuals, equipment, documentation and any other materials belonging to the Council. Their line manager is responsible for ensuring this happens.

6.2 Directors, Heads of Service or delegated Line Managers are responsible for promptly notifying the IT Section of all staff leavers and other movements, including Head of Service between Directorates or Sections to ensure appropriate authorised access to IT systems is maintained. The Head of Service has ultimate responsibility for controlling access to their service data. In addition, the Head of Human Resources will regularly notify the Head of IT, or in his absence an officer acting on his behalf, of the names of all persons leaving the Council.

6.3 Staff are required by law to comply with the provisions of the Data Protection Act 2018 and General Data Protection Regulation 2016. Further guidance is available from the Information Governance / Complaints division. This is particularly pertinent where systems are procured or additional functionality is added. With the introduction of SMARTER working, users are reminded to be data aware in accordance with the Data Protection Act 2018 and General Data Protection Regulation 2016.

6.4 Staff attention is drawn to the Computer Misuse Act 1990 the salient points of which are attached in Appendix B and form part of the Council's IT Security Policy.

6.5 In addition to Line Managers, members of the IT Section or Internal Audit staff are authorised to make periodic checks to ensure compliance with these policies and procedures.

## 7.0 Violation of Rules and Procedures

7.1 Any violation of the rules and procedures contained within this statement of security policy must be reported immediately to the appropriate Director or Head of Service together with the Head of IT who may investigate the matter if appropriate as required by The Councils Code of Conduct.

7.2 Any deliberate or serious violation of the rules and procedures contained in this statement will be investigated in accordance with the Disciplinary Procedure and this may result in disciplinary action.

***7.3 Violation of the rules detailed in paragraphs 3.1, 3.4, 3.5, and 3.10 will be regarded as deliberate or serious violations, and would be considered gross misconduct and could result in dismissal.***

***7.4 Non-deliberate or less serious violation, whether accidental or otherwise, will be considered following investigation and suitable action taken, which could include disciplinary action.***

***7.5 Abuse or violations of these rules and procedures could involve criminal acts and as such this could require the involvement and investigation by the Police.***

## 8.0 Use of Computers within the Authority

These guidelines are intended to assist all Pembrokeshire Council users of Computers including Laptops, Tablets, Smart Phones, PDA's, mobile phones, Digital Camera and other devices to use them effectively, efficiently and legally.

## 9.0 Security

9.1 Computer equipment and their data are at risk for the following reasons:- physical damage, theft, loss of data, or failure of both hardware and software.

9.2 Care should be taken to ensure that all equipment is as physically secure as possible i.e. locking rooms, securing equipment to desk or wall, built in equipment locks etc. When equipment is transported from one location to another then extra care must be taken to ensure that the equipment is in a state to be transported i.e. hard disks should be locked down etc. and the transport and the destination location is secure. Insurance (if applicable) must be checked to ensure that cover extends to equipment 'in transit'.

9.3 Guidance on this matter can be obtained from the Insurance and Business Continuity Manager.

9.4 All authority data should be held in central locations where it can be backed up, secured and access controlled.

9.5 VIRUSES are more prevalent and care should be taken to ensure that no unauthorised or unlicensed software is loaded onto any computer. If there is a need for new software to be loaded it must only be carried out by a member of the IT Section.

## 10.0 Illegal Storage or Disclosure of Data

10.1 All Computer access control systems must require users to enter a valid user identifier and a unique non-shared password.

10.2 Personal Identifiable Data (PID) must never be stored on non-encrypted portable or removable devices including desktop PC's

10.3 Personal Identifiable data which resides on encrypted removable or portable devices must only do so for short periods of time. It must be transferred to central storage as soon as possible.

10.4 Bulk Personal Identifiable Data must never be stored on any local, portable or removable storage device.

## 11.0 Personal Use of Corporate Hardware, Software and Data

11.1 Games - Certain games come preloaded with Operating Systems, and the use of these by an Employee must be restricted to outside working hours in his/her own time. The loading of any other game onto a Computer owned by the Authority and its use is strictly forbidden.

