Cyngor
sir ddinbych
denbighshire
County Council

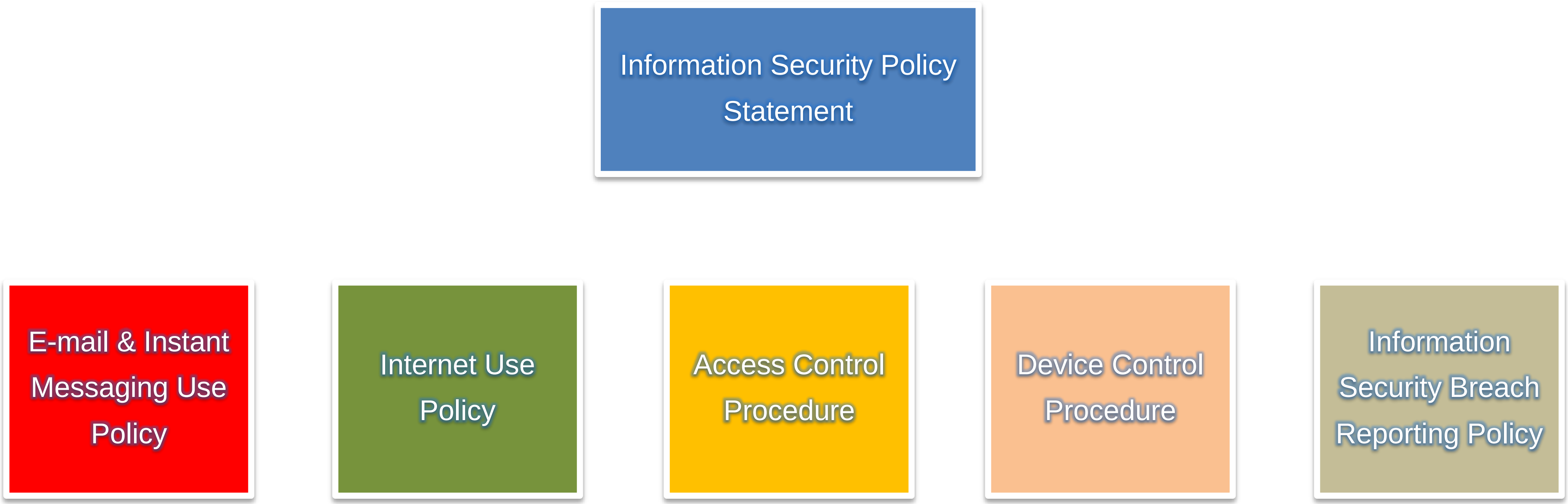
INFORMATION SECURITY POLICY & PROCEDURES

Date agreed and implemented	
Agreed by	
Review date	
Frequency	
Author	

•

Version	Status	Reason for change	Authorised

Information Security Policy Framework



Information Security Policy Statement

E-mail & Instant Messaging Use Policy

Internet Use Policy

Access Control Procedure

Device Control Procedure

Information Security Breach Reporting Policy

Select control and click on the relevant box above to take you to the corresponding section of this document

INFORMATION SECURITY POLICY STATEMENT

1 Introduction and aim

1.1 The information that the Council uses to conduct its day to day business is vital to its core operations. In some instances this information may be classed as commercially sensitive, official information[1] or may be personal data[2]. People and organisations that the Council works with or on behalf of have the right to expect that the Council will manage that information appropriately and keep it secure at all times. The Council has identified Information Security as a key priority in its Information Management Strategy.

1.2 Information Security is defined in the ISO27001 International Standard for Information Security Management Systems as controls which ensure the Confidentiality, Integrity and Availability of an organisation's Information Assets.

1.3 The Corporate Executive Team is fully committed to ensuring that the Council has in place a system of effective controls and processes to ensure the Security of all Information Assets and will ensure compliance with the above standard. Furthermore, the inappropriate use, loss or disclosure of Council owned information is a risk and is subject to legislative controls if this relates to personal data.

1.4 The requirement for sound information security practices needs to be carefully balanced against the need to make information available to internal users, external customers and partner agencies. This policy applies to all Employees, Members and Contractors of Denbighshire County Council. Where reference is made to employees within this policy from this point forward, this also includes Members and Contractors.

1.5 This policy applies to all information assets, which are held by or on behalf of Denbighshire County Council whether held in paper or electronic format. This also includes information which might be held by third parties or commercial organisations for or on behalf of the Council. Non-compliance with this policy and associated policies and procedures may lead to disciplinary and/or legal action being taken against an individual or organisation that is found to be liable.

[1] https://www.gov.uk/government/groups/public-services-network

[2] Data Protection Act 1998 definition of personal data.

2 Key Principles

2.1 The Council has adopted the following principles, which underpin these policies and procedures:-

- Information will be protected at all times in accordance with relevant laws and standards;
- Information should be available at all times to those with a lawful, legitimate need;
- The Integrity of information must be maintained at all times; information must be accurate, complete, timely and up to date;
- All members of staff, members, volunteers and contractors who have access to information have a responsibility to handle it appropriately; and
- Information will be protected at all times against unauthorised access, loss or disclosure with appropriate controls commensurate to the level of risk involved.

