CYNGOR SIR CEREDIGION COUNTY COUNCIL

Information Security Policy

2019

Document Control

Author and service: Corporate Lead Officer Customer Contact
Date approved by Cabinet: 19/02/2019
Publication date: 19/02/2019
Policy Review Date: February 2022

Date	Version	Author	Status
17/10/2011	1.0	Arwyn Morris	Initial Draft
20/10/2011	1.1	Jason Taylor	
07/11/2011	1.2	Arwyn Morris	
22/11/2011	1.4	Arwyn Morris	
20/12/2011	2.0	Arwyn Morris	Final Draft before consultation
30/01/2012	3.0	Arwyn Morris	After Initial Consultation
07/03/2011	3.1	Arwyn Morris	After Union Consultation
10/12/2018	4.0	Arwyn Morris	Review of the policy
10/01/2019	5.0	Arwyn Morris	
10/01/2019	5.0+	Jason Taylor	Updated secure e-mail, password, secure send sections. Homeworking.
19/02/2019	5.0	Cabinet	Approved

Contact Details:

Corporate Manage ICT and Information
Tel 01970 633205 (3205)
Email Servicedesk@ceredigion.gov.uk

Contents

1. Introduction

This document sets out the Information Security Policy (''the Policy'') for Ceredigion County Council (''the Council''). The Council has a duty to meet legislative and regulatory requirements in relation to ICT security and security of information in all other media.

Information is an essential asset to the Council in delivering its services and a consistent approach must be adopted in safeguarding and validating the information stored. It is essential that the Council's systems are adequately protected against physical, technical, business and criminal risks. Such risks include accidental/intentional data disclosure, malicious user damage, fraud, theft, accidental/intentional technical physical changes and natural disasters.

2. Policy Statement

The Council is committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the Council. Information and information security requirements will continue to be aligned with the Council's goals and the Policy is intended to be an enabling mechanism for information sharing, electronic operations, and reducing information-related risks to acceptable levels. In particular, business continuity and contingency plans, data back-up procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to the Policy.

3. Scope

The Policy is applicable to **all** Council staff, elected Members, volunteers, contractors and suppliers of the Council that have access to the Council's information, computers and networks.

4. Objectives

- Protect integrity of data against misuse (accidental or deliberate), loss and any abuse or damage.
- Ensure data access rights are maintained as per classification.
- Ensure systems are accessible and performing properly.
- Make sure that appropriate plans and arrangements are available to deal with disasters and to provide continuity plans for critical services.
- Audit, detect and hold accountable users and services for their use and any misuses of the Council's computer systems, networks and information assets in all media.
- Comply with the Council's legal obligations under the Data Protection Act, Computer Misuse Act, Freedom of Information Act and all other relevant legislation including that set out in Appendix B.

- Identify, classify, catalogue, manage and dispose the Council's information assets and associated risks.
- Ensure that responsibilities for information ownership, management and risk management are clearly defined.
- Comply with the Council's contractual agreements for interconnection with other networks and application systems.
- Ensure users have sufficient training and assistance to enable them to understand and comply with the Policy.
- Develop and maintain documentation and business processes to support the Policy and ensure that these are being properly implemented and adhered to.
- Maintain public confidence in the Council's ability to secure and protect their data.
- Keep all users aware of the limits of privacy while using the Council's information systems, computers and networks in order to meet the security requirements.

5. Privacy and Monitoring

The Council will restrict access to any user that does not accept the Council's information security policy. Logs will be maintained of users' activity. The logs will be monitored and, where appropriate, will be disclosed to line-managers, internal investigators, senior management, auditors, IT staff and other relevant bodies such as law enforcement, external auditors and central government departments.

Any user that logs on to the Corporate ICT services is formally notified that their activity will be logged and monitored. The log files are monitored for any unusual activity and will be used for any investigation of unauthorised activity either on, or using, the Council's systems.

