ISLE OF ANGLESEY COUNTY COUNCIL

ICT SECURITY POLICY

Revision History			
Version	**Date**	**Author**	**Overview of Changes**
0.1	20/05/2014	Business Continuity & Support Manager	Draft Created
1.0	15/07/2014	Business Continuity & Support Manager	Amended following feedback from the Information Governance Board

ICT Security Policy

1. Introduction

1.1. The Council recognises the risks associated with users accessing and handling information in order to conduct official Council business. Sensitive personal information is used throughout the Council and often shared with trusted partners where appropriate.

1.2. In ensuring that the Council meets its legal requirements under the Data Protection Act 1998, securing Council data, particularly that classified as OFFICIAL-SENSITIVE is of paramount importance.

1.3. Loss, disclosure or corruption of such information could have a significant effect on the efficient operation of the Council. It is therefore essential for the continued operation of the Council that the confidentiality, integrity and availability of all information recording systems are maintained at a level which satisfies legislation and meets the Council's needs.

1.4. This Policy aims to mitigate the following risks ;

- Disclosure of information as a consequence of loss, theft or careless use of ICT equipment and storage media
- Harm or distress to individuals caused by the disclosure of information
- Contamination of Council networks or equipment through the introduction of malicious or unwanted computer programs
- Potential legal action against the Council or individuals as a result of information loss or misuse.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of the above.
- Reputational damage as a result of information loss or misuse.

1.5. Non-compliance with this Policy could have a significant effect on the efficient operation of the Council, result in a breach of the law and result in monetary penalties being levied on the Council – accordingly, non-compliance may be considered a disciplinary offence.

2. Scope

2.1. This Policy applies to all Officers, Elected Members, Committees, Departments, Partners, contractual third parties and agents of the Council who have access to the Authority's information, information systems or ICT equipment.

3. Passwords and Login Accounts

3.1. Users will never share their login details or passwords with any other person.

3.2. It is a requirement that workstation, network and departmental systems enforce a password policy of changing every 30 days and meeting a complexity of;

- At least seven characters in length
- A mix of upper and lower case characters
- A mix of numbers and letters

3.3. Where it is not possible to enforce password complexity within a system, it is the responsibility of the departmental administrator to instruct users that passwords must be manually set to meet these requirements. This requirement applies to all systems, regardless of the fact that the workstation is already protected by a password.

3.4. Upon installation of a new computer, ICT will provide the end user with a temporary password which will immediately need to be changed on first login. In the event that the user is not physically present when the PC is delivered a message will be left asking the user to contact the Helpdesk for a temporary password. Under no circumstances will ICT write down the password, nor will they leave it with the user's colleague.

3.5. With regard to network logins, the Technical Services team will disable accounts which have not been used for a period of 6 weeks.

3.6. To allow for auditing of activities, ICT staff will login with their own login account and not Administrator or root accounts.

3.7. To prevent unauthorised persons from gaining access to workstations, the ICT Service will setup a BIOS Power On password when each workstation is built.

3.8. Where shared access is required to the same PC, access will always be made via individual user's own network logins and not via the unauthorised sharing of passwords.

4. Leavers

4.1. Upon termination of employment, it is the responsibility of a user's line manager to notify ICT of the "leaver" so that any login access can be removed. This will help prevent unauthorised access to sensitive data.

4.2. It is acknowledged that ICT are not always reliably informed of leavers and accordingly, a recurring monthly task has been scheduled in the Helpdesk system for staff in the Technical Services team to suspend the accounts of any staff listed on the Starters/Leavers page on MonITor.

5. Third Party Remote Access

5.1. It is common practice for third parties such as suppliers to be provided with remote access to an organisation's ICT Systems in order to provided technical support. In order to protect the security of data and ensure that suppliers meet the security standards required by the Council, the following controls will apply;

5.2. Third parties will only be provided with remote VPN login upon completion of a Remote Access Agreement form (Appendix X) which records their agreement to abide by Council ICT policies as well as their commitment to a Data Processing Agreement (Appendix X).

5.3. Access will only be provided via the Council's secure web portal which offers an encrypted tunnel for communication.

5.4. VPN access will only be granted upon request to the Helpdesk and will be revoked at the end of the working day.

5.5. No external third party (external contractors, partners, agents, the public or non-employee parties) may extract information from the Council's ICT equipment without explicit agreement from the HoS (ICT) or his delegated officers.