3 Roles and Responsibilities

3.1 Corporate Executive Team (CET)

3.1.1 The Council's Chief Executive is ultimately responsible for all the information assets which are owned by the Council.

3.2 Senior Leadership Team (SLT)

3.2.1 Members of the Senior Leadership Team and Heads of Service are responsible for all Information that is held within their service and are the Information Asset Owners for that information. Heads of Service are also responsible for ensuring that their staff are made aware of and fully comply with the Information Security Policy and its associated policies and procedures.

3.3 Senior Information Risk Owner (SIRO)

3.3.1 The Senior Information Risk Owner is responsible for ensuring that effective controls and processes are in place to minimise Information risk for the Council. The SIRO is also responsible for reporting to the Council's Corporate Governance Committee, CET and SLT on all relevant issues, which might affect the security of the Council's information.

3.4 Business Improvement and Modernisation Service

3.4.1 Corporate Information Team

The Corporate Information Team establishes the information security policy framework and monitors compliance.

3.4.2 Business Transformation and ICT Department

The Business Transformation and ICT Department have the day-to-day responsibility for implementing and supporting the technical solutions in place that support the Information Security activities. They are also responsible for ensuring that the Corporate Information Team are made aware of any issues which might affect the Security of Council information and for ensuring that the Council complies at all times with the Public Services Network Code of Connection[3] and relevant laws and policies by implementing appropriate technical controls as advised.

3.5 Data Protection Officer

3.5.1 The Data Protection Officer acts on behalf of the Data Controller to ensure that Denbighshire County Council complies with the Data Protection Act 1998.

3.6 Members

3.6.1 Members are responsible for ensuring that they comply with the Information Security Policy and its associated policies and procedures.

[3] https://www.gov.uk/public-services-network

3.7 Employees

3.7.1 Denbighshire County Council employees, secondees, agency staff and temporary employees are responsible for ensuring that they read and comply with the Information Security Policy and associated policies and procedures.

3.8 Managers and system Administrators

3.8.1 Managers and system administrators are responsible for ensuring that any IT systems within their control are managed and maintained in accordance with Council policies and procedures.

4 Legal Implications/Associated Policies and Procedures

4.1 There are a number of laws and regulations covering Information Management and the security thereof. These include:-

- Data Protection Act 1998
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Copyrights, designs and patents act 1988
- Human Rights Act 1998
- Malicious Communications Act 1988
- Regulation of Investigatory Powers Act 2000
- Pubic Services Network Code of Connection[4]
- Denbighshire County Council Information Risk Policy

[4] https://www.gov.uk/public-services-network

- Denbighshire County Council Disciplinary procedures
- Denbighshire County Council Internet , E-mail and Telephone Use and Monitoring Policy
- Denbighshire County Council Remote Access Policy
- Denbighshire County Council Wireless Access Policy
- Denbighshire County Council Bullying and Harassment Policy
- Denbighshire County Council Data Protection Policy
- Denbighshire County Council Freedom of Information Policy
- Denbighshire County Council Grievance Policy
- Denbighshire County Council RIPA policy
- Denbighshire County Council ICT Procurement Policy
- Denbighshire County Council Social Media Policy
- General Data Protection Regulation / Protection of Freedoms Act 2012

DEVICE CONTROL PROCEDURE

1 Introduction and Aim

1.1 The purpose of this procedure is to provide employees, members and contractors with a set of core principles under which electronic devices issued and managed by Denbighshire County Council are to be used.

1.2 The aim of this procedure is to ensure that all users are aware of their obligations with regards to the use and control of electronic devices issued by Denbighshire County Council.

1.3 This procedure applies to all electronic devices including PC's, laptops, I Pad's and other tablet devices, all types of external hard drives or removable media devices, telephones and mobile devices.

2 Procedures

2.1 Acceptable Use

- Council supplied devices are to be used for work related purposes only. As such, they should not be used to download or store non-work related material. Any material held for personal rather than work related purposes is not permitted in accordance with this procedure.
- Council supplied devices must not be used to conduct any illegal activity including downloading or sharing unlicensed software and/or copyright protected material.
- Council supplied devices should not be used to conduct a business or used for the direct commercial gain of or by its employees.
- Images, cartoons or files containing nudity, sexually explicit, or other content of an illegal, racist or defamatory nature should not be stored on or sent using Council supplied devices.

- All laptops, tablets and removable media devices MUST have mobile device management in place and be encrypted when used to store or transmit Council related information. Any exemptions to this rule must be requested.
- Misplacement, loss or theft of any device MUST be reported to the ICT Service Desk immediately.
- DO NOT write down any password or PIN numbers.
- DO NOT allow any other person to use the device unless specifically authorised to do so.
- Jail broken devices are strictly not permitted. This means that no device which has had its operating system security features disabled is to be used. You must not attempt to disable any of the device security features or install applications that are not for work related purposes.
- Do not store information or files on the c:/ drive or ‘my documents’ area of your computer or laptop. These files are not backed up and are at risk of permanent loss if the device is lost or becomes unusable through breakdown. Files should be stored on a network drive i.e. your personal drive or a team drive.