6. Personal Usage

Personal usage is defined as usage of Council resources that is not directly associated with the performance of a user's official Council duties or job description. The Council shall reserve the right to introduce access controls that limit the extent of personal usage.

Personal usage is only permitted where **all** the following apply:

- such use is of a private nature, not for financial gain and does not contravene any other Council policies;
- such use does not incur costs to the Council;
- such use does not disrupt the official business of the Council;

- such use must not involve anything that promotes illegal, sexual, or other activities that contravenes the Council's policies.

Personal usage will be monitored, and where an user's personal usage appears unreasonable it will be reported to his/her line-manager, internal audit, human resources and/or other staff with responsibility for employee performance monitoring, for investigation and action.

7. Consequences

Where appropriate, failure to abide by this Policy will be handled in accordance with the Council's "Managing Employee Performance", "Disciplinary Procedure'' and ''Code of Conduct''. Disciplinary action (as defined by the Disciplinary Procedure) for failure to adhere to the Policy, may ultimately lead to dismissal.

8. Training and Induction

All employees, Members and volunteers of the Council and, where relevant, contractors and third party users shall receive policy and procedural awareness training (including updates) relevant for their function via an electronic method or through formal training events.

All new staff, Members and volunteers must attend formal induction training before being granted access to Corporate ICT Services.

All staff, Members and volunteers must be appropriately security vetted, as part of the appointment process, to the minimum of the baseline personnel security standard (BPSS) that would include ID checks, previous employment checks (confirmation of employment/educational history for the last 3 years), self-certified spent convictions and DBS enhanced or standard (where applicable),which are renewable every 3 years.

9. Incident Reporting

It is the duty of all employees to report any inappropriate use of the Council's ICT systems and misuse of information in any media. Such incidents include loss of data, accidental or deliberate disclosure of data, use of data/systems for personal gain, unlawful use of ICT systems, accidental or deliberate damage to data integrity, etc. All suspected incidents must be reported to the ICT Service Desk and/or Line Manager immediately.

The Council has an obligation to report information security incidents to external government approved bodies such as NCSC, NLAWARP, CISP, ICO and PSNA.

10. Password Controls

Passwords, pin codes and other authentication information issued to an individual user must be kept secret and not disclosed to anyone. Passwords must be changed on a regular basis. Users are responsible for protecting their password and ensuring that it is sufficiently complex that it cannot be easily guessed. Systems will be configured to enforce password complexity and aging.

If a password is disclosed in any way, then the password must be changed immediately.

11. Roles and Responsibilities

All **Users** must adhere to the Policy

All **Managers** are responsible for implementing the Policy within their business area and for ensuring adherence by their staff

Information Asset Owners are the service managers having responsibility for their service information and for classifying information in accordance to the Council's Information Classification standards.

SIRO is responsible for ensuring that management of information risks is weighed alongside the management of other risks facing the Council in areas such as financial, legal and operational.

Data Protection Officer ensures that all staff are aware of the principles they must follow when handling personal information.

IT Security Officer (ITSO) is responsible for the security of all information held in an electronic form. ITSO is also responsible for reporting incidents to Government Computer Emergency Response Team UK (GovCertUK) and other relevant government bodies.

Information and Records Manager ensures that the information resource of the Council is managed as a corporate asset, and assists in establishing the strategic direction of information management for the Council.

IGG has an ICT Governance role to oversee, review and monitor information risks.

12. Review

The SIRO and IGG will formally review the policy annually and amend if necessary. The amended policy will be distributed to all staff.

The policy will be reported to Council on a 5 yearly basis or when significant changes are made.

Policy Section

13. Physical Security Policy

The Physical security policy applies to all Council buildings where Council information is available for access, either via physical access (paper records) or electronic access (computers, whether on or off the Council network). Physical security will prevent physical damage to content and building, theft of equipment and information and physical attack on staff working in the building.