6. Email Security

6.1. All email received by the Council will be passed through a filter before reaching user's mailboxes; if the email is identified as Spam (unwanted or harmful email) it will be quarantined by the system.

6.2. It is possible that business related emails may on occasion be mistakenly quarantined if they contain word patterns or phrases which are similar to known Spam. The spam filtering system will alert users to any emails which have been quarantined on a daily basis and provide them with the option to release business emails which have been mistakenly identified as Spam, however a great degree of care should be taken in doing this.

6.3. Should users receive emails which appear suspicious (for example, emails with suspect subject lines) they are advised not to open the email or any included attachments. Instead the email should be deleted and the trash emptied. The ICT Helpdesk should also be notified so that any pattern or a wider problem or attack can be identified at the earliest opportunity and preventative action taken.

6.4. Aside from the filter described in 6.1, the ICT Service will only access a user's emails in resolving a reported technical issue or if directed by the Chief Executive, for example in order to investigate misconduct.

6.5. Requests to access another user's mailbox must be authorised by the requestor's line manager. For example, if a Principal Officer is making the request this must be authorised by the Head of Service. If the request is being made by a Head of Service it must be authorised by a Corporate Director.

6.6. Users should be aware that when sending email across the Internet your message is sent as clear text and may be read by persons other than the intended recipient as it is in transit.

6.7. It is for this reason that when sending data externally which is classified as OFFICIAL-SENSITIVE, it should always be carried out Government Secure Email by default. Messages sent by this system are not sent across the internet but across a secure Government network known as the PSN, or "Government Connect".

6.8. Users requiring access to Government Secure Email can find details of the procedure in the ICT Frequently Asked Questions (FAQ) section on MonITor.

6.9. In some circumstance, Government Secure Email may not be an option – for example where the recipient does not have a Government Secure Email account because they are not a public body. In this case, the following procedure should be followed;

- Sensitive information should be stored in a Word document rather than in the body of the email.
- The Word file (and any other attachments) should be compressed and encrypted to AES 256 Bit standard using 7Zip. Guidance can be found on the ICT pages of MonITor.
- The password used should be at least 7 characters and include a mix of upper and lower case alphanumeric characters.
- Double check that the email address you are using is correct – do not use "autocomplete" for this.
- Ensure that the filename of the file and the subject of the email include the classification of the data, i.e. OFFICIAL-SENSITIVE.
- The file(s) should be emailed to the recipient with a note to contact the sender by telephone for the password.

6.10. If you require assistance with the above or require access to 7Zip please contact the Helpdesk.

7. Removable Media

7.1. Removable media includes, but is not restricted to the following ;

- CDs/DVDs
- External Hard Drives
- USB Memory Sticks (also known as pen drives or flash drives)
- Memory Cards
- MP3 Players
- Digital Cameras
- Backup Cassettes

7.2. For the purpose of this policy, the terms Media and Removable Media will be used interchangeably.

7.3. Except as provided for below, it is the Authority's policy to prohibit the use of all removable media devices.

7.4. The use of removable media will only be approved if a valid business case for its use is made. There are substantial risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated and documented before approval is given.

7.5. Requests for access to, and use of, removable media devices in the first instance must be made to the line manager. The line manager will then make that business case to the Helpdesk via email on behalf of the requestor.

7.6. Should the business case for access to, and use of, removable media devices be approved, the following sections apply and must be adhered to at all times;

7.7. All removable media devices and any associated equipment and software must only be purchased by ICT Services and installed by ICT service.

7.8. Non-council owned removable media devices must not be used to store any information used to conduct Council business, and must not be used with any Council owned ICT equipment. These devices will be blocked on Council PC's and Laptops.

7.9. The only equipment and media that should be used to connect to Council equipment or the Council network is equipment and media that has been purchased by ICT services.

7.10. Where removable media is received from outside the Council it should be taken to ICT to be virus checked, the ICT service will then copy the data to a location on the network where end users can access it.

7.11. In the case of job interviewees who are asked to make PowerPoint presentations it should be requested that they email the file beforehand to the interview panel.

7.12. Users should never save data they consider to be of critical importance onto Removable Media unless another copy is held on the network file server.

Should the Removable Media be lost, stolen or become corrupt it would not be possible retrieve the information.

7.13. Removable media devices must not to be used for archiving or storing records as an alternative to other storage equipment.

