NORTHAMPTON
BOROUGH COUNCIL

Corporate General Data Protection Policy

Impact Assessment

The Council strives to ensure equality of opportunity for all, both as a major employer and as a service provider.

This policy has been equality impact assessed to ensure fairness and consistency for all no matter what race, gender, political or religious beliefs a person may be or have or whether able-bodied or not. In particular this policy upholds the rights of individuals including a number of the basic human rights set out in UK and European legislation including the European Convention on Human Rights 1953 (ECHR) and the General Data Protection Regulation 2018 (GDPR).

'The right of respect for private and family life, home and correspondence' (Article 8 of the UK's own Human Rights Act 1998) is a fundamental cornerstone of, and a founding principle of, data protection and the right to expect all Personal data to be handled securely and confidentially.

Document metadata

Document Name	General Data Protection Policy
Type of Document	Corporate Policy
Document File Name	POL-IG-GDPR RMP-09.1
Version Number	V1 July 2018
Protective Marking	Unrestricted - Public
Approved level required	Cabinet approval
Date approved	Cabinet agenda item 18th July 2018
Internal / external publication	External publication on website
Publication date	Post Cabinet approval
Next Review	April 2019 (post Brexit)
Reviewers	Data Protection Officer & Monitoring Officer

Document ownership

Author (Name)	David Taylor
Author (Post Holder Title)	Data Protection Officer
Contact Details	01604 83 8536 djtaylor@northampton.gov.uk
Department	Corporate Governance and Risk
Directorate	Borough Secretary

Version Control

Change History	Date	Comments	Amender
version 0.7	18-7-2018	Cabinet Report	Approved
Version 1	20-7-2018	Final version	Published

Contents

1st Golden DP Rule

Treat others Data as though it was your own

When you think about Data Protection remember that we are all data subjects. Think about how appropriately, sensitively and securely you would expect your personal details to be handled and then manage the personal details of others in the same way and in accordance to the law.

GDPR1

Forewords

Jonathan Nunn
Leader of the Council

As more of our information is held on computers it is reassuring for our customers to know that data protection legislation is in place to protect the personal data we use every day.

Data protection legislation is our customers' assurance that the personal information we ask for from them to provide services is collected lawfully, used appropriately, held securely and destroyed responsibly. It also gives customers the right to access the personal data held and to amend it if it's wrong or delete it if possible.

This policy supports the data protection legislation and helps us all to keep the requirements for handling personal data first and foremost in our thoughts as we work.

The residents of Northampton expect their Council to manage the personal data they give us as though it were our own. This is the standard that we strive to achieve on a daily basis.

George Candler
Chief Executive

We all share our personal data with organisations on a daily basis.

When our customers share their personal data with us they have a right to know that the contact details, the copies of documents, the bank details and all other personal information that they provide to us is not governed merely by terms and conditions set by the Council but by laws that give them the right to control how, where and with whom the data is processed.

Life is too short to have to worry about how that data is managed so the new laws strengthened citizens' rights to allow people to take back control of their personal data.

This policy supports those personal data rights by providing a set of rules here by which everyone who works for, with or on behalf of the Council will abide by.

David Taylor
Data Protection Officer

Putting Data Protection first

Information is one of any organisation's 4 main assets. The others being People, Property and Finance.

At Northampton Borough Council we understand this and put residents and customers personal data as our number 1 information asset.

Though our words in this policy and our actions implementing it we strive to demonstrate our commitment to managing your personal data responsibly and appropriately. Our aim is to always put the secure management of the personal data you entrust to us first.

We acknowledge the trust residents and customers place in us as custodians of their personal data. As Data Protection Officer I pledge to do all I can to ensure the Council manages your personal data in an appropriate, secure and complaint way.

To this end I have developed the 'Data Protection 1st' motto to keep the proper management of your personal data at the forefront of everything we do and say.

The Council will also support and use the Information Commissions 'TH!NK PRIVACY' campaign to keep data protection on everyone's minds and follow Personal Information Promise.

Finally the ICO's 'Your Data Matters' promotion campaign reminds us all that we have a responsibility to ensure our own data is held and processed appropriately.