13.1. Access Control to Council Buildings

Physical access to non-public areas in buildings must be restricted to authorised staff only, and no other person must be allowed access without first signing in and then being accompanied by a member of staff. All restricted areas, such as Computer Data Centres, Secure File rooms must at all times have access control and only approved staff will have access.

13.2. Think Security

Everyone has a responsibility to maintain a secure environment and be vigilant in not allowing any unauthorised access. All security doors, and fire doors, must be kept closed at all times. Door codes will not be disclosed, and keys kept securely, and not made available to any unauthorised person. All windows must be closed and locked before exiting the building. All computer equipment left unattended must be in a secure mode (screen locked, logged off or shutdown) and blinds (when fitted) are closed at night for lower ground and ground floor only, to prevent anyone looking into the offices.

13.3. Clear Desk & Safe Screen

At the end of the working day, or when leaving the office for a major part of the day, papers and any files should be stored securely and out of sight.

During the working day ensure that information is not visible to unauthorised persons, both on your computer screen and in paper form.

14. Password Policy

This Password policy applies to all users having access to any information system that requires password access.

14.1. Authentication

All users must be authenticated via an individual password before gaining access to the Council's ICT corporate domain. The users are responsible for safeguarding their password(s) and must NOT share or disclose their

password(s) to anyone at any time. Users must not allow anyone else to use their login details to gain access to the Council's corporate domain.

All passwords for users, application systems, networking equipment and any other ICT device/service must meet a minimum standard of 8 characters long, including at least one numeric and one upper case character, and be changed regularly.

Advice and guidance is available from the NCSC on selecting an appropriate password policy (https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach). Deviations from the standard policy that are based on this guidance can be utilised after risk assessment agreed with the ITSO.

Authentication for network / infrastructure wide administration systems should incorporate 2 factor functionality if that is available.

Any password that is lost or disclosed in any way must be changed immediately. If it is suspected that this loss could result in an inappropriate access to Council data, it must also be reported to the ITSO via the ICT Service Desk.

15. Email Security Policy

This Email policy applies to all staff that have access to a corporate Email account.

15.1. Email Usage

The use of the Corporate Email service is for performance of official duties and any personal emails sent or received must be kept to a minimum. The Council's Email service is provided for the delivery of Council services and must not be used for the delivery of any other business or service.
No emails should be sent to all addressees on the corporate address book. If there is a need to send a broadcast via email, this must be done through the Council's Communication Team.

16. Instant Messaging Usage Policy (Skype)

This Instant Messaging policy applies to all staff that have access to a corporate Instant messaging service (Skype).

16.1. Skype Usage

The use of Skype service is for performance of official duties and any personal messages sent or received must be kept to a minimum. The Council's messaging service is provided for the delivery of Council services and must not

be used for the delivery of any other business, service or non-work related messaging.

17. Internet Usage Policy

This internet usage policy applies to staff, Members and volunteers accessing websites and other network services on the public internet, using equipment or networks supplied by the Council.

17.1. Online Behaviour

All access to Internet based resources will be associated with the Council. In the course of their work, employees must therefore only access internet based resources in accordance with their job description, or requirements, and in accordance with the Council's employee code of conduct.

All users are prohibited from accessing sites that violate the law or could be offensive to fellow users; and may only access sites for personal reasons under the terms and conditions specified under 'Personal Usage' above.

17.2. Transmission of Personal/Sensitive Data

When online, users must be careful as to what they disclose to others. Users must remember that the internet is not a private or a secure communications medium. Users must not transmit or publish anything that may be damaging to the Council or themselves. Privileged or restricted information, as covered in other policies, must not be transmitted without proper precautions. Users should exercise similar care when transmitting protected data.

18. Telephone (fixed and mobile) Usage Policy

This telephone usage policy applies to all users that have access to a corporate telephone line and/or corporate mobile phone.

18.1. Telephone Usage

The use of Corporate Telephone and/or mobile phones is for performance of official duties. The council telephone service (fixed and mobile) is provided for the delivery of council services and must not be used for the delivery of any other business or service. Only nominated council telephone numbers must be published in any public domain (internet, telephone books etc.) and for the purpose of Council service delivery only.