11.1 Standard packages such as Spreadsheets, Word Processing etc. Personal use of these packages are only allowed for personal development relevant to job function or training.

11.3 Instant messaging software such as Skype for Business or other similar applications should only be used for communication relevant to the business and not for personal use.

11.4 The downloading, storing or manipulating of any non-work related data onto council equipment is prohibited. Any illegal or unauthorised data E.g. MP3's, Films, Music Albums stored or manipulated on council equipment will be treated seriously and staff involved will be subject to disciplinary procedures.

11.5 The connection of any personnel equipment to council PC's via USB ports or other methods is prohibited and may result in their corruption. E.g. MP3 players iPods, mobile phones.

## 12.0 Laptops and Tablets

12.1 The same conditions apply to any device, including Laptops and Tablets as they do to traditional PC's but as they are easily taken off-site special care must be taken to ensure that no unauthorised software is loaded that could introduce a VIRUS e.g. software from a home computer such as games, sample CD's etc.

12.2 All laptops which are removed from or between council premises need to have encrypted hard drives.

12.3 The introduction of a VIRUS through private use will be treated as a disciplinary matter. Laptops (or any Personal Computer) should only be taken home by staff to perform their job functions following specific authorisation by their Line Manager.

12.4 All laptops must be connected to the corporate network on a monthly basis to ensure that all security patches are applied.

12.5 All tablets connected to the Corporate Network will be managed by the Corporate MDM (Mobile Device Management) platform supported by the IT Section.

## 13.0 Working outside the UK

13.1 No PCC IT hardware is to be taken outside of the UK without the express permission of a Director or Head of Service.

13.2 Where permission has been granted, users accessing any PCC services from outside the UK or utilising PCC hardware to access other services (e.g. the internet) in countries outside the UK, must make themselves aware of the countries policy relating security and monitoring of data. Users must be aware of the implication of tariff charges outside of the UK and the costs associated with any use.

## 14.0 Internet, E-Mail, Skype for Business & Telephony Usage

### 14.1 Introduction

The Council invests substantially in information technology and communications systems which enable our Users to work efficiently. It is recognised that Internet, e-Mail unified communications (I.e. Skype for Business messaging) and telephony play an essential role in supporting our business and the way in which Users communicate with people not only reflects on them as individuals but also the organisation.

The Council reserves the right to monitor, access and review an individual's use of ICT equipment, systems, facilities as covered by this policy without the additional consent being required from any employee. Monitoring and surveillance may be undertaken for the purposes of business operations, audit and security or where there is reason to believe that a breach of this policy has occurred.

### 14.2 Operating Principles

The Council will conform with the relevant legislation in force at the time governing the use and monitoring of e-Mails, which principally involves: the *Human Rights Act 1998*, the *Data Protection Act 2018 and General Data Protection Regulations* the *Regulation of Investigatory Powers Act 2000* and the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (S.I. 2000, No. 2699), the Computer Misuse Act (1990) and the Copyright Designs and Patents Act (1988).* All practical steps will be taken to inform users about their legal rights under the legislation in force at the time through the communication of this policy. See Appendices A and B. However, ultimately it is the user who is responsible for their action in compliance with Council's policies and procedures as well as the relevant legislation.

All Internet activity, e-Mails, messaging, Skype for Business and telephony are the property of the Council and are monitored for business and security purposes to ensure that appropriate use is being made of the systems at all times.

The Internet, e-Mail, Skype for Business and telephony are for business use. However, the Council recognises that in certain circumstances, particularly where there is a need to communicate urgently, it may be appropriate for Users to send personal email messages and use the telephone system. Where these limited circumstances apply, messages should only be composed or read during their own time, typically lunch breaks and/or when clocked out and

should be marked with **"PERSONAL"** in the subject line. The use of the employee's Council e-mail address e.g. fred@pembrokeshire.gov.uk for carrying out personal transactions over the Internet is discouraged, as it is likely that these e-Mails will be trapped by the e-Mail monitoring system. Where users need to access internet sites that are non-work related, i.e. internet banking, online shopping, etc. users should ensure that they are clocked out. Where urgent telephone calls have to be made, users should ensure that this is not excessive.