2.2 Use of CD, DVD and USB Memory Storage Devices

- Any information stored on removable media i.e. CD/DVD’s, external hard drives and USB memory sticks MUST be encrypted. The council uses software to encrypt files and information on these types of media. When a removable device is inserted into a Council owned laptop or PC you will be prompted to encrypt that device before it can be used.
- Be wary when opening documents or files from removable media as they may contain viruses. Ensure that only content from a known source is opened or access. In case of any queries, contact the ICT Service Desk in the first instance.
- You must ensure that removable media devices are only used for temporary storage and that any material is saved to a network drive as soon as practicable to ensure business continuity. Material should be deleted or removed from the removable media when no longer required.
- Removable devices should not be used for back-up purposes. The Council operates its own back up methods which should be used in all instances.

2.3 Mobile Phones issue and use

- Please refer to the Council’s Mobile Device guidance which is available on the intranet.

INTERNET USE POLICY

1 Introduction and Aim

1.1 The aim of this policy is to provide guidance to employees and members of the Council regarding the acceptable use and monitoring of the internet.

1.2 The Internet is a valuable information resource which is provided by the Council to assist employees and members to conduct the day to day business of the Council.

1.3 Many council services are increasingly becoming accessible to the public via the Internet and this is actively encouraged to ensure that Council Services are delivered efficiently and effectively. However, this does provide a high level or risk as recent high profile breaches have demonstrated (Sony and Talk Talk). The use of Cloud and Hosted Services is also included within this policy.

2 Core Principles

2.1 The following are a summary of the main requirements of this policy:-

- The internet is provided for work related purposes only.
- Personal use of the internet is allowed outside normal working hours.
- Do not access restricted or illegal websites.
- Do not download software from the internet without the explicit consent of the Business Transformation and ICT Department.

2.2 Managers are responsible for ensuring that their employees are made aware of this policy and comply with it.

2.3 This policy should be read in conjunction with the Council’s Information Security Policy and any associated procedures.

2.4 There are separate policies relating to internet use in educational establishments and public access in libraries and other Council buildings.

2.5 Employees and members of Denbighshire County Council are responsible for ensuring that they comply with this policy at all times.

2.6 Suspected non-compliance with this policy should be reported to the person’s line manager and all reports will be investigated. Any person found to be in breach of this policy as a result will be subject to disciplinary action and potentially criminal action which may result in dismissal.

3 Policy

3.1 The Internet is provided by Denbighshire County Council in order to allow staff to conduct the day-to-day business of the Council.

3.2 Personal use of the Internet is a privilege and should only be carried out outside of normal working hours for example, at lunch time or before and after work. As many staff are on Flexitime, there are no core working hours so employees must ensure that they are clocked out when accessing the internet for personal use. Line Managers are responsible for ensuring their staff understand and comply with this requirement. Staff on fixed hours must refer to their fixed hours agreed with their Line Manager. Personal use of the internet should be kept to a minimum and not interfere with work commitments.

3.3 Staff engaged in the following activities on the Internet will face disciplinary and/or legal action:-

- Knowingly participating in illegal pursuits;
- On-line gambling;
- Knowingly accessing, displaying or disseminating pornography;

- Posting information that may disparage, harass or discriminate against others on the basis of gender, race, age, disability, religion, sexual orientation or national origin;
- Knowingly downloading, using, or distributing copyrighted materials from the Internet without proper authorisation.
- Knowingly downloading, using, or distributing software or executable programs.

3.4 These types of sites are normally restricted however, the filters are never 100% guaranteed and if users inadvertently access a site which you consider may be inappropriate and should be blocked, please contact the ICT Service Desk.

3.5 Denbighshire County Council accepts no liability for any loss suffered as a result of personal usage of the internet. All users are reminded that if entering their credit card or banking details to purchase goods or services, they do so entirely at their own risk.

3.6 Please consider the following:-

- The use of the internet carries many risks. Criminals actively target users of the internet to conduct illegal activities and online fraud is rife in the UK and worldwide.
- The Council does not guarantee the accuracy or content of any external website and users should verify content independently before taking any action.
- Do not respond to requests for your password or personal credentials via e-mail. If in doubt verify the validity of such requests with the organisation concerned but DO NOT reply to the e-mail or follow any links provided.
- Software and programs, even free ones, must not be downloaded without explicit consent of the Business Transformation and ICT Department, as doing so could lead to the introduction of malware, viruses and unlicensed software which could affect the correct operation of other Council IT systems.
- Downloading content, music, and videos for personal use is not permitted.

3.7 Internet Filtering

3.7.1 In order to prevent accidental or deliberate access to filtered sites, e.g. those containing material of a pornographic or illegal nature, the Council has installed sophisticated content filtering software. Websites are restricted in relation to the website category which is determined by a number of factors. Access to restricted sites may be permitted but must be requested via the ICT Service Desk.

3.7.2 The categories of restricted sites may change from time to time, without prior notification however, whilst every attempt is made to verify the effectiveness of the filtering software, Denbighshire County Council does not completely guarantee it effectiveness.