For example: Use your apps personal settings buttons to ensure only the data you want public is shared.

Please let me know where we get things right or wrong. Both are equally important in helping me ensure the Council continues to manage your **Personal Data First**.

You can contact the Data Protection Officer:
By phone: 01604 83 8539
By email: djtaylor@northamtpon.gov.uk or dataprotection@northampton.gov.uk

To make a subject access request please email requests@northampton.gov.uk

Introduction

Northampton Borough Council ("the Council") is fully committed to compliance with the requirements of the **General Data Protection Regulation 2016** (**GDPR**) and the **Data Protection Act 2018** ("**the DP Act**"), which came into force on the 25th May 2018.

Obligations and responsibilities under both laws are not optional; **they are mandatory**. There can be harsh penalties (up to 4% of gross international turnover or the Sterling equivalent of €20,000,000) imposed for non-compliance including breaches, loss and misuse. The Council will follow procedures that ensure all staff, elected Members, contractors, agents, consultants, partners or any other person or organisation working for the Council who have access to any personal data held by or on behalf of the Council are fully aware of, and abide by, their legal duties and responsibilities under both laws.

All individuals permitted to access personal data in line with their work duties must agree to comply with this policy and agree to undertake any relevant training that may be appropriate to the job, position and work being undertaken. Some departments may also require employees to sign a further undertaking relating to the systems and/or data they will use or have access to.

As well as the Council, any individual who knowingly or recklessly processes data without appropriate consent or proper authorisation, for purposes other than those for which the data is intended, or is deliberately acting outside of their recognized responsibilities may be subject to the Council's disciplinary procedures. This may include dismissal where appropriate, and possible legal action liable to prosecution and, since 1st April 2010, possible criminal conviction under the Criminal Justice and Immigration Act 2008.

Compliance

In order to operate efficiently, the Council has to collect and process personal data about people with whom it works with or for. This may include members of the public, current, past and prospective staff, clients, customers, contractors, partners and suppliers. In addition, the Council may be required to collect and use personal data in order to comply with its statutory obligations.

This personal data must be handled and dealt with in accordance with the GDPR and this policy. There are safeguards within the GDPR and DP Act to ensure personal data is collected, recorded and used with due regard to a natural persons rights, whether it is on paper, computer records or recorded by any other means.

The obligations outlined in this policy apply to everyone listed above who has access to, holds copies of or processes personal data. This includes those who work at / from home or have remote or flexible patterns of working.

Directors, Service Heads and Managers have immediate responsibility and accountability for data protection matters in their own areas of work including:

- Development, implementation and review of departmental data protection procedures that support this policy.
- Ensuring compliance with Information Governance policies and standards established by the Council to support provision of service.

- Ensuring that new information systems, or updates to existing systems, in their work area are designed and tested against the Data Protection Impact Assessment (DPIA) toolkit to comply with this policy.
- Notifying the Data Protection Officer (DPO) of the development of any new/updates to systems in their area of work that process personal data.
- Reporting any data breach immediately to the DPO

Staff at all levels (including consultants, contractors, temporary/agency workers, part time and full time staff) will have immediate responsibility to;

- Work in a manner which will ensure the security and good management of all personal data within the work environment.
- Proactively alert the DPO to suspected poor data protection practices and data processing concerns.
- Report any data breach or suspected data breach immediately to the DPO. Whenever possible this should be before line management and as soon as known.

Elected Members are data controllers in their own right. They have similar responsibilities to that of a DPO as set out in Part 12 of this policy. These include:

- Maintaining with the Council's DPO a valid ICO data processing registration.
- Maintaining a comprehensive privacy statement.
- Ensuring all personal data are processed in line with this policy and good practice.
- Recording all processing activities using case management software provided.
- Reporting breaches and data loss to the DPO immediately.

Elected Members also process personal data in relation to committee work (such as licensing applicant details and residents planning application details). This processing is carried out under the Council's data protection registration.

Elected Members may also process constituents ward data for election purposes. This will be under their party's national or local data protection registration.

The General Data Protection Principles

The GDPR stipulates that anyone processing personal data must comply with **SIX Data Principles** of good practice. These Principles summarised below are fully defined in GDPR Article 5 and are legally enforceable. They must be followed by all data processors at all times.