18.2. Personal Calls

Personal calls are defined as telephone calls that are not directly associated with an employee's job description. Personal calls are permitted, provided that the call is kept to a minimum and only when necessary.

19. Network Connection Policy

The network connection policy applies to everyone that connects their device (both council and personal) to the Council network.

19.1. Network Security

Only authenticated and approved devices must be connected to the Council's network for both fixed and wireless connections. The only exception being where the corporate ICT section has provided public or "guest" Wi-Fi access for the convenience of staff, partners or service users.

20. Mobile & Home Working Policy

This Mobile & Home Working policy applies to all users that have access to a laptop/tablet PC, or any other mobile phone device, that enables them to work from their normal place of work or home.

20.1. Mobile Working

For all mobile devices, an access code must be set (Pin code for mobile phones and two factor authentications for laptop/tablets) and the access codes must not be disclosed to anyone to gain access to the device. Users that have been allocated a mobile device are responsible for that device at all times when outside a Council office and must take extra care of the device when in public areas and on public/private transport. Any loss or damage to a mobile device must be reported immediately to the ICT Service desk. When using mobile devices in public areas, extra care must be taken by turning off Bluetooth and wireless connections when not needed. When using a mobile phone in a public area, be aware of other people overhearing your conversation. If you need to take a Council mobile device (laptop or phone) abroad, you will need to get approval from your line manager and only take the device if necessary for work purpose.

20.2. Home Working

Home working introduces additional risks particularly if office facilities or technical support is unavailable.

As an example, producing and handling paper documents at home introduces storage and destruction problems. The lack of secure release printing facilities and access to appropriate shredding or paper destruction facilities may introduce opportunities for loss of information. This may necessitate convoluted processes such as the transfer of materials back to the office for disposal that may lead to loss of personal data when transported.

Other workarounds that introduce similar risks include sending work documents to personal e-mail accounts to work on home equipment. Viewing / editing person or sensitive documents bypasses our technical security controls.

It is the responsibility of staff members electing to work from home or flexibly that the support and setup of their home working arrangements is compliant with other areas of this policy and does not introduce new risks.

Staff are advised to seek advice from their line-manager, ICT Section and/or DPO if they have any doubts about the appropriateness of any home or flexible working location.

21. Computer Software Policy

This Computer Software policy applies to all users that have access to a corporate PC/Laptop.

21.1. Software

Only software approved by corporate ICT will be installed on PCs/Laptops (including Councillors' Laptops) and all software must be licensed for Council use. Software can only be installed by corporate ICT with appropriate administration rights. No other user will have administration rights to install/amend or remove software, or alter configuration settings, on any PC/Laptop. Requests for installation of software for personal use will not usually be accepted.

22. Computer Hardware Policy

This computer hardware policy applies to all users that have access to a corporate PC/Laptop.

22.1. Staff Computer Hardware Usage

The use of computer hardware is for the delivery of Council services and must not be used for personal gain, or financial and business purposes. Care must be taken of all computer hardware, especially laptops, and users must always use the provided laptop carry case when they are used from the office. When any hardware device supplied by the Council is taken from the office, the user is responsible for the safeguard of that device until it is returned. Any loss or damage must be immediately reported to the ICT Service desk.

Care must be taken at all times to ensure that computer equipment is physically secure (not left unattended outside the office) and that the appropriate access lock is enabled on all PC's and laptops that are left unattended. All security

features enabled on computer equipment (virus protection, encryption etc.) must not be turned off at any time.

22.2. Councillors' Computer Hardware Usage

Councillors may use Council owned computer hardware for Ward and Council work purposes, and personal use as described in this policy.

