Derby City Council

Appendix 2

Corporate Resources:
Information Security and IT Acceptable Use Policy

Author	Information Security Officer
Key stakeholders / contributors	Information Security Officer (ISO), Interim Director of IT (SIRO), Head of Technology, Data Protection Officer (DPO) IT Senior Project Managers, IT Infrastructure Team Leader, IT Security Officer, Team Leader - End User Computing, Information Governance Board.
Lead Directorate	Corporate Resources
Implementation due date	June 2018
Approval date and approving body	13th June 2018: Information Governance Board

Version Control

To make sure you are using the current version of this policy please check on iDerby or contact Information Governance when using printed copies.

Version Number	Date	Author	Reason for Version
1.0	May 2018	Information Security Officer (ISO)	Replacement of IT Policies: Information Security Policy v9.1 Laptop, Desktop and Tablet Device Security Policy Email, Internet Security and Monitoring Policy Remote and Mobile Computing Policy Email and Internet User Policy Internet File Sharing and Collaboration Sites Policy Malware Prevention policy Network User Policy
1.1	July 2018	ISO	Minor table amendment in S.14 to reflect secure e-mail details

Supporting information

Policy or strategy type	Internal Policy
Equality impact assessment date completed	17th May 2018
Review date	June 2019

Please tell us if you need this in large print, on audio tape, computer disc or in Braille.

You can contact Ann Webster on 64 3722, Minicom: 01332 64 0666 or Text Relay: 18001 01332 643722

Contents

Warning:

Because of the potential to compromise our cyber security defences, no-one should supply details of Derby City Council's IT infrastructure to any third parties without the explicit consent of the Head of Technology and Service Delivery.

1. Purpose

1.1 The purpose of information security is to protect the highly valued information assets of Derby City Council ('the Council', 'DCC'). The objective is to reduce the risk of information security incidents and be able to demonstrate to citizens and businesses that we collect, handle and store their information securely and in line with relevant legislation and compliance requirements.

1.2 Actions or neglect leading to a breach of this policy will be investigated, which could result in disciplinary action against employees. Breaches of this policy by a user who is not a direct employee of Derby City Council may result in action being taken against the user and/or their employer. In certain circumstances the matter will be referred to the police to consider whether criminal proceedings should be instigated.

2. Scope

2.1 The Information Security Policy applies to:

- Elected members of Derby City Council
- All permanent and temporary employees
- Consultants, contractors and agents employed by DCC
- Casual employees and volunteers

2.2 Please note that throughout this document, the words "employee" and "user" are used to cover all the groups of people listed above.

2.3 All employees should read this policy in conjunction with Derby City Council's Code of Conduct Policy and the Data Protection Policy available on iDerby.

3. Definition

3.1 The International Standard ISO/IEC 27001:2013 standard specification for Information Security Management defines Information Security as protecting three aspects of information:

- ***confidentiality-*** making sure that information is accessible only to those authorised to have access

- ***integrity-*** safeguarding the accuracy and completeness of information and processing methods

- ***availability-*** making sure that authorised users have access to information and associated resources when required.

4. Application

4.1 The Information Security Policy applies to **all forms of information**, including, but not restricted to, text, pictures, photographs, maps, diagrams, video, audio, CCTV and music, which is owned by, administered or controlled by the Council, including information, which is:

- Spoken face to face, communicated by fixed line, by mobile telephone, or by two-way radio.
- Written on paper or printed out from a computer system
- Stored in structured manual filing systems
- Transmitted by electronic mail, fax, over the Internet and via wireless technology
- Stored and processed via computers, computer networks, cloud computing storage, or mobile computing devices, including, but not restricted to, PCs, mobile phones, laptops, tablet PCs, electronic organisers and personal digital assistants (PDAs).
- Stored on **any** type of removable computer media including, but not restricted to CDs, DVDs, tapes, microfiche, diskettes, USB memory sticks, external hard disks, and memory stores in devices including, but not restricted to, digital cameras, MP3 and MP4 players.

5. Roles & Responsibilities

5.1 ***Information Security is not an option.*** We are all required to keep a minimum level of security to meet our legal and contractual obligations; and data sharing protocols with our partners.

5.2 All Council staff must:

- Comply with this policy and all related processes, procedures and guidelines at all times.

- Play an active role in protecting information in day-to-day work.

- Report any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or the Council's legal obligations without delay.

5.3 All Managers must:

- Promote good information security practice.

- Ensure this policy is communicated to all employees including temporary staff and that it is adhered to. In must be communicated to all elected members, contractors, agents and partners working for or on behalf of the Council.

- Ensure that all employees complete mandatory Information Security training.

- Assign owners to all information assets within their area of responsibility and ensure that roles and responsibilities are clearly understood - within Job Descriptions if appropriate.

- Ensure that information security is an integral part of all departmental processes including, but not limited to, business planning and risk audits.

5.4 The Information Governance Management Framework sets out the Council's Framework and arrangements for its management of Information Governance and includes a description of the following roles:

- The Senior Information Risk Officer

- The Caldicott Guardian.

- The Information Governance Team.

- Information Asset Owners.

- Information Asset Administrators.