3.7.3 When a user has attempted to access a blocked site, a warning message will be displayed. If you think this is incorrect please contact the ICT Service Desk and forward them a copy of the message along with the full URL.

3.7.4 Monitoring the use of the internet and other communication facilities is governed in the UK by legislation.

3.7.5 The use of the Internet and e-mail will be monitored only for the purposes of ensuring the detection of excessive personal use of the internet during normal working hours, enforcement of this policy, or to detect attempted unauthorised access to Council IT systems and the prevention, detection and investigation of crime.

3.8 Cloud Hosting

3.8.1 The terms “cloud computing” or “the cloud” are relatively recent introductions to the workplace, but represent an important and ever-growing industry. Cloud computing is internet-based computing, where resources are hosted externally to the Council and accessible via the internet. This gives the user the ability to access services from any location, at any time and from a range of different devices including laptops, tablets or mobile phones.

3.8.2 Cloud services can generally be classified into three models:

- **Software as a service (SaaS):** this encompasses “off-the-shelf” applications such as Verto, cloud storage facilities such as Dropbox or e-mail services such as Egress secure e-mail for sharing sensitive information.

- **Platform as a service (PaaS):** a development platform provided by a third party where the Council can develop and run our own applications.
- **Infrastructure as a service (IaaS):** where the third party provider hosts hardware, software, servers, storage and other infrastructure components on our behalf.

3.8.3 The big difference between cloud and traditional computing is that the Council does not directly host these resources, instead entering into contracts with third parties to provide the appropriate level of service we require.

3.8.4 Increasingly, Local Government software suppliers are moving their applications onto a cloud model, which brings with it advantages to the Council (for example, no need to provide and maintain our own servers to host applications) but also introduces significant risks.

3.8.5 The biggest risks with cloud lie primarily with the processing and storage of data and we must consider this when engaging with a third party to handle sensitive information. The Data Protection Act (1998) applies to data stored or processed in the cloud – as it does to data which is stored or processed locally. This means that the Council's legal obligation to maintain the security of personal data under the DPA still applies.

3.8.6 To mitigate the risks of loss or unauthorised access to personal data, the Council requires potential cloud suppliers to complete a mandatory ICT Security Specification questionnaire in respect of externally-hosted solutions. This form is available upon request to your ICT Business Partner and must be completed prior to the purchase of any new system or solution.

3.8.7 Some of the aspects addressed in the questionnaire are:

- The physical location of any data centres and their security arrangements e.g. fire detection capabilities
- Details on vulnerability assessments carried out on the supplier's website e.g. to reduce threats from hacking
- Application specific details, such as whether there is a full audit trail to monitor changes and controls in place to manage user passwords

3.8.8 Successful completion of this questionnaire demonstrates to the Council that the third party can be trusted to store the Council's data securely and responsibly and in line with the Data Protection Act.

E-MAIL & INSTANT MESSAGING USE POLICY

1 Introduction and Aim

1.1 The aim of this policy is to provide guidance to employees and members of the Council regarding the acceptable use and monitoring of the Council's e-mail and instant messaging system.

1.2 Both systems are provided by the Council to assist employees and members to conduct the day-to-day business of the Council.

1.3 E-mail is considered the primary communication tool used by the council and many organisations and individuals and as such must be used appropriately. Instant messaging provides a more informal and faster means of communicating internally.

2 Core Principles

2.1 The following are a summary of the main requirements of this policy:-

2.1.1 Reasonable personal use of e-mail is permitted, provided this is legal, not excessive, and does not interfere with work related performance.

2.1.2 Do not use the e-mail system as a storage repository. The E-mail system is a communication tool and not a filing system. Save any important attachments or files to either your network drives or EDRMS for future reference.

2.1.3 Managers are responsible for ensuring that their employees are made aware of this policy and comply with it.

2.1.4 Suspected non-compliance with this policy should be reported to the person's line manager and all reports will be investigated. Any person found to be in breach of this policy as a result will be subject to disciplinary action which may result in dismissal.

3 Policy

3.1 Like the internet, the e-mail system is provided by Denbighshire County Council to enable users to conduct the day-to-day official business of the Council.

3.2 The following instances of misuse of the e-mail facility could result in disciplinary action being taken against those responsible, including suspension of e-mail facilities:

- Knowingly entering into a legally binding contract by e-mail without having the authorisation to do so;
- Knowingly sending or forwarding e-mails containing defamatory statements or information about individuals;
- Knowingly sending or forwarding unwanted e-mails to individuals;
- Sending aggressive, abusive, or deliberately antisocial e-mail;
- Knowingly sending of forwarding e-mails containing pornographic content including attachments;
- Knowingly sending or forwarding e-mails containing information that may disparage, harass, or discriminate against others on the basis of gender, race, age, disability, religion, sexual orientation, or national origin;
- Sending e-mails in another person’s name without their authorisation;
- Opening another person’s e-mail without their authorisation unless done so for investigative purposes;
- Sending sensitive information via a non-secure e-mail route; and
- Excessive use of e-mail for personal use.

3.3 Similar to letters, memos and other forms of communication, e-mails are a record of council business and should be treated appropriately. For advice on the storage and retention of e-mails, please refer to the Council’s Records Retention Schedule, which is available on the Intranet. If further advice is required please contact the Corporate Information Manager.