The Principles require that personal data are processed;

a) **Lawfully, fairly and transparently.**
b) **Purpose limitation** – ('Collected for specified, explicit and legitimate purposes').
c) **Data minimisation** - ('Adequate, relevant and necessary').
d) **Data accuracy** - ('Accurate and up-to-date').
e) **Storage limitation** - ('Permit identification for no longer than necessary').
f) **Integrity and confidentiality** - ('Appropriate security & protection against unauthorised or unlawful processing and against accidental loss, destruction or damage').

Data Protection Promise – going further than the letter of the law

In addition to meeting its legal obligations to safeguard personal data, the Council endeavours to go further than the letter of the law. To demonstrate this commitment to data protection the Council's Management Board have agreed to work in a way that wherever possible and practical supports the Information Commissioners' Personal Information Promise**.**

Accordingly we promise that we will:

1. Value the personal information entrusted to us and make sure we respect that trust;
2. Go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
3. Consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
4. Be open with individuals about how we use their information and who we give it to;
5. Make it easy for individuals to access and correct their personal information;
6. Keep Personal information to the minimum necessary and delete it when we no longer need it;
7. Have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
8. Provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;
9. Put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and
10. Regularly check that we are living up to our promises and report on how we are doing.

Personal data & Special categories of Personal data

The GDPR provides conditions for the collection and processing of all personal data. It also makes a distinction between personal data and "sensitive" personal data now called **special categories of personal data** in **GDPR Article 9**.

Personal data is defined in Article 4 section 1;

*'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person**;***

Special categories of personal data are defined in **GDPR Article 9 1.** as personal data consisting of information as to:

- racial or ethnic origin;
- political opinion;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data;
- physical or mental health or condition;

- sexual life or sexual orientation;

How special categories of personal data can be processed and what conditions must be met before such processing are set out in **Article 9 Paragraph 2 a. to j.**

Although there are clear distinctions between personal data and special categories of personal data, for the purposes of this policy the term 'personal data' refers equally to 'special categories of personal data' unless otherwise stated because additional controls are necessary.

Policy Scope

The General Data Protection Regulation (GDPR), the Data Protection Act 2018 (the DP Act), the 6 Data Principles and the 10 Personal Information Promises form the framework and reference points for the following policy statements. Complying with the policy statements and following the Councils DP Golden Rules demonstrates our commitment to managing all personal data to the very highest standards at all times.

This policy has been approved as corporate policy at Cabinet on 18th July 2018

Compliance with all aspects of this policy is mandatory

The policy is divided into parts for ease of reference. It follows the natural process of data management using the acronym CHAPSSTEAD

1. **Collecting**
2. **Holding**
3. **Accessing**
4. **Processing**
5. **Subjects Rights**
6. **Sharing**
7. **Transmitting and/or Transporting**
8. **Encrypting**
9. **Assessing and retaining**
10. **Destroying and Decommissioning**

Guidance notes supporting each part and giving detailed compliance advice are available to assist staff and departments comply with their duties and obligations.

This policy is part of a series of interlinked policies relating to information governance, records management, information technologies, access to information requests, risk and security.

GDPR Policy Statements

Part 1

Collecting personal data

2nd Golden DP Rule

Only collect the absolute minimum amount of personal data required to provide the services you deliver.

GDPR2

1 Privacy notice

GDPR Article 13.1 requires the Council to ensure individuals (data subjects) are told:

a. The name and contact details of the data controller (and details of third party processors and controllers if applicable).
b. The name and contact details of the Data Protection Officer;
c. The purpose and legal basis for data processing that the data controller and/or the third party will rely on to make the processing lawful.
d. The legitimate interests in respect of data processing by the data controller and third parties;
e. The people or organisations that will process the personal data;
f. Whether personal data will be transferred or held in another country (and specifically if held outside of the EEA).

The Council will do this in two ways.

Firstly, the Council will maintain its registration with the Information Commissioners Office to hold and process personal data. The Register of Fee Payers is publicly available to view on the ICO website at https://ico.org.uk/esdwebpages/search The Council's registration number is Z5256045. In addition the Council will only ever use third party data processors who are similarly registered to hold and process personal data.