7.14. Each user is responsible for the safety of the Removable Media they are issued and as such, users must sign their acceptance of this policy upon collection.

7.15. All data stored on removable media devices must be encrypted. Removable media purchased by the ICT Service will enforce encryption to the AES 256bit standard as a minimum. This will be carried out in a user friendly manner that will simply prompt for the entry of a password before the device can be accessed.

7.16. Upon delivery of the removable media ICT staff will provide users with a password and demonstrate its correct use. This must be kept a secret and not written down.

7.17. It is the responsibility of end users to remember the password for their Council issued Removable Memory device – should this be forgotten the ICT Service will be unable to assist with recovering the data held.

7.18. Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the ICT Helpdesk should removable media sustain damage.

7.19. Removable media which is no longer required, or has become damaged, must be disposed of securely to avoid data leakage. Removable media should not be simply discarded in general office waste bins - users with removable media which is no longer required should contact the ICT Service and make an appointment to hand them over. The ICT Service will then ensure their secure disposal.

7.20. Any previous contents of any reusable media that are to be reused, either within the Council or for personal use, must be erased by ICT. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools and as such, all removable media devices that are no longer required, or have become damaged, must be returned to ICT services for secure disposal.

7.21. Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

7.22. In the event that Removable media is lost or stolen the Data Loss procedure outlined in this Policy must be adhered to.

8. Malware and Unwanted Programs

8.1. Malware is a broad term used to describe computer viruses, spyware, trojan horses and other malicious computer programs.

8.2. The possibility of malware infection is a real and serious threat to the security of the Council's data and systems - unless adequate precautions are taken to prevent malware, the effects of infection can be catastrophic, leading in the worst cases to the theft or loss of data. This may render the data held irrecoverable, and is potentially disastrous to the business of the department, and organisation.

8.3. If infected machine(s) are connected to the network then the effects may not be limited to a single machine; the malware is likely to be transmitted to others on connected networks, potentially including other authorities.

8.4. To mitigate against the risk of malware, the ICT Service will install antivirus software on all new PC's, prior to installation in the user department. Deliberate removal of the antivirus software or any other deliberate actions which might prevent the software from functioning correctly will result in disciplinary action.

8.5. New malware is being developed constantly and although the Council does have protective measures in place, it is not always possible to detect newly developed threats. It is for this reason that it is important for users to exercise caution, particularly when receiving email attachments or visiting unfamiliar websites.

8.6. Software audits will be carried out on an ad-hoc basis, either by the ICT Service, Internal Audit, or external agencies. Any software which cannot be accounted for will be removed. Access to the corporate network will be denied until the machine is proven to be free of such software. As well as being good antivirus practice, this ensures that the law is adhered to in terms of software licensing, and protects the Council from the risk of litigation.

8.7. The installation of illegal copies of software on any PC is forbidden. Likewise, the installation of legal copies of Council purchased software on staff members' own equipment at home is not permitted due to the implications of managing these licenses and ensuring compliance.

8.8. In order to remove the risks posed by files downloaded from the Internet and to ensure all software held is correctly licensed, the necessary privileges to install software or to make changes to the configuration of PC's will not be granted to end users.

8.9. Any removable media received into a department must be submitted to the ICT Service, who will check it for the presence of malware.

8.10. Should malware be found on removable media from an external source, the source of the media will be notified of the presence of the malware, to enable them to identify its source and take appropriate action.

8.11. Installation media for software purchased by and installed within the Authority is to be securely contained within the ICT Service.

8.12. In the event of a malware infection being detected or suspected, the following procedure must be followed:

8.12.1. Notify the ICT Help Desk immediately and they will attempt to establish the source of the virus.

8.12.2. The affected machine(s) will be physically disconnected from any network to which it is connected by disconnecting the network cables from the ports. This will prevent the malware from spreading to other machines, if it has not already done so.

8.12.3. All removable media held by the end user concerned, for example USB Memory Sticks, will be brought to ICT's attention so that they can be suitably checked for the presence of infection.

8.12.4. Any removable media found to contain malware which cannot be removed will be destroyed. In this event, the data on such media cannot be considered safe for transferring to other media and will be lost.

9. Incident Reporting

9.1. For the purpose of this Policy, an incident is defined as a potential, or actual security breach or loss of information.