3.4 Users are reminded that e-mails, like other types of communication may be disclosed in legal proceedings or in response to a request for information, for example in response to a Freedom of Information request. Similarly, care should be taken in respect of how information is recorded as it could be subject to release to any other person in response to a request for information.

3.5 Members of Denbighshire County Council are obliged to comply with this policy and are permitted to use the Council's e-mail system for communicating with members of the public in their official council duties but are not permitted to use the Council's e-mail system for canvassing or political petitioning purposes.

3.6 To help you avoid unsolicited e-mails and to protect the security of Denbighshire IT systems, do not post your official DCC e-mail address onto public mailing lists or internet forums including the Denbighshire County Council website or any other website. Where contact details are required, a departmental e-mail address should be used. This will help us to protect your personal internet safety and prevent you from receiving unsolicited e-mails and to assist in the reduction of attempted ID fraud.

3.7 The content of official e-mails should be factually accurate and not contain any personal opinion or bias.

3.8 Secure, encrypted e-mail such as egress or GCSx mailbox should be used to send personal data or confidential information. Both of these can be obtained upon request to the ICT Service Desk.

3.9 Do not open any files that have come from an unknown source as these may contain a virus. (Files with extensions such as .vbs, .bat, .exe, .pif and .scr are particularly vulnerable and are often used to propagate malware). Contact the ICT Service Desk if you have any concerns.

3.10 Forwarding joke, chain or hoax e-mails is not permitted. They can cause offence and distress to some individuals as well as causing unnecessary demand on valuable IT resources. Inappropriate e-mails could be classed as bullying.

3.11 Your personal e-mail/webmail account must not be used to conduct council business.

3.12 Do not respond to e-mails or telephone calls from individuals asking for your password. These e-mails often state that the account will be suspended if you if you do not comply. This is a type of fraud known as 'phishing'. Reputable companies will never ask you for your password or for you to confirm it by e-mail. Do not open the links provided in these e-mails as they will direct you to bogus sites. Contact ICT Service Desk for further assistance.

3.13 Do not respond to unsolicited e-mails even to ask to be removed from their list. This just confirms that your e-mail address is in use and actually encourages them to send you more. Don’t respond to any direct e-mail from any organisation stating that they will remove you from mailing lists, or any offering to clear up your credit reference file. All these are attempts to gain your personal data.

3.14 Denbighshire County Council does not guarantee the accuracy of external e-mails received and users should take their own action to verify content before taking any action.

3.15 Staff should select “Reply” to the sender unless it is imperative that everyone on the recipient list needs to know your response when the “Reply to All” option should be selected.

3.16 The use of abbreviations and acronyms should be avoided wherever possible, as this will help with their understanding.

3.17 As e-mails are a record of Council Business and may need to be retained for set periods of time. Please refer to the Council’s Corporate Retention Schedule for guidance on this.

3.18 Although e-mail has a sense of immediacy, staff should not expect an instantaneous responses. Those matters which are urgent and require an early or immediate reply should be flagged accordingly and followed with a phone call or instant massage to ensure receipt.

3.19 Staff must consider the requirements of the Welsh Language Standards when using e-mail as a method of communication.

3.20 The Council’s Instant Messaging system has been provided to deliver a more informal and faster way of communicating with internal colleagues. The following key principles should be followed:

- Correspondence that involves a business decision or transaction should be conducted via a more formal method where a record can be retained e.g. e-mail;
- Please respect the recipient’s status e.g. if they have “do not disturb” or “in a meeting” shown, do not contact them; and
- Do not use the instant messaging system excessively. Usage can be monitored.

ACCESS CONTROL PROCEDURE

1 Introduction and Aim

1.1 The purpose of this procedure is to provide employees and members of the Council with a set of core principles under which access to Denbighshire County Council Information and IT Systems is permitted.

1.2 The aim of this procedure is to ensure access to our IT equipment, network and information is only provided to those individuals or organisations with a legitimate and lawful right.

1.3 This procedure does not apply to access to Council Information by members of the public in accordance with legislative or in connection with a legitimate customer service request.

2 Procedures

2.1 Acceptable Use

2.1.1 Council owned or supplied equipment and applications are for work related purposes only. As such, they should not be used to download or store non-work related information or files. Any information or file, held for personal rather than work related purposes is not permitted.

2.1.2 Denbighshire County Council's IT equipment and network must not be used to conduct any illegal activity including downloading or sharing unlicensed software and/or copyright protected material.

2.1.3 Denbighshire County Council IT equipment and network should not be used to conduct a business or used for the direct financial or commercial gain of or by its employees.

2.1.4 Images, cartoons or files containing nudity, sexually explicit, or other content of an illegal, racist or defamatory nature should not be stored on or sent using Council owned of supplied equipment.

2.1.5 There are additional policies relating to the use of the Internet, E-mail and Telephones which should be read in conjunction with this policy.

2.2 Access Control

2.2.1 Access to the Council's IT Systems is permitted for all Council employees as deemed necessary in accordance with their day to day duties and as requested by the Head of Service or their nominated representative. All requests for access should be directed to the ICT Service Desk.