Secondly, the Council will publish and make available the following:

Corporate Privacy Statement (CPS)
The Council's Data Protection Officer will ensure the Council publishes and keeps up-to-date a Corporate Privacy Statement in compliance with GDPR Article 13.1.

Departmental Privacy Notices (DPN)
Where departments process personal data, either because of the service they provide or the legislation they work under, they will publish further information about the specific circumstances and context in which the personal data are processed. [Recital 60 & A13.2]

Privacy Notices will;

- be written in the same font, size and layout as the rest of the publication,
- be written in plain English,
- state why the personal data is required and how it will be used,
- identify who can access personal data and who it may be shared with,
- say how long personal data will be retained and how it will be destroyed.

GDPR Guidance Note 1 - Details the type of information required in a Departmental Privacy Notice in the form of a template. It also provides advice on drafting privacy notices and how best to make them public and accessible.

3rd Golden DP Rule

A Privacy Statement or Notice, (previously Fair Processing Notices), must be made available when asking for or collecting any personal data

GDPR3

2 Lawful processing

Personal data can only be collected if there is a lawful reason to do so. The 6 reasons are set out in Article 6 of the GDPR and are;

(a) the data subject has **given consent** to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a **legal obligation** to which the controller is subject;
(d) processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
(e) processing is necessary for the **performance of a task** carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

All personal data collected by the Council will meet at least one of these lawful reasons and will be identified within the Councils ICO registration and in each DPN.

A Data Privacy Impact Assessment (DPIA) must be completed before any change to existing or new physical or electronic personal data collecting, holding and/or processing begins, *(See part 9, section 28 and GDPR Guidance Note 9).*

3 Consent

Where there is no legal requirement, legitimate or vital interest, contract or public interest lawful reason to collect, hold and process personal data then the consent of the individual must be obtained at the time the data is collected.

This policy cannot identify or predict all such instances the following examples should assist you determine if consent is required;

- Mailshot database, e.g. to update members of the public on events.
- Membership of a group, e.g. contact details for residents associations.
- Forum, e.g. Landlords Forum, Enterprise Zone or BID.

When seeking consent from individuals you must make it very clear;

- Why you are asking for the data.
- What data you require, usually restricted to names and personal contact details.
- How the data will be held.
- Who will have access to the data.
- How long the personal data will be retained and how you will destroy or delete it.
- A record must be kept of the consent.
- Without exception new consent must be obtained if you intend to use the data for any other purpose or share the data with a new third party or organisation.
- The Council requires consent to be refreshed at least every 2 years.

You should seek the advice of the Data Protection Officer if you identify consent as your only form of lawful processing.

Part 2

Holding personal data

4 Holding data

Personal data will only be held as long as is necessary in line with statutory, industry and best practice retention guidelines (Guidance Note 9).

Personal data will be:

- held securely and only accessed by authorised personnel,
- held in password protected folders and files when restricted access is necessary,
- transported securely or transmitted using secure encryption,
- securely destroyed or deleted when no longer required.

A record of all personal data held and the measures used to protect that data will be maintained by the Council's Data Protection Officer.

5 Information security

The Council will ensure appropriate physical and electronic safeguards are in place to protect all personal data held and in its care.

The Council undertakes to have in place a level of data security appropriate to the nature of the data and the harm that might result from a breach of security. Where necessary additional provisions, safeguards and controls will be employed to ensure special categories of personal data can only be accessed by authorised personnel.

This will include, but is not limited to:

- Building entry security passes,
- Password protection on all computers, Laptops and tablets (Part 3, section 9),
- Multi layered and up-to-date antivirus software,
- Encryption of all removable drives and storage media holding personal data (Part 8, section 26),
- Use of secure file transfer protocols sites, secure email transmission or door-to-door courier services when personal data is in transit,
- Physical file control measures both on and off site.

6 Electronic files

Where files are not held in Electronic Document Record Management Systems (EDRMS) or Electronic Case Management Systems (ECMS) then all electronic files must be held on the corporate drive structure. This ensures files and folders are backed up and protected behind the firewalls and that staff that may need access to files you have within the same department can access them. No electronic files whatsoever should be stored on local C Drives. This creates an unacceptable risk of data loss and, in respect of personal data, a possible data breach.