9.2. If an individual becomes aware of, or suspects an incident it will be reported immediately to the service manager of the relevant service area. Any such incident should be regarded as a serious matter and has the potential to;

- breach statutory restrictions on the disclosure of information
- adversely affect relations with other agencies
- cause substantial distress to individuals
- cause financial loss or loss of earnings potential to, or facilitate improper gain or advantage for, individuals or companies
- prejudice the investigation or facilitate the commissioning of a crime
- breach proper undertakings to maintain the confidentiality of information provided by third parties
- impede the effective development or operation of Council policies
- disadvantage the Council in commercial or policy negotiations with others
- undermine the proper management of the Council and its operations

9.3. Upon becoming aware of an incident, the service manager will report it to the Helpdesk who will log the incident within the Helpdesk tracking system.

9.4. The system will generate an email and an electronic “job ticket”

9.5. Either the Business Continuity & Support Manager or Technical Services Manager will act as Incident Response Lead (IRL) and will investigate the incident, recording the stages of response within the system including ;

- Date and time of reporting the incident
- Who or what reported the incident (e.g. system alerts, end user report)
- Description of the circumstances surrounding the incident
- Details of any information of records affected
- Any other relevant information

9.6. Any host relating to the incident that is either believed to be unauthorised or compromised by malicious software or a hacking attack and remove the host form the network, noting the host identity (IP, name, serial number)

9.7. Best practice should be followed in investigation of incidents by use of;

- Logging by firewalls, operating systems and applications
- Security alerts configured within logs
- File integrity checking
- Anti-virus measures
- Anti-spam measures
- Email and web content checking
- Retention of logs and backup tapes for a minimum of 6 months

9.8. The incident handler will determine the extent of the incident and the source of the incident;

- Is a single host affected?
- Is a network segment affected?
- Is the LAN affected?
- Is the WAN affected?
- Impact of the incident?

9.9. The IRL will determine if the loss or suspected loss is to be handled by ICT or passed to the Corporate Information Officer who in turn will then decide whether the Information Commissioner should be notified.

9.10. If required or necessary, the IRL should write a report on the incident for internal distribution to enable management to consider any recommendations and any wider business implications. The report should include;

- Log entries
- Extent of the incident
- Measures taken to eradicate the incident
- Future preventative measures
- Impact of the incident

- Recommendations to prevent future re-occurrence

10. Personnel Assurance

10.1. The purpose of staff screening is to provide a level of assurance as to the trustworthiness, integrity and reliability of all council employees, contractors and temporary staff who access the Council's networks and those of government agencies.

10.2. The Cabinet Office mandate that the Council meets several requirements with regard to ICT and Information Security, one of which states the Council ensures "that any user, supplier or 3rd party involved in the consumption or provision of PSN Services receives appropriate security vetting. The vetting standards shall be based on the Baseline Personnel Security Standard (BPSS) or comparable".

10.3. To meet this requirement the HR Unit carry out identification and reference checks on potential recruits. In addition, the ICT Service requires proof that BPSS has taken place before access is provided to Government Connect systems. In the event that proof cannot be produced that BPSS has already taken place the ICT Service will carry out an additional BPSS.

10.4. Although BPSS can provide assurance as to a person's identity, it is not a substitute for effective line management, nor should it be considered an alternative to the correct application of the 'need to know' principle or to access and information security controls.

10.5. Personnel security is an important element of an effective protective security regime as well as good overall management practice. The security clearance process only provides a snapshot of an individual at a particular time. This standard is the beginning of an ongoing and actively managed personnel security regime, which requires senior and line management support, awareness and education, and formal periodic reviews of security clearance.

11. Home Working

11.1. As the ICT Service does not have sight of personal ICT equipment staff may own at home it has to be assumed that they may contain security vulnerabilities which pose a threat to the security of the Council's data.

11.2. Typically, home users operate as the system administrator for everyday use such as web browsing and reading email, rather than as a user with minimised privileges.

11.3. Home users may download and install un-trusted content from the Internet. This could include applications as well as content such as on-line games which run within the user's web browser. In any case, home users are highly unlikely to conduct a risk assessment before using the application or content;

11.4. It is for the reasons outlined above that personally owned equipment cannot be used for Council business. Should there be a documented business case for individuals to work from home, it is the responsibility of departments to provide those individuals with Council owned equipment which will be built by the ICT Service to the necessary security standards.