The Council's disciplinary procedures will be available as the vehicle to handle disputes concerning the application of this policy.

The Council will provide suitable awareness mechanisms for Directors, Heads of Service, line managers, human resource practitioners and employee representatives in order to ensure full compliance with this policy and an informed approach to its application.

The procedures set out in this policy are designed to minimise the risk of incurring liability in relation to Internet, e-Mail and Skype for Business usage. Disciplinary action will be taken against any employee who breaches any of the instructions or operating rules contained in this policy, which will include summary dismissal for t committing acts of gross misconduct.

Any employee who considers that the policy has not been followed by someone in respect of Internet, e-Mail, Skype for Business or telephone usage, the results of which could be damaging to co-employees or the Council, or may be illegal in some way, should raise the matter with their immediate line manager, or if this would not be appropriate in the circumstances, with the Head of IT & Central Support Services or the Director of Financial as required by The Councils Code Of Conduct. Employees should be assured that they will not be victimised in any way for raising issues of genuine concern, in good faith; this is also covered in the Council's 'Whistleblowing' Code.

Internet, E-Mails, Skype for Business and other messaging systems are subject to the Freedom of Information Act (FOIA) and need to be filed correctly in the relevant project area.

Any e-mails that contain sensitive and / or personal information **must be** encrypted before being sent.

**Skype for Business must not be used for the sharing of sensitive and / or personal information.**

Where an employee inadvertently does something which breaches this policy, or makes a genuine mistake or the unexpected occurs it should be reported to their immediate Line Manager and/ or the Head of IT.

## 14.3 Monitoring

The Council reserves the right to monitor, at any time, internet, email, Skype for Business and telephone usage, including deleted e-Mails, and the systems upon which such e-Mails are stored and circulated. This right is reserved solely for the purpose of monitoring for business, operational, audit and security purposes.

The IT Section and Internet Audit will review Internet, Email and Telephony activity and analyse usage patterns. They may choose to publicise this data to management to assure the Councils resources are devoted to maintaining the highest levels of productivity.

While an e-Mail or message that is clearly private does not fall within the definition of a communication that is relevant to the Council's business, we maintain a right to monitor such a communication where there is a reasonable suspicion that the content breaches Council policy; for example, transmitting defamatory remarks, is illegal or other inappropriate or offensive content or excessive usage.

The Council exercises the right to intercept e-Mails under the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (S.I. 2000, No. 2699)* ('the Regulations') for the following reasons: to investigate or detect the unauthorised use of the systems, e.g. that this policy is being observed, that no discriminatory or offensive content appears in e-Mails, etc.; to maintain an adequate level of security for our computer systems; to detect any computer viruses; and, to check mailboxes of absent employees.

To exercise its right under the Regulations, the Council must have made all reasonable efforts to inform every person who may use the system that interception may take place. We believe that the notice which is displayed on every PC when sign-on occurs (and the content of this Policy) meets this requirement. As far as external senders of e-Mail are concerned, a statement will be included in any automatically generated 'signature' to outgoing e-Mails.

In exercising its right to monitor e-Mails the Council is conscious of its obligations under the *Data Protection Act 2018 and General Data Protection Regulation 2016* as information derived from the interception of communications is covered by the data protection principles.

## 14.4 Responsibilities

Responsibility for overall ownership, communication and monitoring of this policy rests with the Head of IT, who will review the policy periodically.

Overall responsibility for training people on the use of the Internet, e-Mail, Skype for Business and Telephony systems lies with the individual's supervisor/manager, who may delegate responsibility for training to suitably qualified and accredited trainers and which will include training in use of e-Mail as part of the induction programme. It is expected that this will be undertaken before access is granted.

Overall responsibility for the strategic development of Internet access, e-Mail, Skype for Business and Telephony systems, technological developments and the day-to-day management rests with the IT Infrastructure Manager.