The Corporate drive structure is as follows.

'I' Drive – This drive is for employees personal files relating to you such as timesheets, performance and appraisal, voluntary roles. IT IS NOT A CORPORATE WORK STORAGE AREA. Work data you store here cannot be accessed in your absence.

'J' Drive – This is the joint department shared drive. Almost all of your day-to-day work should be stored here. It provides colleagues with access to information you have created as part of your role and ensures departmental continuity when staff are absent. Personal data such as spreadsheets containing consultation contact data should be password protected to ensure it is not used for a new purpose. ICT can create restricted access folders on this drive, for example for a manager to hold local employee personnel files.

'N' Drive – This is the corporate shared drive, not a departmental drive. The only files that should be held on this drive are:

- Corporate projects.
- Inter department files when they relate to shared work. ICT should be asked to create the folder and set the permissions to only those staff that need access.
- All staff file sharing. E.g. Sometimes it is easier to place a file on the shared drive and link to it in an email, especially when the file is large (over 10mb) or when a file is over 1mb and being emailed to more than 10 staff.
- Corporate messages and work streams such as 'Local Government Review' where the intranet can link to documents that everyone can access.

It should also be noted that email is a communication tool and not an electronic document storage solution. Files received via email that need to be retained should be stored either in their case file or in the relevant drive.

7 Diary notes and free text

4th Golden DP Rule

Only write in free text note pads what you'd want recorded about you.

GDPR4

Free text covers, for the purposes of this policy, all notes placed on files relating to an individual or property that would be subject to disclosure as part of a subject access request. This includes:

- Hand written file notes.
- Electronic note pad and file notes (such as in case management systems).
- Meeting notes relating to the data subject.
- Recordings and transcripts.
- All correspondence including letter, emails and memoranda.
- Phone messages (such as on note pads).

Care must be taken to only record factual information about individuals. Do not record opinions or anything else that cannot be substantiated. All free text file notes must be accurate, succinct and above all verifiable.

Remember data subjects have the right to request copies of the personal data the Council holds about them, including notes written onto their case file. What you write is likely to be disclosed if requested.

Table 1 - Free text do's and don'ts

Do's	Don't
Keep text brief. No essays.	Do not use full names except for the data subject's, use initials.
Record facts. Only write what can be substantiated.	Do not include personal thoughts.
Link to evidence where necessary.	Do not record comments that in hindsight you would retract / can't substantiate.

8 Personal data audit

All personal data being collected, held and processed will be subject to periodic audit against the agreed data flow process maps by the DPO to ensure good data practices are being followed.

It is essential that any changes to the way personal data is collected, held, accessed, processed, stored, shared, transmitted or destroyed is documented. This is done using the DPIA (*see section 12 and GDPR Guidance Note 9*)

GDPR Guidance Note 2 – Provides further guidance on how and where to hold personal data. It also includes the Council's Version Control Policy.

Part 3

Accessing personal data

9 Password protection (access controls)

The Council has a number of layers of password protection. Staff and members cannot log on to a PC without first inputting a secure password (with additional layers of password protection for mobile devices). The ICT Policy stipulates and fully defines passwords and their use. The points below summarise those security controls.

- Log in passwords change every 55 days and cannot be reused.
- Passwords must contain a minimum of 9 characters and include lower and upper case, at least 2 numbers and preferably at least one special character.
- Log in passwords must not be shared or written down. They provide the core security to ensure only those accessing the Council IT servers are authorised.
- Set a network password that conforms to three out of the four following rules

    1. Contains upper characters (A to Z).
    2. Contains lowercase characters (a to z).
    3. Contains numerics (0 to 9).
    4. Contains symbols (# £ ! & $ % £ etc.).

- Change your password immediately if you suspect that its confidentiality has been compromised.
- Other systems containing personal data should also be password protected at the user sign-in screen.
- Spreadsheets and other documents, files or folders containing lists of more than one personal data record should be 'open protected' or held in a restricted access folder, cabinet or server area.
- Never give your password to other members of staff so that they may log in as you in your absence.