6. Legal Framework for Information Security

6.1 The Council has an obligation to make sure that all information systems and processes meet the terms of all relevant legislation, mandatory compliance regimes and contractual requirements. The list below demonstrates the importance of using information correctly.

Common Law Duty of Confidentiality (below)
The Protection of Freedoms Act 2012
Health and Safety at Work Act 1974
Theft Act 1978
Indecent display (Control) Act 1981
Obscene Publications Act 1984
Copyright, Designs and Patents Act 1988
General Data Protection Regulation 2016 (GDPR)
Equality Act 2010

Computer Misuse Act 1990
E-Privacy Regulation 2018
Data Protection Act 2018
Human Rights Act 1998
Protection of Children Act 1999
Freedom of Information Act 2000
Regulation of Investigatory Powers Act 2000
Terrorism Act 2006
Limitation Act 1980

6.2 The Duty of Confidentiality

Coinciding with legislation is 'Judge-made' or case law; where Judges apply the law with reference to previous cases, or 'based on precedent'. This is called 'Common Law'. The Council, as a social care provider, has a duty of confidence derived from Common Law. The circumstances surrounding this duty are:

1. An individual gives information to the Council with an expectation that a duty of confidence applies to that information;
2. The information will not normally be disclosed further without the information provider's consent.

There are generally three circumstances which allow the Council to disclose confidential information:

1. Consent has been obtained by the information provider; or
2. The disclosure is necessary to safeguard the individual, or others, or is in public interest; or
3. The Council has a legal duty to disclose the information for example, to comply with a court order.

6.3 For requests relating to a deceased individual's information please see: 'Requests to access deceased individuals information' guidance available on the Information Governance intranet page.

6.4 Justification for setting aside an individual's right to confidentiality must be substantial and overarching, for example, 'public interest' tests require specialist knowledge and training of staff to determine this reason. Further information and guidance regarding the common law duty of confidentiality can be obtained from the Information Governance team, the Legal Service team or on iDerby.

7. Physical Security

7.1 Building Access and Identification

7.2 Building security is everyone's responsibility. Suspicious activity or any security weaknesses, for example, a broken lock on a secure door, must be reported immediately to the Facilities Management Team on FacilitiesManagementEnquiries@derby.gov.uk; 01332 640769 or Text Relay 18001 01332 640769.

7.3 Maintaining the physical security of offices and rooms where data is stored, maintained, viewed or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored must have a method of physically securing access to the room – for example, combination key lock mechanism. Lower /

floor level windows could also provide access to the room/office and must also be securely locked – particularly when the room is left unattended.

7.4 Rooms which have not been secured should not be used to store sensitive or personal information and data - concerns about any rooms/office which should be securely locked or access restricted must be reported to the Facilities Manager via FacilitiesManagementEnquiries@derby.gov.uk or on 01332 640769 or Text Relay 18001 01332 640769.

7.5 A clear distinction must be made between staff-only areas and publicly-accessible (escorted) areas such as meeting rooms and public spaces, to ensure that no documentation or viewable computer screens can be seen by non-DCC or DCC's agents.

7.6 Identification must be worn and displayed at all time. Tailgaters should be challenged.
Access to certain areas within the Council is restricted to certain members of staff who require access to carry out their role. Access is strictly controlled and can only be authorised by a Senior Manager.

7.7 Staff Taking Payment

Derby City Council must comply with externally imposed security standards, such as the Payment Card Industry security standards (PCI). These security standards ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. All Derby City Council employees taking card payment must refer to the Taking Payments and User Guidance document for specific guidance about PCI, as well as completing the mandatory PCI training course. The Council's Merchant Services intranet page, containing details of PCI can be found here. For further information about PCI, please refer to the official PCI standards council.

7.8 Staff with access to financial data as part of their role must ensure it is handled appropriately, particularly when it is in unencrypted form, such as direct debit, BACS and customer bank account details.

8. IT Asset Management

8.1 DCC purchases assets (laptops, tablets, mobile phones etc.) for the express use of executing DCC business. These assets are assigned individually and recorded centrally in an asset register managed by the End User Computing (EUC) team within IT Services.

8.2 Staff are personally responsible for assets assigned to them. Devices kept at home should be locked away when not in use if at all possible. Assets should not be left visible in vehicles or left out on desks.

8.3 If leaving assets overnight in council buildings they must be locked in a secure location (locked cupboard or locker).

8.4 Devices no longer in use should be returned to EUC as soon as possible for assignment to another user. Only EUC can reassign equipment to a different owner. Equipment should not be reallocated within a service. This is because the asset register will record the original owner and this will need to be modified. It is normal practice for EUC to rebuild the laptop for the new user.

8.5 The EUC team are based on 3rd Floor of the Council House, area T21.

Note: Redundant equipment must be returned to the End User Computing Team and must not be kept by Services as ‘spares’. Please see the IT Device Lifecycle Policy here for more information.

8.6 Disposal of IT Equipment

Disposal of computer equipment must be via IT Services who will ensure that disposal is managed in accordance with the equipment disposal policy and WEEE regulations.