Each individual in the Council who is an authorised user of Internet, e-Mail, Skype for Business and or Telephony is responsible for complying with the rules, procedures, guidelines and good practice statements set out in this policy.

## 14.5 Operating Guidelines

Because a wide variety of materials may be considered offensive by colleagues, customers or suppliers, it is a violation of Council policy to store, view, print or redistribute any document or graphic file that is not directly related to the user's employment with the Council or the Council's business.

The downloading and/or display of any kind of sexually explicit image or document or other offensive or obscene material, e.g. racist, homophobic, anti-religious, paedophiliac, etc., on any Council system capable of constituting any form of discrimination or criminal offence is a violation of our equal opportunity policy. In addition, sexually explicit or other offensive or obscene material **must** not be archived, stored, distributed, edited or recorded using our network or computing resources other than for the purpose of retention for evidence purposes. Any evidence relating to an investigation, prosecution or other legal action **must** be saved in an IT secure area and this area will not be accessible to any officer other than those directly involved with the investigation or proceedings relating to the case. Any such action will be considered as gross misconduct.

The downloading and/or display of any kind of illegal material likely to damage the reputation of the Authority, on any Council system is prohibited. In addition, such material may not be distributed, edited or recorded using our network or computing resources. Any such action will be considered as gross misconduct.

Illegal, racist, sexist, defamatory, obscene, pornographic or otherwise abusive

or threatening messages must not be communicated via the Company's communication systems.

ICT systems, devices, applications or other communication networks such as social media must not be used for what could be considered as a defamatory statement. For the avoidance of doubt, a defamatory statement is one, whether oral or written and whether of fact or opinion, which tends to damage the reputation of another individual or company. Remember that damaging e-Mail may have to be disclosed in litigation or in investigations by other authorities.

Never distribute documents, pictures, music or works of others without the copyright owner's permission. Copying materials which are protected by copyright, without the permission of the copyright owner, is an offence which can give rise to both personal liability and liability on the part of the Council.

## 14.6 Internet

The Council has installed an Internet firewall and filtering platform to assure the safety and security of the Council's networks. We may block access from within our networks to all such sites that we know of. If you find yourself connected accidentally to a site that contains sexually explicit or offensive material or illegal material, you must disconnect from that site immediately and report the occurrence to your line manager and the IT Helpdesk.

On occasions some sections within the authority will require access to research that may trigger the blocked sites. If your require access to certain internet areas as part of normal business purposes, permission from your line manager, supported by your Head of Service or Director must be obtained and forwarded to the IT section for action.

The Council's Internet facilities must not be used to violate the laws and regulations of the United Kingdom or any other nation. Use of any Council's resources for illegal activity is grounds for immediate dismissal and we will cooperate with any legitimate law enforcement activity.

Any software downloaded via the Internet into the Council's network must be carried out by the IT Section. Any such software may be used only in ways that are consistent with their licenses or copyrights.

No employee may use Council's Internet facilities to:

- Download or distribute pirated software or data
- Propagate any computer virus
- Disable or overload any computer system or network,
- Circumvent any system intended to protect the privacy or security of

another user or the council

Any such action will be considered as gross misconduct.

The Council retains the copyright to any material posted on the Internet by any employee in the course of his or her duties.

**Employees may use their Internet facilities for non-business research or browsing during their own time, typically lunchtime, or outside of work hours where approved by their manager, provided that all other usage policies are adhered to. The internet is not to be used for non-work related activities whilst "clocked in".**

**The Council's Internet access is not to be used for any commercial or private business activity use other than which directly relates to The Councils core business.**

Beware of viruses which may be present as part of any file download. Although software tools are in place to scan all file for viruses upon entry to the corporate network, staff are required to take all reasonable steps to guard against viruses being introduced into the Council's computer system or the systems of third parties. Intentional introduction of viruses is a criminal offence under the *Computer Misuse Act 1990*. Concerns regarding any e-mail or attachment should be reported to the IT helpdesk immediately.