GDPR Policy Statements

10 Confidentiality

Personal data is often provided to the Council 'in confidence'. This confidential information is arguably the most valuable information business asset the Council holds.

Staff automatically have duties to ensure that confidential data (and commercially sensitive information) is held securely and not knowingly or recklessly misused. Staff should only access systems and records containing confidential information that are relevant to their work /duties.

Where appropriate, signed declarations of confidentiality should be employed and records kept of signing to further emphasise the importance of the reason why access controls are so important.

5th Golden DP Rule

It is good practice to treat all personal data as provided 'in confidence'.

GDPR5

- Those who use the Council's computer equipment will only have access to the data that is both necessary for the work they are doing and held for the purpose of carrying out that work.
- Do not try to access personal data you should not have access to.
- If you find others accessing or misusing personal data it is your duty to report the issue, in confidence, to the Data Protection Officer.
- In respect of manual / physical files (paper records) - access must be restricted solely to relevant staff and stored in secure locations (e.g. lockable cabinets), to prevent unauthorized access.
- Personal data held electronically must only be accessed in compliance with this and the ICT policy.
- Preventing abuse and discrimination. The Council processes special categories of personal data in respect of staff and residents. The Council will have regard to its various equality and diversity policies to ensure that if instances of abuse or discrimination occur, appropriate action is taken.

NB.

Additional safeguards must be adopted when special categories of personal data are involved and those safeguards documented and shared with relevant staff where appropriate.

11 Clear desk

The purpose of a Clear Desk and Office Environment Policy is to ensure that all paper and electronic records containing person identifiable information, or any other confidential/sensitive information (including corporate or commercially sensitive information) are suitably secured when not in use and are not left visible on an unattended desk or computer desktop.

Clear desk is extended to anywhere in a work place environment where personal, confidential and commercially sensitive information can be held and communicated both inside a building, in transit or on site. This includes: at the Council offices, on the move (either walking or in a vehicle), in court, at a customer's property, in a meeting or any other place where data is taken, communicated or held.

Clear desk includes any electronic device or storage media holding or providing access to personal data, confidential data and or commercial data.

The full Clear Desk and Secure Office Environment Policy is contained within GDPR Guidance Note 3.

In summary the personal data measures in the clear desk policy are:

- Computer access must be locked when you are not at your workstation. The simplest way to do this is by holding down the windows key and L at the same time. Your screensaver should also be set to auto lock after a maximum of 15 minutes inactivity with a password required to unlock.

- Computers must be locked or preferably shut down when leaving the office.

- Clear your immediate desk space of all personal data when you are away from your workstation, particularly at lunch or at a meeting.

- Desks must be cleared at the end of each working day of all confidential, commercial or person identifiable information. Personal data must be locked securely in desks, filing cupboards or designated secure rooms at all times, other than when being used by staff.

- Personal data and confidential or commercial information must be securely disposed of in accordance with part 10 of this policy.

- Don't forget your own personal data and personal items (such as keys, handbags, wallets, phones, etc). It is your responsibility as owner to ensure all personal items and documents are safe and secure.

- Mobile network devices (such as laptops, tablets and iPads) and data storage devices must be encrypted and kept locked away when not in use.

- Health & Safety – desks and other work spaces must be sufficiently tidy at the end of each working day to permit the authority's cleaning staff to perform their duties.

GDPR Policy Statements

Part 4

Processing personal data

What is processing?

Article 4 (2) defines processing as:
'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;'

It covers personal data held:

- electronically (e.g. digital images (static or moving), audio and anything written in all formats) and/or;
- physically (e.g. person or property file).

It is difficult to envisage any operation performed on personal data that does not amount to processing. This includes just storing the personal data on a database or in paper form for future use or reference.

All actions performed on personal data are covered by the Regulations and must be compliant with the GDPR and this corporate policy.

