Doncaster Council

Information Security Policy

Version:	3.4
Author:	Information Governance Team
Approved by:	
Date approved:	
Review date:	
Target audience:	All Staff / Citizens

Contents

1 Summary

This policy sets out how the council will protect information and explains what the council's rules are to ensure information is held and used securely. It shows how we comply with recommended security standards, how we define different categories of information, how it is valued, and how it is managed.

2 Scope

This policy applies to employees, contractors, agency staff and councillors. It covers information we collect and use on paper and electronically. It covers video and photographs, voice recordings, CCTV and mobile devices such as laptops, mobile phones, memory sticks and pendant alarms. It covers all information used on council premises, stored locally or in the cloud including social media and / or worked on by staff or other people or organisations working under the direction or authorisation of the council

3 Aims

The aims of this Policy are to ensure that:

- Information is valued and protected accordingly from unauthorised use, access or disclosure,
- Information is accessible and available and the integrity of information is maintained,
- The council knows where all information is held and used,
- Information held by the council is protected from all threats, whether internal, external, deliberate or accidental,
- Regulatory and legislative requirements are met,
- All members and officers of Doncaster Council, processors acting on the council's behalf and third party organisations are aware of, understand and are accountable for the appropriate handling of information,
- Everyone duly authorised to use information, is aware of procedures to protect information in different circumstances,
- Originators of content are authenticated and provide non-repudiation,
- All breaches of information security, actual or suspected are reported, investigated, reviewed and acted upon,
- Individuals and the council have a clear understanding of their responsibilities and accountabilities.

4 Definitions

The *General Data Protection Regulation* (GDPR) is an EU regulation which applies to all EU countries and will remain in force in the UK after the country leaves the European Union.

The *Data Protection Act 2018* is UK law which supplements GDPR and covers areas where countries have discretion under GDPR to set their own legal standards.

In this policy *personal information* means any information relating to an identifiable living person. This means they can be identified from information such as a name, an address, an identification number (e.g. your National Insurance number, NHS number or case reference number), location data etc.

"Special category information" previously referred to as 'sensitive data' is data regarding an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data and biometric data (fingerprints, eye scans etc.) for the purpose of uniquely identifying a person, data concerning health or data concerning a person's sex life or sexual orientation. There are extra safeguards for special category information to ensure no one is discriminated against when it comes to receiving a service.

A *Secure* state means that only authorised people or systems can access information.

The *Data Protection Officer* is the Council's Information Governance Manager, the Data Protection Officer a position required in law to ensure the council complies with data protection legislation and acts as a single point of contact for individuals who want to find out about their information. (See also section 23 of the DP policy)

Information Governance (IG) – Information Governance is the control of information, assessing its value, ensuring it is appropriately managed, accessible, accurate, processed lawfully, secure and disposed of when appropriate.

The *Senior Information Risk Officer* (SIRO) is the Assistant Director for Legal and Democratic Services who is accountable for protecting the council's information assets.

The *Caldicott Guardian* is a member of the Council's Adult Health & wellbeing Directorate. The Caldicott Guardian is responsible for protecting the confidentiality of people's health and social care information and making sure it is used properly.

The *Information Commissioner* is the independent regulator appointed by parliament to check compliance with data protection law.

Information Asset Owners (IAOs) are the person who has responsibility for and are held accountable for the management of Information Assets.

Most personal information processed by the council will fall within the security classification of *OFFICIAL*. There is no requirement to mark this type of data.

The council also handles special categories of data, information relating to vulnerable adults or children, and commercially sensitive information which requires higher levels of protection. This is classed as *OFFICIAL-SENSITIVE*. Further information can be found under section 14 references.

5 Data Protection

The council must comply with all current data protection legislation which provides the framework for compliance.

- Article 32 of the GDPR requires that personal information must be processed in a secure manner
- The Data Protection Act 2018 provides further requirements for using certain types of information

These requirements are detailed in the council's Data Protection Policy, other Information Governance policies and procedures, and ICT policies.