8.7 Records Management

Due to the nature and informational value of records created, controlled and processed by the Council, good records management must not be undervalued for the vital and effective delivery of services. Paper and Electronic records must be stored, managed, archived and destroyed in accordance with law and the Council’s Information Asset register and retention schedule.

8.8 Backup and Storage

8.9 Users must be aware that data copied to local device drives is not backed-up. Locally stored data (for example; saved to desktop or ‘My Documents’) is at risk of loss, corruption or denial in the event of device failure, corruption or malicious software attack.

8.10 The IT Service takes responsibility for backing-up data to the servers. Data backed-up to server storage is usually overwritten within six weeks. Do not assume deleted documents will be available from back-up once they have been deleted. There is potential for IT Services to restore data from back-up but this cannot be guaranteed. The assumption is that due to the effort, time and cost of recovery, restores of user data will only be done in extreme circumstances.

9. Malware

9.1 Malware is short for **mal**icious soft**ware** and covers viruses, worms, spyware, Trojan horses etc. Its various forms are designed to disrupt computer operation, gather information, corrupt and/or delete data on a computer and gain access to computers and networks. The most common way that Malware is spread is from an email attachment, downloaded internet file, infected CD/DVD or USB memory stick; they can infect networked and stand-alone computers.

9.2 By understanding and implementing our responsibilities we will help minimise the risk of:

- an infection
- a denial of service attack
- data loss should Malware break through our defences.

9.3 Malware can be introduced to a computer by:

- downloading files from a web page
- launching software or tools from a web page
- infected web pages
- opening emails and email attachments from known and unknown external sources
- opening compressed files sent by email (to avoid mail gateway security)
- CD's and DVD's
- external storage devices, such as a USB memory stick.

9.4 The indicators of a possible infection include:

- applications that don't work properly
- file size changes for no apparent reason
- date of last access does not match date of last use
- an increase in the number of files on the system when nothing has been added
- unusual error messages
- system slows down, freezes or crashes.

9.5 This list is not comprehensive but the consequences of a malware infection can include:

- lost productivity through data and devices being unavailable
- lost data and access
- legal implications if deadlines are missed
- financial loss if deadlines missed
- compliance failures which may mean partners or the government deny the Council access to their systems and data
- confidential and/or sensitive data being put into the public domain

- put at risk citizens or businesses whose data was compromised
- cost of additional compliance assessments to demonstrate security vulnerability has been closed
- cost of cleaning the network
- unreliable applications, and corrupted files.

9.6 Hoaxes usually take the form of an ‘urgent virus warning’ email message. They usually contain false reports about new undetectable viruses and urge recipients to forward the warning to as many people as possible. This mass forwarding then produces similar effects to a true malware infection and could potentially overload an email server. Another common hoax is when an email tells you to look for certain files on your computer and delete them and then email everyone in your address book. If you follow the instructions without checking if it is a hoax, you may delete essential system files which are necessary to run your computer.

9.7 **If you suspect malware on your PC disconnect from the network (including disconnecting from Wifi using the function key) if this is not possible then turn the PC off, and call the IT Service Desk on 640 530 (01332 640 530) or Text Relay 18001 01332 640769 immediately or visit the IT Clinic on the 3rd floor of Council House.**

9.8 Do:

Connect DCC equipment (laptops etc.) to the Council at least every 30 days for a period of four hours to receive all necessary security patches; and

Do not:

Ignore any malware warnings or share suspect emails with others (except IT services under their guidance);
Download any software to Council ICT systems or equipment .This includes ‘free’ software, screensavers and games;
Download software following a warning from a software program you do not recognise;
Connect a personal memory stick to a Council owned computer;
Leave any removable media in a computer when switching off; or
Power down your laptop during software updates.

Note: Beyond the technical measures implemented by the IT team, you are the last line of defence against Malware.

10. Network Access and Account Management

10.1 User ID – Unique Network User Identification

All authorised DCC IT users are provided with a unique User ID to access the DCC network; these are referred to as ‘Network’ accounts.

10.2 No attempt shall be made to sign on to or use any system or database using someone else's User ID. Users **must not** use or encourage others to use anyone else's personal ID and password to log onto or a PC, the network, individual system or email.

10.2 It is a criminal offence under the ***Computer Misuse Act 1990*** to access a computer system without authority to do so.

10.3 New Starters, Transferees and Leavers

10.4 All employees, permanent or temporary, of the Council, and any volunteer working for the Council with access to information, has an absolute duty to respect the confidentiality, integrity and availability of information they have access to in the course of their duties.

10.5 Employees and Members must adhere to the Council's Code of Conduct which details obligations regarding disclosure of information, use of IT and data security, use of systems, equipment and confidentiality.

10.6 All employees also have a duty of privacy and trust to all our customers and data subjects.

10.7 New Starters

10.8 Completion of the Council's Information Governance training courses is mandatory and failure to complete this as part of employee induction and/or refresher training may mean that you are unable to access the information required to fulfil your job. The level of training will vary between jobs depending on the access to information the job involves but a minimum level will apply to all employees. If in doubt ask your line manager or contact the Information Governance team.

10.9 Council Members will receive appropriate information during their induction training.

10.10 Network User Account Creation

User accounts will only be set up following completion of an IT Service request via the new user e-form on iDerby to ensure the correct authorisation is achieved and recorded.