22.3. Disposal of Computer Hardware

All computer hardware, including laptops and mobile devices must be returned to corporate ICT when staff leave or move to alternative employment within the Council. All redundant and broken computer hardware must be disposed by corporate ICT in accordance with the WEEE regulation. All electronic information stored on the hardware will be wiped clean. No computer hardware will be donated or sold to anyone outside the Council.

23. Information Classification & Usage Policy

This information classification & usage policy applies to all users that have access to any Council information either electronically or in paper format.

23.1. Information Sharing for personal or sensitive information

Information can be shared both internally and externally where appropriate agreements are in place. Information sharing for personal or sensitive information must be approached carefully. It is important that we understand that the recipient has appropriate training / technical controls in other that this information is safely handled outside of our own organisation

A secure data transfer process is described in Appendix 3. A secure e-mail process is described in Appendix 4.

Responsibility lies with the sender to perform an appropriate risk assessment. If you lack the capability to make this assessment you are advised to contact either the ICT Section or DPO for advice.

23.2. Information Access

Staff should not attempt to access either electronic or paper records that may be accessible to them unless specific permission is given.

In line with the council's code of conduct, staff accessing information that may cause a conflict of interest to themselves, such as information about a relative, friend or neighbour who is receiving a council service, have a duty to notify their Line manager immediately and appropriate safeguards are implemented.

23.3. Reporting

The Council will log all usage of information systems and expect any staff member to report any loss or inappropriate use of Council information immediately to their line manager, or if unable to take this course of action, use another appropriate line of reporting, as specified in the Council's Anti-Fraud and Corruption Strategy.

24. Removable media Policy

This Removable Media policy applies to all users.

24.1. Removable Media usage

Removable media is defined as any device that enables a user to copy data and transport it on a device outside the place of work. The use of non-Council approved removable media is prohibited at all times and anyone found copying Council data onto a personal removable media device may be the subject of disciplinary action. Requests for a Council approved encrypted removable media device shall only be done through logging a request with the ICT Service desk.

Any removable media received by the Council must be from a verified source and must be virus checked before transferring the information. The removable media must be either returned to sender, if requested or securely disposed and not used by the recipient for future use.

25. Confidential Waste Policy

This Confidential waste policy applies to all users.

25.1. Think Privacy!

Staff should not attempt to distinguish between confidential and non-confidential documents on a per-document basis. As a rule, **all** day-to-day paperwork, printouts and correspondence shall be disposed of in the confidential waste facilities.

Exceptions are:

- Tissues, hand towels and other soiled items shall be disposed of in other appropriate bins
- Non-confidential bulky items such as catalogues, cardboard packaging, books, newspapers and magazines shall be placed into recycling facilities.

All confidential waste must be put into the confidential waste bins, or the confidential waste sacks provided by the Facilities Management Service for disposing. Confidential waste is still recycled after shredding.

26. Faxing Policy

This Faxing policy applies to all staff that have access to a Council Fax Service/machine.

26.1. Faxing

The use of the corporate faxing service is for performance of official duties only and any personal faxing is prohibited. The Council fax service is provided for the delivery of council services and must not be used for the delivery of any other business or service.

Wherever possible, frequently dialled numbers must be stored in the memory of the fax machine (speed dial) to reduce the chances of dialling an incorrect number. The fax machine must not be left unattended if waiting to re-dial. If it is necessary to send information by fax, the sender must notify the recipient (or duly authorised person) prior to transmission. If sending restricted or protected information to a new recipient or non-speed dial number, a test fax of unclassified data must be sent to the recipient and the recipient asked (using the detail on the test fax) to confirm via telephone that they have received the test fax. Once the live transmission is sent the sender must then contact the recipient to confirm receipt. A standard cover sheet containing a “Confidentiality Clause” must be used. Only the minimum amount of relevant information required by the recipient must be sent. In the event of the intended recipient not being present, received faxes must be handed to the intended recipient (or duly authorised person) immediately, and not left in the print tray.

27. Printing Policy

This Printing policy applies to all users that have access to Council printers.