6 Technical Compliance

The council has a number of organisational and technical processes in place that provide a level of assurance to external compliance authorities, such that they continue to award the council their respective technical security certifications.

Currently these are:

Cyber Essentials Plus
PSN – Public Services Network (Government Secure network)
PCI DSS 3.2 (Credit card information)
Data Security and Protection Toolkit (NHS)
Local Public Service Data Handling Guidelines (Socitim)
Government Baseline Security Standard v1.0

Further information on ICT policies and procedures, including Technical Security Policy: ICT-policies

7 Classification of Information

The council follows the HM Government Security Classification (GSC) scheme. All council information is classed as OFFICIAL under this scheme but there is no requirement to routinely mark this classification of information.

Information which is personal or commercially or politically sensitive is classed as SENSITIVE. This is information which we would therefore handle more carefully. For example, if we were to send this type of information externally by email, we would only send it via an encrypted email link.

Information which is stored, processed or transferred within the Council's network is deemed **SECURE** and requires no further technical protection.
Other organisations that have appropriate security in place may also be deemed secure.

8 Information Security Procedures

8.1 Identity and Authentication Management

All users with access to our data will have been authenticated and provided with a unique ID.

Group / shared IDs: If a process or system requires the use of a shared ID where more than one person can access with shared password, it is good practice for there to be an alternate means to identify the user responsible for actions taken and this should be used wherever possible. Group / Shared ID's and access to them must be authorised by the relevant Head of Service.

Delegated access: If a system or process utilises delegated access, the identity of the delegator and delegate, as well as specific authority delegated should be clearly documented and authorised by the delegator.

8.2 Sending information by email

DMBC, DCST and SLHD all use the council's email system and therefore operate within our secure network. Some schools are also on our secure network and can be found in the Academy (secure) and Maintained Schools (secure) Email groups.

If an organisation is not within our network, email containing OFFICIAL SENSTIVE information can be sent directly from your organisational email account to public service network attached organisations (as of March 2019, this includes .gov, .nhs.net, .pnn).

However, when sending OFFICIAL SENSITIVE information to all other organisations or individuals it should be sent with [encrypt] in the subject line or in the body of the email.

8.2.1 Sending emails securely to Public Sector Organisations

Sending an email with OFFICIAL and OFFICIAL SENSITIVE information will be secure if sending from your @doncaster.gov.uk. @stlegerhomes.co.uk or @DCST.co.uk address to .pnn (police), .gov, .nhs.net (NHS).

8.2.2 Sending emails securely to other email addresses

To send a secure email to organisations or individuals who are not on the Public Services Network you need to use the encrypt facility. Further guidance on how to do this is available on the link . Secure Email

8.3 Transferring information off the Council secure network

If the files are over 25MB then alternative options exist for the secure movement of information. These include the use of secure data transfer systems; physical electronic media or registered post / courier. Further details on the intranet under ICT policies and procedures: ICT-policies

8.4 Clear desk procedure

Doncaster council operates a clear desk procedure. All information must be securely stored at the end of the working day and must not be accessible by anyone not authorised to access it. Further guidance is available on the intranet at:
Security Awareness

8.5 Locking screens

If you are leaving your desk ensure you lock your screen so that information on databases or the network cannot be accessed inappropriately. Press 'windows key+L' to lock your screen and logout at the end of the day. Further guidance is available on the intranet at:
Security Awareness

8.6 Handling paper documents

Paper documents containing sensitive information must only be seen by authorised individuals. Keep these documents secure by storing them in team lockers. When taking paper documents off-site ensure they are in your direct possession or out of

sight, ideally in a locked case. Only take the minimum necessary to complete your business purpose.