10.11 Transferees

Where an employee transfers from another job within the Council, the manager of the team they are joining must provide notification to IT Services of the transfer and ensure that access privileges are revoked, amended and set up where necessary via the appropriate e-form on iDerby.

10.12 User Account Amendment

Changes to User accounts including access rights to files, folders and databases must be agreed by the user's line manager and permission forwarded to the IT Service Desk.

Note: Accessing data/information that is no longer required in your role is contrary to data protection legislation. Disciplinary action may be taken against employees should they access data/information inappropriately.

10.13 End of Employment

10.14 All DCC assets remain the property of the estate and on leaving the employment of the Council, all equipment & software must be returned to the EUC Team. The EUC team are based on 3rd Floor of the Council House, area T21.

10.15 Managers must follow the Managers Guide for Leavers and ensure that arrangements are made to remove all access privileges:

- For permanent staff leaving the Council an Establishment Control Form (ECF) should be completed by managers and forwarded to the IT Service Desk.
- For temporary employees, the relevant form on iDerby should be completed by managers.

10.16 Where notice of termination or transfer is provided managers should ensure that any current or relevant computer files and/or emails that need to be retained have been identified with the leaver prior to the termination date, to ensure service continuity and in line with records retention practices.

10.17 Emails should be forwarded as appropriate for the needs of the business and the remainder deleted. Home drive files should be moved if appropriate and files no longer required should be deleted.

10.18 Ownership of 3rd party contacts, contracts etc need to be transferred from the leaver to appropriate user(s), for example transfer of licence ownership of particular software.

10.19 DCC will take the necessary action to reclaim all equipment, software and information that has not been returned by the member of staff (for example, by means of final salary payment).

Note: Unless there is a policy or legal obligation for them to be retained, the IT Service Desk will delete the User account and all contents in the User's Home drive on the date they cease employment with the Council.

11. Password Policy

Access to DCC systems on the network requires a password. Keep all passwords secure and change them regularly. Do not reveal, write them down or share[1] them with anyone, unless as a reasonable adjustment under the Equality Act.

IT Services automatically enforces a password change every 150 days on a user's network account.

Passwords shall consist of the following:

- Minimum of 8 characters
- Contain at least one character from ***each*** of the following categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Numbers (0 through 9) or a symbol (i.e."£!$%^&*).

Passwords shall not contain the user's account name, team name or parts of the account name.

Users must not use the following words or any variation of them utilising numbers and symbols:

- 'password', i.e. Passw0rd, P@ssword or Pa55word
- Training/Trainer – Training1, Tr4ining, Tr4iner
- Testing/Test – Testing1, T3sting, Te5ting
- Derby – Derby1

Passwords cannot be reused within 20 changes.

Users must not use recognisable patterns or words in their passwords, examples include months and years eg Januarry2016!, Names and birthdays eg; J0Eblogs01062000

11.1 Any document containing passwords must not be stored on shared drives or written in an accessible location, for example, in shared desk diaries.

11.2 Unattended computers or Wyse terminals must be logged out or locked (note: turning the screen off on a Wyse terminal does not disconnect the user session). Documents that contain passwords must be encrypted or passwords should be stored in an appropriate electronic key vault.

11.3 Users must not store personal, non-business related information on network drives. If IT Services identifies non-work related personal information, for example, family photos, held on any server or network drive as part of a

[1] For the purposes of resolving a service call, the low level password/PIN may need to be divulged to a member of IT in order to complete the request.

storage audit they will notify Information Governance and they will be removed.

11.4 Authorised users must not view, amend, or delete any record of any individual service user known personally to the authorised user or on the request of someone known personally to the authorised user unless authorisation has been sought and given by line managers. If you realise you are accessing a record of a person known to you, you should stop and report this to your manager unless the issue is time critical (in which case you should inform them as soon as possible).

11.5 Authorised users must store all business related information on shared team drives. This ensures that all files are accessible to the team.

11.6 Users must **not** connect non-Council owned equipment or mobile devices to the corporate network.

11.7 Password Do's and Don'ts
Do:

Lock computer screens when temporarily leaving devices which are in use;

Log out or shut down computer devices when they are not in use;

Protect PINs, passwords and Usernames from inappropriate disclosure; and

Change passwords regularly, avoid using the same password for multiple systems.

Do not:
Cause, allow or assist with the unauthorised access to, or disclosure of, personal or
corporate sensitive information.

Note: Staff must be mindful that writing passwords down is a significant security risk and should not do so. The back page of a diary or day book is NOT a secure place to write down passwords!

11.8 Laptops

11.9 Laptops are secured with low-level, high-end encryption, the password for which is the responsibility of the laptop user. The password and/or PIN used with laptops must not be divulged to anyone.*

11.10 Do not:
Leave laptops, other devices or documents containing personal information in vehicles overnight;
Under no circumstances should users write PIN codes or passwords down and keep them with the device; or

Power down your laptops during software updates.

12. Removable media

By default users are not granted permissions to use removable media such as DVD drives, USB memory sticks or portable hard disks. Access to removable media is granted where a clear business need is present. If a USB memory stick is required for work purposes, it must be encrypted.