11.5. Council data should never be copied to a personally owned computer; neither should Council owned USB Drives be connected to a personal computer.

12. Workspace Security

12.1. For the purpose of this policy, workspace refers to the area in which you are using ICT faciliites to carry out your work, this includes, but is not limited to working at your desk in the office, working on-site or working at home. This section details specific workspace related measures which should be carried out to protect the security of your ICT equipment and information assets.

12.2. When away from your workspace from a substantial period of time, clear away any papers and removable media, locking them away in desk drawers or cabinets avaible.

12.3. Do not store papers, removable media or ICT equipment near ground floor windows. Where this is unavoidable, ensure that the windows are locked when the workspace is unoccupied and that blinds are closed.

12.4. Where your workspace has a lockable door, ensure that this is locked when the workspace is left unattended.

12.5. When laying out your workspace, always consider whether information you are viewing or creating could be observed by unauthorised persons – for example, through a window.

12.6. Information relating to usernames and passwords should never written down and should not be visible in your workspace.

13. Portable Computing Devices

13.1. For the purpose of this Policy, “Portable Computing Devices” includes, but is not restricted to; Laptops, Tablets, PDA’s and Smart Phones.

13.2. This document highlights the security risks arising from the use of portable computer equipment outside of the Authority’s premises and to provide guidelines to minimise them.

13.3. The need to use portable computing facilities outside of the Authority’s premises has become commonplace, and a significant number of Officers now have access to such equipment.

13.4. When off the Authority’s premises, Portable Computing equipment is at risk of:

- Theft
- Accidental loss
- Unauthorised access
- Damage

13.5. The equipment must be immediately and visibly identifiable as the property of The Isle of Anglesey County Council. This is achieved by affixing the tamper proof property asset sticker to the portable equipment.

13.6. The equipment should be accompanied by a card containing the Name, Department, office address and telephone number of the Officer who is principally responsible for the equipment. (Most portable computer equipment is kept in a carry-case. This card should be kept in the carry-case.)

13.7. Passwords can be applied at different levels, and for different purposes. Used in combination, access to both locally held information and unauthorised access to central information systems can be made extremely difficult.

13.8. The BIOS password for portable devices will be invoked where possible. This will make it very difficult, but not impossible, for anyone stealing the equipment to either use it, or clear the hard disc and reconfigure it.

13.9. All laptops will have their hard disk drives encrypted to the AES 256 bit military standard – this is controlled by a login password with no special training required by the user. Providing the laptop's encryption passwords have not been written down or shared this will render the data held totally unreadable to unauthorised persons.

13.10. To reduce the risk of unauthorised use or theft, equipment should not be left unattended if at all possible. If it is absolutely necessary to leave equipment unattended it should be powered down to prevent access.

13.11. To protect the integrity of a device's security credentials, appropriate care must be taken to ensure that the entry of usernames and passwords cannot be overlooked by persons nearby.

13.12. To prevent the equipment being used to access the Authority's central information systems, any software used to access those systems must not be pre-configured to automatically enter the user's login name and password.

13.13. Any documents that are held on the computer's local hard disc that contain sensitive information should be protected by passwords, where the originating software permits.

13.14. No user login names or passwords that are associated with the equipment must be written on any paper or card accompanying the equipment.

13.15. In the event of the equipment's theft or loss, the Officer responsible for the equipment at the time of the loss will immediately notify their line manager in

accordance with the Incident Reporting procedure of this Policy. The police and the Authority Insurance Officer should also be informed.

13.16. The ICT Service, on receipt of the necessary information, will delete the user's existing passwords. The user will then change the passwords for continued usage on other Council-owned ICT equipment.

13.17. Used in combination, the above facilities should protect the County Council from loss of data and breaches of security arising from the loss of portable computer equipment.

13.18. Portable Computing Devices should not be used over public, free wireless access such as those provided in fast food restaurants - since the Council has no assurance as to the security of the wireless network there is potential for your passwords and data to be viewed by unauthorised persons.

14. Policy Compliance

14.1. If any user is found to have breached this Policy, they may be subject disciplinary action. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

14.2. If you do not understand the implications of this Policy or how it may apply to you, seek advice from ICT services on ext. 2666 or helpdesk@anglesey.gov.uk

15. Review and Revision

15.1. This Policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

15.2. Policy review will be undertaken by ICT Services and authorised by the ICT Steering Group.