2.2.2 Access is permitted for non-council staff or contractors in certain circumstances. Access will only be granted with the express permission of the Head of Service or their nominated representative where there is a specific business need and access is necessary in order to perform any function as directed by the Council or for the performance of any contract for and on behalf of the Council. All contractors or non-DCC staff should sign the personal commitment statement, which can be found in appendix 1, prior to access being granted.

2.2.3 Generic User ID's and Group ID's are not permitted. This is in accordance with the Code of Connection requirements for the Public Services Network[5] however; there are particular circumstances where this may be necessary and additional controls must be put in place to track and trace usage in these instances. Generic ID's must be specifically authorised by the Business Transformation and ICT Department. .

2.2.4 Sharing User ID's is also not permitted and all staff should have their own unique ID. Any request by a colleague to share ID's must be reported to your line manager.

2.2.5 Remote access to Denbighshire County Council IT network will only be permitted in accordance with the Council's Remote Access Policy and in accordance with the requirements of the Public Services Network Code of Connection.

[5] https://www.gov.uk/public-services-network

2.2.6 Access to IT Systems must be regularly reviewed by the systems administrators to identify any individuals who no longer require access or whether their access level is not appropriate for their current job role. It is suggested that access be reviewed at least once per year.

2.3 Wearing Official Identification

2.3.1 Employees of Denbighshire County Council are issued with official identification and these should be worn at all times whilst on Council premises.

2.3.2 Loss of Identification should be reported to a line manager who should arrange with HR Direct for a replacement to be issued.

2.3.3 People who are present on council premises and not wearing official identification should be challenged and requested to wear a visitors badge for the duration of their visit.

2.4 Visitors to Council Premises

2.4.1 Visitors and contractors who are required to have access to Denbighshire County Council premises should be logged in a visitors log or book and be issued with a temporary visitors pass, which they should be instructed to wear at all times whilst on council premises.

2.4.2 Ensure that where appropriate, visitors are accompanied and supervised at all times.

2.4.3 Staff based at publicly accessible sites or leisure facilities, should ensure that members of the public only have access to the areas that they are authorised to and not have access to designated staff only areas. In most cases access is controlled by the use of electronic door entry systems or cipher locks.

2.4.4 Any suspicious or unauthorised persons attempting to gain access should be challenged and reported immediately to the building manager for appropriate action to be taken.

2.5 Password Security

2.6 Passwords are an important security feature and the following guidance exists in relation to public services network connected organisation.

- It cannot contain your username or parts of your full name
- It must be at least seven characters in length
- It must contain characters from three of the following four categories:

  English uppercase letters (A through Z)
  English lowercase letters (a through z)
  Numbers (0 through 9)
  Symbols (for example, !, $, #, %)

  Examples of valid and invalid passwords:

  Q Invalid password examples: jones12345 or password1 or bob21
  R Valid password examples: Sunwindr&in99 or Za50yB*h or H0w*sthat

  In addition to the above password requirements, please also be aware of the following:

- You will be required to change your password every 45 days (with a 5 day reminder prompt)
- You will not be able to reuse any of your last 20 passwords
- You must not share your password with anyone
- You must not write down or display your password

2.6.2 Your password should be changed immediately if you suspect that it has been compromised. Any such suspicions should be reported to the ICT service desk as soon as possible.

2.7 Locking Workstations

2.7.1 Computer workstations must be locked using the ‘windows symbol + L’ or by pressing ‘control, alt + delete’ when you leave your computer unattended for a short break, at lunch time, when you attend meetings or are away from your desk temporarily. This ensures that any applications or information that you may have open and are working on are protected from unauthorised use.

2.8 Clear Desk

2.8.1 In accordance with the Council’s flexible working policy, a clear desk policy is in use within the Council. In particular, confidential, sensitive, information classed as official[6] or personal data should not be left unattended when not in use. This should be kept in a locked drawer or locker.

2.8.2 Any employee who discovers information of this nature has been left unattended should report this as an incident in accordance with the Information Security Breach Procedure.

[6] https://www.gov.uk/government/groups/public-services-network

INFORMATION SECURITY BREACH REPORTING POLICY

1 Purpose

1.1 In order to operate efficiently, Denbighshire County Council (DCC) has to collect and use information about people with whom it works with and for. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, there is other information which is created and held by the Council to perform its function which may be classed as commercially confidential or information which is protectively marked in accordance with Central Government data handling standards.

1.2 Organisations which process personal data and other sensitive data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. Many organisations take the view that one of those measures might be the adoption of a procedure on dealing with an information security breach incident.

1.3 Some key terms that are used in this procedure are:

- **Information assets -** our data, files and documents in any format (paper and electronic);
- **Information Security Breach -** an activity which causes or may cause the loss, damage, misuse or corruption of data (examples are shown in paragraph 2.4); and
- **Security Incident Management** – this refers to the process by which an information security breach may be investigated and the related management procedures; and
- **Personal data** – data which identifies a living individual either by itself or when matched with other data that would allow a clear identification to be made. Examples include – name, address, age, health, ethnic background etc.
- **Official Sensitive Information** – information which is confidential. This is the term used by central government in accordance with their protective marking scheme.