Note: All removable media must be encrypted when being transported.

13. Home and Remote Working

13.1 Home Working

13.2 When working at home, information must be used and managed in accordance with the policies and procedures within this policy and with the home workers and occasional home workers policy available on the Council's intranet.

13.3 Council data **must not** be shared with unauthorised individuals. Only authorised members of staff are allowed access to Council information being used at home in any form, on any media. No unauthorised individuals shall be allowed access to the equipment or information.

13.4 Where employees work permanently from home, they must do so in accordance with the home based workers policy, and this Information Security Policy.

13.5 All paper files must be neatly filed and stored away when not in use. Confidential documents must be stored in a locked container (filing cabinet, lockable briefcase). When files or equipment are stored at home they should not be openly accessible to other members of the household or visible from outside the premises.

13.6 Council data must not be stored on personal cloud storage such as Onedrive, Dropbox, amazon files or google storage. Council emails should not be forwarded to personal mail accounts such as Outlook, Hotmail or Gmail.

13.7 Using the Citrix Access Gateway

DCC permits the use of an approved secure remote gateway to Council emails and files. This is currently the only way users can access such information from a non-Council computer. See 'Bring your Own Device', Section 16 in this Policy. 'Citrix' can be requested and installed by following instructions provided on iDerby; it will not allow staff to make local copies of any email or Council file.

13.8 Usage in any publicly accessible area

13.9 Confidential corporate or personal information should not be discussed in a public area or anywhere it can be overheard. Do not display confidential corporate or personal council data on your laptop or on paperwork in a public place. Keep usage to a minimum in public areas due to the threat of ‘overlooking’ and / or theft.

13.10 Any member of staff choosing to use information and/or devices in public areas that results in any security breach will be required to state why the usage was necessary and the steps they took to protect the information and / or equipment.

13.11 Equipment in use must not be left unattended at **any time**.

13.12 Usage in Areas not generally accessible to the Public (including other organisational premises)

13.13 Employees are responsible for ensuring that unauthorised individuals are not able to see information or access systems.

13.14 If equipment is being used outside of its normal location and might be left unattended, the user must secure it by other means (for example, security cable, available from EUC).

13.15 Transferring Data outside of the European Economic Area

The DPA 2018 has strict guidelines regarding the sharing of information outside of the European Economic Area (EEA) and to countries outside of the privacy shield. Please refer to the guidance on the ICO website that provides further guidance and detail around sharing information outside the EEA and the relevant considerations. If we are considering transferring data to another country our Information Governance Team will be consulted in the first instance and they will advise on whether the transfer can take place.

13.16 Transporting Data

13.17 Files and equipment should only be removed from the workplace where there is a business need to do so and they should be returned as soon as possible.

13.18 Keep equipment secure and out of sight during transit for example, in a locked car boot.

Council equipment or personal information must not be left in any vehicle overnight. Where a courier service is used to transport packages containing sensitive information, tamper proof packaging must be used.

14. Email and Internet Use

14.1 Use and Monitoring of Email

14.2 The Council's email and internet facility is made available to authorised users for Council business purposes with limited personal use being permitted.

14.3 The Council recognises there are risks associated with the use of email and users must take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Email users should assume that email messages may be read by others and not include anything that would offend or embarrass any reader, or themselves, if it found its way into the public domain.

Compliance with this policy will help mitigate the following risks:

- Harm to individuals
- Damage to the Council's reputation
- Potential legal action and/or fines against the Council or individual(s)
- Inappropriate use of council resources
- Viruses and other malicious software (malware)
- Service disruption

14.4 Authorised users **must not** use email for doing anything that is illegal under any law or would contravene any Council policy, procedure or guideline. Particular regard must be given to emails containing information described in the OFFICIAL – SENSITIVE categories in section 17.8 of this policy, including:

- Gender
- Gender identity
- Race
- Sexual orientation
- Age
- Disability
- National origin
- Religious beliefs
- Political beliefs

14.5 All authorised users must take care to ensure that emails are sent only to those who should receive them. It is advisable to re-read emails before sending to ensure that:

- the recipient's address is correct (particularly if they include personal or sensitive information)
  - Consider if the address is a cached e-mail addresses - for example if you have two people of the same name in your Outlook addresses, are you sure you are sending the email to the correct person;

- the email is intelligible and clear in its content;
- the content will not embarrass or subject the Council to legal proceedings or a fine; and
- Personal information is NOT included in the subject field of the e-mail.

14.6 An email address can be considered personal data. When you send an email and the address is visible to others it could be a breach of data protection laws if they have not given permission for it to be shared. If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (Bcc), not carbon copy (Cc). When you use Cc every recipient of the message will be able to see the address it was sent to. Users should be aware that if they are a Bcc recipient and reply to the email all the recipients in the To and Cc lines will see the reply – thereby losing the anonymity.

14.7 In the interests of transparency then use of BCC should be avoided except for this purpose.

14.8 Other than shared mailboxes, email accounts are unique to each employee and account details must not be shared. If another party needs to administer an individual's account the delegate facility within Microsoft Office should be used.

14.9 For any planned absence an appropriately worded 'Out of Office' automatic response must be used with a format detailing unavailability and alternative contact(s).