8.7 Malevolent Emails

Email is an essential business tool. However, it is equally useful for criminals to gain unauthorised access to council systems, information and passwords. Be especially vigilant for Emails not addressed to you specifically, containing links taking you to another website, or having attachments that you don't recognise. If you are suspicious of an email and / or actually click on a link it is essential you log this on iServe straightaway. It only takes a minute to report but ransomware could have trashed all your team's files within 10! Additional information and training is available on the learning zone and the intranet: Spam and Phishing

8.8 Passwords and multi factor authentication

In order to ensure that only authorised users are able to access or process information, systems are in place to prevent accidental or deliberate unauthorised access. For access to OFFICIAL SENSITIVE information, the council may employ multiple factors. Passwords are a single factor, and should be set so that they cannot be easily guessed or cracked.

Guidance on setting strong passwords can be found here: Information Security

8.9 Role based access controls

Access to information and systems will be based on access required for each individual role. Service areas will provide justification for the access requirements and management will authorise

9 Human Resources

You should only have access to the information you require to undertake your current role and responsibilities. Managers must ensure that this happens and that all staff are adequately trained on Information Security and that they complete any mandatory training.

For further details refer to staff recruitment and management policies: Human Resources Code of Conduct

All staff must have adequate training, training must be monitored and understanding must be tested. Managers should monitor access to systems and data if mandatory training has not been completed.

All DMBC employee contracts make it clear that a breach of policy can lead to disciplinary action. Where staff have access to sensitive data additional safeguards may be implemented to provide a higher level of security, e.g. DBS checks for staff working directly with vulnerable adults or children and / or Baseline Personal Security Standard checks for staff with elevated privileges.

10 Protection of Information

Where sensitive information is processed, stored and transmitted, additional safeguards must be in place to mitigate the higher impacts associated with the unauthorised use of, or loss of that information.

10.1 Protection of stored or saved information

Electronic information must only be stored on the council network (S: or U: drives) or applications published on the council software catalogue. In certain circumstances information may be stored suitably encrypted on media or in the cloud.

10.2 Protection of information in transit

Sensitive information must only be transmitted by the following **SECURE** methods:

- Emails between Doncaster Council, St Leger Homes Doncaster, Doncaster Children Services Trust and schools who use the council email system
- Over other encrypted systems or services
- Using encrypted physical medium and sent via a tracked service
- Shared via a cloud service that has been ratified as meeting the National Cyber Security Centre standard (as advised by ICT), encrypted where appropriate
- Microsoft Teams will be available later in 2020

Please see Secure Email

11 Retention and Deletion of Information

Data should be collected in a lawful manner. Information should be kept no longer than necessary in line with statutory or best practice document retention periods.

Once the information has reached the end of its retention period it should be disposed of in accordance with the council retention guide.

Guidance: Document retention privacy Data Protection Policy

12 Incidents

When information is accessed or disclosed inappropriately or any equipment or information is lost, the incident must be reported to information.governance@doncaster.gov.uk logged with ICT on iserve and if appropriate, a police crime number obtained.

It is imperative the incident it reported as soon as possible to protect the integrity of the councils data and systems.

Information Governance and ICT teams will investigate and take appropriate mitigation measures.

13 Audit

Compliance with this policy is monitored by the Senior Information Risk Officer (SIRO) and the SIRO Board.

14 References

PSN connection requirements and compliance
https://www.gov.uk/guidance/securing-government-email
Government Security Classification Scheme: Pages 17, 18, 20, 24(d) Government Security Classifications

Payment Card Industry Data Security Standard

May-2018_Government-Security-Classifications-2.pdf

May-2018_Working-with-OFFICIAL.PDF

15 Associated Documentation

Data Protection policy

Internet and Acceptable Use policy

Records Management policy

Social Media policy

Data Protection – Individuals' Rights procedure

IG Security Incident procedure

Technical security guidance: technical-security

- Transmitting information securely: transmitting information v4.2.pdf
- How to manage passwords
- How to send passwords securely