27.1. Printing

The use of the corporate printing service is for performance of official duties only and any personal printing is prohibited. The Council print service is provided for the delivery of council services and must not be used for the delivery of any other business or service.

All users must ensure that they only print what is necessary and are responsible for all printed material they produce. Printouts must not be left on the back of printers and any unwanted prints must be disposed of in the confidential waste bins/bags provided. If the users are printing to a non-secure release printer, they must collect the printed material as soon as possible and ensure that only relevant printouts are retrieved from the printer trays. When printing information, the user should use a secure print release printer if at all possible and retrieve the printouts as soon as the print has completed.

If the central printer does not, for any reason, print any items of a personal/sensitive information, upon request, but lists it as ‘queued’ on the

machine, users should contact the ICT service desk immediately with the printer reference code, to request them to delete the queued documents before printing is resumed.

28. Mailing Policy

This Mailing policy applies to all users.

28.1. Mailing

When mailing any paper correspondence, either internally or externally, staff must ensure that they insert the correct correspondence in an envelope. Ensure that all the pages of the document to be posted are included, and that no other non-relating documents are included that could have been picked up in error from the printer. Extra care must be taken when posting personal/sensitive information.

Staff must ensure that the correct address is used and should, wherever possible, use Names and Addresses for mailing from corporately managed systems. Only windowed envelopes should be used, unless not practicable to do so, to ensure that the correct address on the correspondence is used as the postal address - this will minimise the risk of correspondence being inserted into an incorrect addressed envelope.

29. Shared Services Policy

The Shared Services policy applies to all contractual third parties and agents of the Council who use Ceredigion County Council IT facilities, or who require access to the Council's Information Systems.

29.1. Shared Services

For all Shared Services, a Third Part Agreement must be signed by all other organisations that form the shared service. This agreement covers connection requirements and procedures relevant to third party suppliers and business support contractors. Any breach of conditions could result in automatic disconnection from the Ceredigion County Council Network until satisfactory conditions can be restored.

Appendix 1 - Dos and Don’ts

Dos

DO ensure that protected and restricted data are only disclosed or seen by those people authorised to do so.

DO ensure that only those people that “need to know” can access protected and restricted data

DO take all reasonable steps to prevent loss, damage, inaccuracy or unauthorised access or disclosure of data.

DO be aware of computer security. Ensure that your PC/Laptop’s Anti-virus software is active at all times and firewalls/security features enabled.

DO leave your computer in a secure state, i.e. at appropriate password screen if leaving the computer and/or office unattended.

DO keep passwords locked in a safe and secure place away from your computer.

DO notify Data Protection Officer of any changes/additional requirements in type of data/uses/disclosures of protected and restricted data.

DO contact Data Protection Officer if asked to disclose protected and restricted data to persons, companies, and organisations other than those you normally deal with or known to you.

DO ensure all software/programs used on computers have been legally obtained and used in a manner not likely to infringe Copyright Acts.

Do inform ICT Service Desk and/or Internal Audit of any suspected or actual security access attempts.

Don`ts

DON`T discuss protected and restricted data in the presence of unauthorised recipients, e.g. other members of staff, cleaners, friends outside work.

DON`T leave protected and restricted data in view of the public or non-authorised users/councillors

DON`T give protected and restricted data to anybody that asks for it, rather, follow the appropriate departmental disclosure procedure. If in doubt, contact your section head/director or the Data Protection Officer.

DON`T throw out computer produced listings. Dispose of all “Confidential Rubbish" in an appropriate bin for proper disposal. If in doubt, treat the material as confidential.

DON`T use the Authority's computers and equipment for you own personal business/gain, or for personal use other than as described in this policy

DON'T copy software for use on other Council computers or for home or for friends.

DON`T use illegally copied software/programs.

DON'T use the Council's internet and telephone service for excessive personal use. Keep the usage to a minimum and only when necessary

DON`T be afraid to ask questions. It`s better than losing data/confidentiality OR EVEN YOUR JOB.