14.10 If you are unexpectedly away from the office access may be given to your line manager to view your mailbox for incoming mail items. This will be for urgent, business reasons only.

14.11 The use of email and internet must comply with national and European regulations which will, where possible, be enforced by email and internet gateway security and audit logging tools. If the Council receives a report of a suspected breach of the regulations it is duty bound to investigate. Email messages may be disclosed under data protection laws, Environmental Information Regulation, the Freedom of Information Act 2000 or in legal proceedings.

14.12 Email messages should be treated as potentially retrievable, either from the main server or using specialist software. Staff should not treat email as a storage solution and rely on IT services being able to recover old emails.

14.13 Managers can request access to a member of staff's emails or Home drive in circumstances such as sudden sickness, or as part of an investigation, by completing the relevant form on the intranet and sending it to the IT Service Desk who will then confirm access with the appropriate HR business manager.

14.14 Secure email

14.15 Information sent by email outside of approved government networks is not secure. Do not send confidential data via email to other organisations unless a secure email link has been set up, a secure messaging system is being used by both parties or the data is encrypted before sending.

Any User who wishes to send email securely to other public organisations (police/health etc.) shall do so via secure mail ensuring the recipient is known. Secure Email can only be assured when following the principles, below.

The address you are communicating with	**The type of email account you require**
(anyone)@**derby.gov.uk**	You do not require a secure mail account. Your normal **@derby.gov.uk** email account can communicate securely with these organisations.
(anyone)@**derbyhomes.org**	
(anyone)@(anything).**gcsx.gov.uk**	You will require a Government Connect (GCSx) email account to securely email these organisations (this may change from April 2019)
(anyone)@ (anything).**gse.gov.uk**	
(anyone)@(anything).**gsi.gov.uk**	
(anyone)@(anything).**gsx.gov.uk**	
(anyone)@(anything).**pnn.uk**	
(anyone)@(anything).**nhs.net**	
(anyone)@(anything).**nhs.uk**	
(anyone)@(anything).**cjsm.net**	You will require a CJSM account if you are sending emails requiring secure transfer. See 14.16.
(anyone)@**justice.gov.uk**	You will require a CJSM account to share material requiring secure transfer.
Secure email to other recipients (not listed)	You need an Egress Switch account. This is free to receive email, but there is a licence required to be able to send. Contact IT Services for further information.

14.16 CJSM clarification:

Other organisations may have set up CJSM accounts for their staff. Their email address will appear to be a normal address with ".cjsm.net" added on the end.

Example: john.smith@hospital.nhs.net.cjsm.net

As this email address ends CJSM.net, you will need a CJSM account to be able to securely email this person (not required for routine emails).

14.17 **Email Do's and Don'ts**

Do:

Use the email system in line with this policy and the staff Code of Conduct;
Use appropriate language in messages, offensive content will not be tolerated;
Check the address of the intended recipient is absolutely correct; and
Use an appropriate signature on emails; an appropriate template can be found on iDerby.

Do not:

Engage with mass emailing transmission of unsolicited emails (SPAM);
Attempt to assume the identity of other users, entities or organisations;
Change the content of a third party's message without their approval;
Transmit material intended to misguide or mislead the recipient regarding the originator;
Forward Official or Official Sensitive information to your home email address;
Open emails which you consider to be suspect. Contact the IT Service desk;
Open an email attachment or a link in an email from an unknown external source; or
Reply or forward emails you suspect may be a malware attack or a hoax.Include personal information in the subject field of the e-mail.

14.18 Use and Monitoring of the Internet

14.19 Authorised users must recognise that the Council's Internet facility is provided for business use and must be protected from unreasonable and excessive personal use:

- Use must be minimal and take place outside of your working hours (i.e. during lunch hours, before or after your recorded working hours);
- Use must not interfere with business or office commitments;
- Users must comply with the Council's information security policies and the Employee or Elected Members' Codes of Conduct

14.20 If you make an electronic comment on the Internet (blogs, social media, twitter etc.) on a personal basis you must be aware that, as an employee of the Council, you are expected to comply with the standards of conduct and behaviour in this policy and the Employee and Elected Member's Code of Conduct. The Council can be held legally liable for on-line content published by one of its authorised users – even when posted in a personal capacity at home or at work.

14.21 **Internet Don'ts**

Don't:

Allow third parties, contractors or suppliers to remotely access/take over your

PC or laptop via the Internet (a supplier or contractor can instigate this by asking you to accept a connection or click on a link on their website) without first obtaining approval from IT Services. For advice contact the IT Service Desk.

Claim to represent the views of the Council unless you have permission to do so as part of your job. Similarly, you must not try and pass off your own comments or views as being from someone else by, for example, falsifying your email address or using someone else's.

Use social media, the Internet, intranet, media, or social media sites to make complaints about your employment. If you want to make a complaint about any aspect of your employment with the Council you must use the appropriate employment procedure.

Create, download, upload, display or knowingly access sites that contain, or might be deemed to be:

- Pornographic
- Illegal
- Obscene or offensive (racially, sexually, religious, disability, sexual orientation, or otherwise discriminatory, or of an extreme political nature)
- Subversive or violent.