Employees may not use Council's Internet facilities to download entertainment software or games, chat rooms or to play games against opponents over the Internet at any time.

Employees with Internet access may not use Council's Internet facilities to download images or videos unless there is an express Council business-related use for the material.

Any employee who attempts to disable, defeat or circumvent any Council security facility will be subject to summary dismissal for gross misconduct.

It is not acceptable for employees to make inappropriate comments about their workplace or colleagues on a social networking website or blog facility, Officers that use social media to defame other officers, elected members or the Council will face disciplinary action. Further detail can be found in the social media use policy.

It is not acceptable for staff to make personal use of websites such as Facebook, Bebo, MySpace, Flickr or Twitter, or to blog, during working hours or using Council equipment or resources. This includes use of their own personal devices such as mobile phones, smart device whilst clocked in.

Any “official” presence on social networking sites must be co-ordinated by the Marketing and Communications team.

### 14.7 Email & Skype for Business

E-Mail and Skype for Business are extremely powerful communication tools, but, if abused, can cause a massive waste of resources.

Its strength is in providing a vehicle to share information with one or more colleagues quickly and efficiently. The benefits are dissipated when Inboxes are always full of inconsequential material for which there is no time to process. Because it is so simple to use, it is easy to fall into the trap of overusing the system. Email and Skype for Business should not be used as a platform for office chat.

Employees are prohibited from sending confidential information by e-Mail to external bodies unless authenticity is established and there is adequate security in place for such transactions. For the avoidance of doubt, confidential information covers items such employee data, customer information, pricing information, and so on; In addition, employees must never send ‘off the record’ e-Mails or Skype for Business communications – nothing is ‘off the record’ where the law requires disclosure of information. This is the case for both internal and external e-mails and Skype for Business communications. Skype for Business should never be used to send confidential information.

Ensure you have correctly spelled your intended recipient's e-Mail address thus avoiding non-delivery or mail failure error messages. Be careful when using global address lists and personal address lists. Check that only recipients for whom the mail is intended have been included.

The Council’s standard e-Mail Server enforces a maximum mailbox size of 240Mb. Once the limit is reached an employee will not be able to send or receive e-Mails. This 240Mb limit includes Inbox, Sent Items and Deleted Items. The size of a corporate email and its attachment is restricted to 25MB

All e-Mails and their attachments which are stored in the recipient’s mailbox on the e-Mail Server which are older than 30days will be automatically deleted. Once these items have been removed there is no way that they can be retrieved.

Employees are therefore instructed to determine whether or not they wish to retain particular e-Mails and their attachments, if so, they should file them electronically in the relevant project area. Delivery confirmations cannot be guaranteed as proof of delivery for e-Mail messages sent across the Internet.

Never access another employee's e-Mail account without appropriate permission or authority, typically, where the employee concerned has given express consent in writing to gain access during that employee's prolonged absence due to holiday, ill health or some other valid reason. Even if such access is granted, never send an e-Mail under the original account holder's name. If there is a need to respond in an emergency, the message should be sent from an individual's own account, headed 'sent on behalf of [*enter your co-employee's name]*'.

If you are unable to access your email, e.g. on holiday, make sure you activate the "Out of Office Assistant".

There will be occasions when it is necessary to send an e-Mail message to everyone on the Council's Address Book. This will usually be used only for emergency or similar messages. The use of this facility will only be possible if approved by a Director or Corporate Head of Service. Once approval has been given, the IT Helpdesk will need to be contacted on 5882 for the message to be distributed.

Users should ensure they are always logged in to Skype for Business and make full use of calendaring facilities to support availability of presence information.

Ensure Email and/or Skype for Business are the most appropriate method of communication for the task.

Skype for Business supports the use of Profile Images. Staff should be reminded of the following when uploading an image to Skype for Business and should:

- *be appropriate and professional,*
- *be the person associated with the Skype for Business User,*
- *be front facing,*
- *does not include additional information within the image (ie, text),*
- *and is reviewed by the user to ensure it remains appropriate.*

Uploading of inappropriate photos may lead to disciplinary action.