1.4 This procedure has been developed based upon good practice published by the Information Commissioner's Office (ICO) and the Cabinet Office who are responsible for information assurance in the UK. It will ensure that DCC responds appropriately and consistently to any actual or suspected breaches of security, which may jeopardise its information assets and systems and will ensure compliance with government standards for reporting and handling incidents relating to information transmitted via the public services network. This means that:

- a record is made of all such breaches;
- the breach is investigated thoroughly with associated documentation produced and stored on the corporate EDRMS;
- an assessment is undertaken on the on-going risk;
- the breach is contained;
- appropriate actions are taken to address the problem;
- management procedures exist to ensure and incident is handled correctly
- reports are made to external bodies and individuals as required;
- there is proper monitoring and oversight;
- any trends are identified and acted upon; and
- lessons are learned and our information security is improved.

1.5 This procedure encompasses the above requirements and aims to:

- reduce the impact of information security breaches by ensuring events and incidents are investigated and resolved appropriately;
- identify areas for improvement to decrease the risk and impact of future breaches; and
- protect the confidentiality, integrity and availability of our information assets at all times.

2 Context/Scope

2.1.1 This procedure applies to all DCC employees, members, contractors and other third parties who may have access to our information assets.

2.1.2 The consequences of an information security breach can be severe. From an organisational perspective, an information security breach can result in financial penalties, reputational damage, service disruption or even major service failure. Information security breaches may cause real harm and distress to the individuals they affect – lives may even be put at risk.

2.1.3 Disciplinary action could be issued against any employee that has found to have been negligent.

2.1.4 The following are examples of events that should be reported using this procedure. In summary, any event which potentially jeopardises the security of our information assets should be reported. It is also important that near-misses are reported to enable lessons to be learned and further protective measures to be considered.

- The theft or loss of any Council IT equipment such as laptops, mobile phones, USB stick, CD/DVDs;
- Theft or loss of any files or papers containing personal or confidential data (including credit card data);
- Break-in or other unauthorised access to a Council buildings where personal data or official-sensitive information is stored and may have been put at risk; and
- Disclosures of personal data or official-sensitive information verbally, in writing or electronically to someone who should not have access to it.

3 Procedure

3.1 There are a number of steps involved in this procedure which are detailed below:

3.1.1 **Step 1** - If a breach is suspected, the first step is to ascertain if there are any steps you can take to immediately recover the information that might have been lost or stolen and inform your Line Manager immediately. Your Line Manager must then contact ICT Service Desk (ext. 6299) to report the breach. Depending on the nature of the incident, the Line Manager may also need to contact the following:

- Police, e.g. if there has been a theft or break in; and
- Facilities Management Staff to make premises secure after a break in; or.
- CET Officer on duty (rota available on the DCC intranet) in the event of a critical incident occurring out of hours or at weekends.
- Consideration should be given as to what steps you can do in the short term in order to immediately to retrieve the information
- Where personal data has been lost or stolen or disclosed to unauthorised third parties then the Deputy Monitoring Officer and/or the Corporate Information Manager must be contacted in all instances.

3.1.2 **Step 2** – The ICT Service Desk will ask for and record basic information regarding the incident within the 'Supportworks' system.

3.1.3 **Step 3** – The ICT Service desk will refer the incident onto the appropriate person for investigation. The investigating officer will contact the person reporting the incident in order to gather information about the reported incident in more detail. In certain circumstances, this may require a face-to-face meeting and staff must be made available to attend this meeting.

3.1.4 **Step 4 -** The investigating officer will, in consultation with the person reporting the incident, complete an 'Information Security Incident Report Form' (see appendix 2). The purpose of the form is to create a record of the incident, which will include:

- details of the circumstances of the breach;
- identify the data affected*;
- identify the likely impact of the breach;
- assess the on-going risk;
- identify the causes of the breach;

- identify containment and recovery options;
- identify who to notify;
- agree upon a resolution or workaround; and
- agree corrective actions to be taken to prevent reoccurrence, with target dates for their completion.

*where the information security breach involves the loss or compromise of personal data the Council's Data Protection Officer will be contacted.

3.1.5 **Step 5** – Dependent upon the outcome of the investigation there might be a number of actions agreed at this stage. It will be the responsibility of the Line Manager to arrange for the implementation of the agreed actions.

3.1.6 **Step 6 -** After a mutually agreed period of time after the event (maximum of 14 days), the investigating officer and Line Manager will review the progress of implementing the agreed corrective actions.

4 Roles and Responsibilities

4.1 All DCC employees, contractors, members and other third parties who have access to our information assets are responsible for:

- ensuring the safety and security of that information and the systems that support it; and
- following this procedure for reporting all information security breach incidents.
- informing the service desk of an information security breach; and
- assisting with the completion of an 'Information Security Incident Form'.

4.2 Line Managers are responsible for:

- ensuring that a breach is reported appropriately by their staff;

- assisting with the completion of an ‘Information Security Incident Form’;
- arranging the implementation of the actions within the agreed timescales; and
- considering whether management action against the employee should be taken.