Access to such sites may be granted role based approval by IT Services.

14.22 As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that the Council's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

14.23 Copyright

The unauthorised copying, distribution or possession of intellectual property (copyright material, designs, patents, trademarks, inventions, ideas, know - how, business information and lists) are an infringement of copyright and are strictly forbidden. Copyright works include text, graphics, still images, computer software, music and video clips. Any unauthorised copying of those materials by an authorised user could render the Council and staff liable under civil and criminal law.

15. Internet File Sharing/Collaboration

15.1 The Council defines an internet file sharing or collaboration tool as a tool that allows users to connect with each other and to upload or download files from an internet location. Examples include Dropbox, Google- drive, Microsoft One Drive, but there are many other such tools. The use of such sites is **not**

allowed as they pose a number of risks that could lead to a serious breach of data security, these include:

- The data may be hosted on servers outside of the European Union and in territories without equivalent data protection regulations.
- Data uploaded to such sites is not always fully encrypted and may be subject to unauthorised access.
- We cannot audit or control data once uploaded, and therefore cannot ensure unauthorised access does not occur, or if it does cannot trace the access and take mitigation action.
- We cannot control and remove access from former authorised users when they leave and thus they may still have access to confidential documents.
- Many of the providers of such sites include in their terms and conditions either transfer of ownership of the uploaded documents and images or a right for the site to share them without consent of the owner. They also often transfer the jurisdiction for any disputes outside of the UK and European Union.

15.2 We are exploring the possibility of an internet file sharing utility that can meet the respective data protection and information sharing regulations and that can be managed in terms of audit trails, access security and user account management but until we can establish such we have no option to prohibit the use of such internet file sharing/collaboration sites.

15.3 For the avoidance of doubt **no** Council employee, elected member, contractor, agent, partner or temporary staff member is allowed to register for internet file sharing and collaboration sites using their Council email address. Any authorised user doing so may face disciplinary action.

15.4 If you can justify a valid need to do this, then on approval of a business case that explains why this is needed and how we can address the security requirements permission may be given by the Information Governance team and/or the Council's Senior Information Risk Owner. A register of such exceptions to the otherwise total ban on such sites will be held centrally.

15.5 The Council cannot prevent authorised users registering for such sites with their own, non-council, email. However, uploading Council data to such sites using a personally registered email account is a breach of this policy and may lead to disciplinary action.

16. Bring/Use Your Own Device (BYOD)

16.1 If approved by their management, staff are able to use their own personal smart phone or tablet to receive and send email, access the intranet etc. via Council approved and managed software. In allowing access to emails (and potentially other services in the future) the employee must agree to this Information Security Policy. In addition, agreement to this policy is implicit from the point that the application is installed on the personal device. It is the authorising manager’s responsibility to direct the employee to the appropriate policies so that they can make an informed decision before installing the application on their personal device.

16.2 Should a user decide that they no longer require work related email on their BYOD device, it is the user’s responsibility to ensure that the works email account is removed from the device, either before continued use or planned disposal. The user must also inform IT services that they no longer want to access corporate email on their device.

16.3 The user must inform IT services immediately should the device be lost or stolen. IT Services can then remotely wipe the Council email content from the device.

16.4 As a minimum, Bring Your Own Device (BYOD) Mobile devices must be secured using an eight character PIN or via biometrics (fingerprint, facial recognition, eye recognition etc).

16.5 Council equipment must not be used to download and store copyrighted material, music files and videos. This is illegal and may result in disciplinary action. Regular monitoring and reporting on this takes place.

16.6 **BYOD Don’ts**
Do not:
Connect any personally owned or non-Council owned devices to the DCC network. Doing so could introduce malicious software and related security risks.

17. Government Security Classification (GSC)

17.1 GSC affects all public sector organisations and applies to information that we create, collect, store and process.

17.2 GSC applies without exception to all employees whether they are permanent, temporary or contract, together with Councillors, volunteers and staff working for partner or subsidiary organisations including the police service and arms-length management organisations. Delivery partners, such as Derby Homes Ltd, and their wider supply chains are also expected to comply.

17.3 There are four key principles underpinning the scheme:

- All information has intrinsic value and so requires an appropriate degree of protection
- All of us who work with a public organisation have a responsibility to safeguard data we access, (whether or not it is marked), and we should undergo appropriate training
- Access to sensitive information must only be granted on the basis of a genuine need to know and with appropriate security controls in place

- Assets we receive from or exchange with external partners must also be protected in accordance with any relevant legislative or regulatory requirements. This includes any international agreements and obligations

17.4 Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats. It means that all our information has to be classified in such a way that we can easily see the level of sensitivity contained in it.

17.5 Classification Types:

17.6 OFFICIAL: This classification covers all information created or processed by us that is not covered by the classification Official - Sensitive. There is **no need to mark these documents as Official as it is the default for everything other than those specifically identified as Official – Sensitive.**

17.7 OFFICIAL covers routine business operations and services, even if it might have damaging consequences if it were lost, stolen or published in the media. Examples of this type of information are available on iDerby here.