When participating with third party contacts you must only share or discuss information in line with established Information Sharing Agreements. Also consider whether Skype for Business is the most appropriate communication method above others including Secure Email, telephone etc.

Skype for Business provides real-time collaboration with participant's including the ability to remote share and control desktops. Users should be mindful to whom they allow control of their desktop to, what content is being presented

and be reminded that the any control will be in the guise of the current logged in member of staff.

**Do not leave unattended remote sessions available to any user at any time.**

Users should immediately contact the IT Service Desk if they suspect abuse or inappropriate use of eMail or the Skype for Business Communication Network.

## 14.8 GCSX Mail Users

The above rules regarding Email also apply to users of GCSX, in addition.

No Bulk e-mails are to be sent across the GCSX network without prior consent. The internal IT Helpdesk will seek this permission on behalf of users and should be the first point of contact.

No email should be sent or forwarded to anybody on a lower security domain i.e. not on a. GCSX e-mail address.

GCSX email should not be used to send emails classified any higher than RESTRICTED.

The size of a GCSX email and its attachment is restricted to 15MB.

For further information on GCSX please see http://pccintranet/content.asp?nav=231%2C236%2C271&parent_directory_id=101

***Communications sent or received by means of the GSi Network may be intercepted or monitored.***

## 15.0 Remote Working

This policy should be read in conjunction with Information Governance and Data Protection Policies.

Individuals working remotely and working SMARTER are responsible for taking adequate steps to ensure the security of Council equipment and information in their possession, including reasonable care of the IT equipment in their possession.

Remote workers and those working SMARTER are responsible for the confidentiality and security of equipment and information handled by them and should not willingly allow anyone who is not authorised by Pembrokeshire Council to use or have access to the equipment, information or documentation.

Remote and SMARTER workers must ensure that sensitive Council information is not viewed or overheard by anyone else in public areas (including their homes).

All remote connections initiated by members of staff will only be permitted using equipment purchased and owned by the Council.

All connections must be made via the Councils corporate solution.

All previous paragraphs of this policy relating to storing and transporting data must be understood and adhered to.

All previous paragraphs of this policy relating to usage of Council equipment must be understood and adhered to.

It is the responsibility of all users to immediately report any actual or suspected breaches in information security to the Head of IT in line with the council's Security Incident Management Policy. Any such incidents must be reported through IT Service Desk.

## Appendix A GDPR Data Protection Principles:

Article 5(1) of the GDPR:

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, transparency')"

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes." (purpose limitation)

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)"

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')"

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')"

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'

Article 5 (2) of the GDPR:

Accountability Principle: The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles.

## Appendix B

### Computer Misuse Act 1990

109. The above Act affects all members of staff, Members of the Council, and the general public.
110. The Act concerns what is colloquially known as ‘hacking’, that is attempting to, or getting into the working parts of a computer or system, which the person doing so knows he/she has no right to access. The Act makes these actions a criminal offence, and any person perpetrating them can be prosecuted.
111. The salient points of the Act are:-
112. The Act makes it a criminal offence for an employee or Member of the Council, as well as outside persons to:-
113. Cause a computer to perform any function with the intent to secure unauthorised access to any computer program or data held in any computer.
114. Committing unauthorised access with intent to commit or facilitate the commission of a further more serious offence.
115. Causing an unauthorised modification of the contents of any computer.
116. A person found guilty of an offence under paragraph 1 above shall be liable on summary conviction to imprisonment for a term not exceeding 6 months, or to a fine, or to both.
117. A person found guilty of an offence under paragraph 2 and 3 shall be liable on conviction on indictment to imprisonment for a term not exceeding 5 years, or to a fine, or to both.
118. The Act applies if you deliberately try, or succeed in getting into part of the computer or system which you know is outside your scope of work. If you accidentally get into a part you do not normally use, or even want to, then of course the Act does not apply.
119. The penalties are harsh because the possible results of these illegal acts could be extremely costly to the Council.
120. The Council will investigate all incidents listed above, and actions under the Act will be seriously considered.