4.3 ICT Delivery are responsible for:

- recording of all information security breach incidents on the ‘Supportworks’ system;
- referring all information security breach incidents onto Corporate Information Manager for investigating;
- providing staffing and other resources as necessary to respond to IT security incidents in a timely manner; and
- Arrange or co-ordinate the procurement and installation of new products and services as required to recover from an incident or prevent the re-occurrence

4.4 Corporate Information Manager

- ensuring all associated documentation is created and stored appropriately;
- ensuring that an “Information Security Incident Form’ is completed;
- coordinating the response to a reported incident;
- analysing trends in information security breaches and recommending solutions;
- supporting the implementation of any recommend solutions; and
- providing reports on information security breach incidents to (SIRO);

4.5 Senior Information Risk Owner (SIRO)

- responsible for information risk on behalf of the Council;
- maintains overall responsibility for ensuring compliance with this procedure;

- providing reports on information security breaches to Corporate Governance Committee; and
- leads on an investigation into a suspected breach.

4.6 Data Protection Officer

- involved with investigating any incidents that involve the loss of personal data;
- act as the Data Protection Officer on behalf of the Council;
- determine whether the incident requires reporting to the ICO;
- make any reports as necessary and act as the point of contact with the ICO in relation to the loss of personal data; and
- provide legal advice and assistance as required.

5 Quality Control and Monitoring Compliance

5.1 This procedure is owned by the Council’s Senior Information Risk Owner (SIRO)

6 Further Guidance

6.1 Further advice and guidance on the details of this procedure is available from the Corporate Information Manager.

Appendix 1

DENBIGHSHIRE COUNTY COUNCIL
Personal Commitment Statement
Acceptable Use of DCC IT Systems

I understand and agree to comply with the Denbighshire County Council Information Security Policy, supporting policies and guidance which may be issued from time to time.

For the avoidance of doubt, the rules relating to IT systems usage include the below:-

- I agree that I am responsible for my use of the Denbighshire Network using my user credentials (User ID, password and/or access token if accessing via the Citrix Access Gateway) and e-mail address.
- I agree not to attempt to access any computer system that I have not been given explicit permission to access.
- I will not write down my password.
- I will not share my password with any other person, including colleagues.
- I will comply with the Denbighshire Information Security policy and associated policies at all times.
- I acknowledge that should I fail to comply with the Information Security Policy access to the Denbighshire Network may be suspended and/or withdrawn without prior notice.
- I will inform a representative of Denbighshire County Council and/or the Information Security Officer immediately if I detect, suspect or witness an incident that may be a breach of security.
- I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended.
- I will not remove DCC's equipment or information from the premises without appropriate approval.
- I will take all reasonable precaution to protect all computer media and portable computers when transporting them outside DCC premises.
- I will make sure I take every effort not to introduce viruses, trojans or other malware into the Denbighshire Network.
- I will ensure that my use of the internet is appropriate and I will not attempt to access unsuitable material (i.e. pornographic, sexually explicit or racist or defamatory content)
- I understand that my use of the internet is monitored regularly and that any suspected misuse may result in internet access being withdrawn without prior notice.
- I will not disable anti-virus protection provided on any DCC computer.

- I will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that Denbighshire County Council informs me are relevant.
- I acknowledge that my use of the Denbighshire ICT Network may be monitored and/or recorded for lawful purposes.

Send To: ***IT Service Desk, County Hall, Ruthin, LL15 1YN***

I agree to comply with all the requirements of the Denbighshire County Council Personal Commitment Statement – Acceptable use of DCC IT Systems, Denbighshire County Council Information Security Policy and associated policies and any subsequent guidance that may be issued from time to time.

Signed: ………………………………………………. **Date: ……………………..**

Print Name: ………………………………………………………………………..

UserID: …………………………………..

Appendix 2 – Security Breach Incident Form

Denbighshire County Council Information Security Breach Incident Form	
Date of Incident:	**Time of Incident:**
Time Reported:	**Date Reported:**
Name of person who discovered incident:	**Location of Incident:**
Reported By:	**Any other parties who have been involved** (Police, Caretakers, ICT etc.):
Service:	**Department**
Detailed description of the incident:	
Details of any IT equipment or applications involved:	
Description of any information/data compromised:	

Media of information/data (paper, electronic file, USB, CD/DVD etc.):	
Any personal data involved?:	
Cause of the breach:	
Is there any on-going risk?:	**Y/N**
What steps have been or will be taken to recover records/data (if applicable):	
What lessons have been learned from the incident and how will recurrence be prevented:	
For Information Management use only: Include in this space any other relevant information in order to make any follow up recommendations or actions.	
Actions Agreed:	
Action 1:	**Deadline:**

Action 2:	**Deadline:**	
Action 3:	**Deadline:**	
Follow-up Date:	**Officer Responsible for follow up:**	
Recorded on Supportworks?:	**Y/N**	
Does this incident need reporting to the ICO?:	**Y/N**	
Do the subjects need informing of the loss?	**Y/N**	
Who will inform the data subject? (insert name of officer)		
How will the data subject be informed? (insert agreed method of communication)		
Have the individuals involved undertaken any DP training within last 12 months?	**Y/N**	