17.8 **OFFICIAL – SENSITIVE**: This classification covers a more limited set of information that could have more damaging consequences if it were lost, stolen or published in the media. It **must** be used on all information that falls within the statutory definition of special categories of personal data and criminal convictions defined in Section 10 of the Data Protection Act 2018. This is where the information relates to a person's:

- Race;
- Ethnic origin;
- Political opinions;
- Religion;
- Membership of a trade union
- Genetics;
- Biometrics (where used for ID purposes);
- Health;
- Sex life;
- Sexual orientation;
- Gender identity; or
- Criminal offence data, including convictions and offences or iinvolvement in any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court.

Examples of this type of information are available on the ‘Classification Types’ page of iDerby here.

17.9 When classifying a document as ‘Official – Sensitive’ the classification text should be placed in both the header and footer of the document or manually placed in the subject field of written communications such as in an email.

18. Security Incidents

18.1 Security incidents can include a range of situations which could lead to damage to operational effectiveness, harm to reputation both organisationally and personally.

18.2 All breaches of Information Security, actual or suspected must be reported, investigated, reviewed and acted upon.

18.3 Recognising an Information Security Incident

There is no simple definition of an information security incident but generally it will involve an adverse event which results, or has the potential to result in the compromise, misuse or loss of Derby City Council owned or held information or assets.

Some examples of information security incidents include (but are not limited to):

- The loss or theft of information or equipment;
- Incorrect handling of protectively marked information;
- Poor physical security, hacking, computer virus;
- Information disclosed in error;
- Unauthorised use or access to information or systems;
- Physical records lost, damaged or destroyed;
- Data posted, faxed or e-mailed to the incorrect recipient.

18.4 An incident can be caused by any number of reasons for example human error, lack of awareness or training, deliberate or accidental disregard for policy.

18.5 The impact of a security incident can vary greatly depending on the type of information or asset involved. It may for instance lead to an infringement of privacy, fraud, financial loss, service disruption or reputational damage.

18.6 Once reported, the Information Security team will review the incident details and if necessary, provide details to the regulatory body.

18.7 Reporting an Information Security Incident

18.8 All actual or suspected breaches of security and / or the information security policy must be reported in accordance with the process described on iDerby in the link below:

https://iderby.derby.gov.uk/governance/information-governance/information-security/

18.9 **Information security incidents should be reported to the information security team within 24 hours of becoming aware.**

Cyber Security incidents should be reported to the information security team OR to the IT Service Desk immediately. If the Service Desk is not available leave the PC disconnected from the network until you can take advice.

Note: The purpose of reporting an incident is primarily to ensure that any impact is minimised and lessons learnt can be identified and disseminated.

18.10 Major Incident Policy

18.11 In the event of a major incident, IT Services may need to withdraw services with little or no notice in order to protect the network environment. Whilst every effort will be made to consult with key stakeholders and to notify services of any imminent outage there will be occasions where this isn't practicable. IT management have delegated authority to react as necessary in the face of a serious threat.

Note: In the event of a major IT incident all staff are required to respond positively and in a timely manner to instructions from IT Services.

18.12 All major incidents will be thoroughly investigated and a report of the event and any lessons learned will be published on the Council's Intranet where appropriate.

19. Electronic and Confidential Waste Disposal

19.1 Confidential Waste disposal

19.2 Official DCC documents must be disposed of via the DCC confidential waste system in the designated print areas of the Council house or designated confidential waste repositories in offices.

19.3 The destruction of information should be carried out in accordance with the Council's Approved Retention Schedules.

19.4 On no account should any confidential waste be placed in other types of waste receptacles for example, those for normal recycling, wheeled bins, skips etc.

19.5 Staff with approval for mobile working or have authorisation to work from home or another work base must have procedures in place to safeguard information effectively. This includes the safe disposal of any confidential waste. In such circumstances, this information should be brought back to the Council for secure disposal by shredding or placed in the secure confidential waste containers where available.

19.6 Electronic Device Disposal

The process for the secure disposal of computer devices and erasure of hard drives and memory sticks can be found in the IT Device Lifecycle policy on iDerby and by contacting the IT Service Desk.

20. Business Continuity and Risk Management

The Council's critical business systems must be identified by the system and/or asset owners. They must ensure that a risk assessment is undertaken which will inform future resilience, service continuity and disaster recovery arrangements. This must be reviewed and submitted to the Information Governance team.

21. Compliance with the Information Security Policy

21.1 The Information Security Officer is responsible for monitoring compliance with this policy and will advise the Council's Senior Information Risk Officer (SIRO) and Chief Officers both periodically and following major incidents.

21.2 If employees knowingly do not comply with Council policies, procedures or guidelines, the Council may take appropriate action in accordance with the Employee Code of Conduct.

22. Other Relevant Policies, Standards and Procedures

Supporting resources can be found on iDerby or contact the Information Governance team.

23. Contact Details

The Council's Information Governance team:
Email: information.governance@derby.gov.uk or telephone: 01332 640763 or Text Relay 18001 01332 640763

To report an information security incident, please access the Information Security page on iDerby, complete an incident form and forward it to the Council's Information Security team:
Email information-security-breach@derby.gov.uk or telephone: 01332 643117 or Text Relay 01332 643117