Appendix 2 - Legislation

Regulation of Investigatory Powers Act 2000 -
http://www.legislation.gov.uk/ukpga/2000/23/contents
Copyright, Designs and Patents Act 1988 -
http://www.legislation.gov.uk/ukpga/1988/48/contents
Freedom of Information Act 2000 -
http://www.legislation.gov.uk/ukpga/2000/36/contents
Data Protection Act 2018 -
http://www.legislation.gov.uk/ukpga/1998/29/contents
The Waste Electrical and Electronic Equipment (WEEE) Directive -
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
The Human Rights Act 1998 -
http://www.legislation.gov.uk/ukpga/1998/42/contents
Police and Justice Act 2006 -
http://www.legislation.gov.uk/ukpga/2006/48/contents
The Theft Act 1968 –
http://www.legislation.gov.uk/ukpga/1968/60/contents
The Telecommunications Act 1984
http://www.legislation.gov.uk/ukpga/1984/12/contents
Telecommunications (Fraud) Act 1997 -
http://www.legislation.gov.uk/ukpga/1997/4/contents

Appendix 3 – Secure Document Send Process (Fax/E-Mail/Post)

When sending Personal/Sensitive information the following steps must be followed:

- Double check that the content of the files to be sent is only what's required by the recipient.
- Check that the correct address has been entered (i.e. to ensure that it is sent to the intended recipient).
- Verify that the address / contact information is current. Consult the primary source for this information. Do not use second/third tier sources that may be out of date.
- Check that any personal information referred to in the content matches the address. (To avoid copy/paste errors on letter templates)
- If there's any doubt, you should send unclassified information as a test transmission and request the recipient to confirm receipt before going on to send personal/sensitive information.
- Ensure that you are following a recognised business process prior to sending the file out. If you are unsure, then contact the ICT Service desk or DPO.
- If sending data files ensure that these are encrypted. See Appendix 4 for pre-encrypted (in-transit destinations). If this is not possible then password should be sent via alternative means (e.g. over the phone or text message, with file sent via e-mail). The password should be suitably complex.(14.1 of Information Security Policy)

If the sending of personal/sensitive information is routine in your service area, please seek advice from ICT Section OR DPO. Routine transfers should undergo a proper risk assessment with a view to identifying a stream-lined simple process.

Appendix 4 – Secure Government E-Mail

For the purposes of sending Emails from Ceredigion to other public sector organisations in Wales. Secure sending is available using existing @ceredigion.gov.uk or @ceredigion.llyw.cymru addresses.

You no longer need to access a designated "secure" mail service to send e-mail securely to these organisations. GCSX / GCMail has now been decommissioned.

For organisations not on this list. Please utilise a secure Document Send Process (Appendix 3), use the secure mail facilities provided by that organisation OR Contact ICT/DPO for advice.

Wales National:
NHS Wales: wales.nhs.uk
Welsh Government
Welsh Assembly
WLGA
National Adoption Service (adoptcymru.com)

Police/Fire:
Dyfed Powys Police
Gwent Police
Mid & West Wales Fire Service
North Wales Police
South Wales Fire Service
South Wales Police

Local Government (All 22 Local Authorities):
Blaenau Gwent County Borough Council
Neath Port Talbot County Borough Council
Bridgend County Borough Council
Newport City Council
Caerphilly County Borough Council
Pembrokeshire County Council
Carmarthenshire County Council
Powys County Council
Ceredigion County Council
Rhondda Cynon Taf County Borough Council
City and County of Swansea
Merthyr Tydfil County Borough Council
Torfaen County Borough Council
Cardiff Council
Pembrokeshire
Vale of Glamorgan Council
Conwy County Borough Council
Wrexham County Borough Council
Denbighshire County Council
Shared Resource Service Wales
Flintshire County Council
Gwynedd Council
Isle of Anglesey County Council

National Parks:
Brecon Beacons National Park