Examples of the Council processing against all of the above definitions are:

- **Collection –** Asking a resident for details to progress their enquiry.
- **Recording –** Keeping a record of interactions with a resident.
- **Organization –** Storing information about a resident in a file relating to them.
- **Structuring -** Organizing personal data into an order such as by issue.
- **Storage –** Keeping personal data in an email folders or case management system.
- **Adaptation or alteration –** Updating a residents records e.g. their preference.
- **Retrieval -** Recovering the information to contact them or work on their case.
- **Consultation –** Keeping a record of a residents' response to a survey.
- **Use –** Processing personal data about a resident for any purpose.
- **Disclosure by transmission, dissemination or otherwise making available.**
- **Alignment or combination -** Merging two or more records about a resident.
- **Restriction –** Password protecting a data about a resident.
- **Erasure or Destruction –** Deleting a personal data file from a computer.

Where a third party processes personal data on the Council's behalf, the third party will be required to act in a manner which ensures compliance with the Act and this policy and have adequate safeguards in place to protect the personal data. To this end the Council will only allow personal data to be processed by 3rd parties registered to hold and process personal data with the ICO and will, before any personal data is provided to the third party processor, put in place a formal and signed Data Processing Agreement.

GDPR Policy Statements

12 Processing (using) data

In line with the GDPR Article 5 Principle (a), all information will be ***'processed lawfully, fairly and in a transparent manner in relation to the data subject'.***

Data must be processed:

- Only for the purpose it was collected for,
- Lawfully and in line with the privacy notice,
- By authorised and trained personnel,
- Using secure auditable processes,
- Respecting the individuals' rights.

There are a number of ways that processing can be lawful (see part 1, section 2). Consent is one method, but it is important to know that consent is not always required and the Council can lawfully process personal data as long as one of the conditions in Article 6 are met. For example, the Council would be unlikely to collect Council Tax arrears if residents could withdraw their consent for processing their data.

You can find out more about the conditions for processing on the ICO website.

6th Golden DP Rule

Without exception, personal data must not be processed for any additional purposes without notifying the individual and, if required, obtaining their consent prior to the commencement of new or changed processing.

GDPR6

13 Protective markings

The Council does not currently have an approved Protective Marking Scheme however it is committed to introducing a scheme by 31st March 2020. The Scheme will be based on the Government Security Classification – May 2018 and other local authority Schemes.

In the interim period all employees and members are encouraged to adopt the following:

Interim PROTECTIVE MARKING SCHEME

The Council holds a significant amount of information, some of this information is of a very sensitive nature. The Council also works very closely with other public sector partners who also hold very sensitive information. It is important that at any time the level of sensitivity of a document can be easily and accurately understood by those handling it. This is achieved by the use of protective markings and, in the case of this interim scheme, associated descriptors.

GDPR Policy Statements

All documents must be considered as to whether they should be protectively marked, in accordance with the sensitivity of their content and this interim scheme. Protective markings enable a policy to be set around a documents' use and its allowable levels of distribution in all formats. This policy sets out the protective marking to be used at the Council and encouraged with its partners. The protective marking of a document provides people with information on the following aspects of the document:

a) The correct level of protection the document should be given.
b) The procedures to be followed regarding the production, dispatch, receipt, handling and destruction of the document.
c) The severity or impact of the loss or compromise of the document.

DEFINITIONS

CONFIDENTIAL

This is information that carries the highest level of protection that the Council is likely to hold. Information is only 'confidential' if for example it includes information that is likely to impede the investigation of a serious criminal offence. A serious criminal offence is murder, rape or manslaughter.

Please note, this marking has a different meaning to the legal definition of confidential and therefore this Scheme distinguishes the two means by referring to the latter as "Confidential in law".

RESTRICTED

This is information where the release would, or would be likely to cause **significant** harm or prejudice to:

I. an individual if it contains sensitive personal data,
II. the Councils, or a third parties, commercial interests,
III. the investigation or prosecution of a crime, or the apprehension of an offender,
IV. the effective conduct of public affairs.

Please note that the level of marking may depend on the potential consequences of the release of the information. If any harm or prejudice has the potential to be suffered under the categories listed, then a marking should be applied. If the harm or prejudice is significant then the level should be 'Restricted'. Therefore the term significant is used to judge if the information should be 'Restricted' or 'Protect' in a number of examples.

Significant harm or prejudice means that it would be likely to cause substantial distress or damage. The information would be of both a sensitive nature and be likely to impact heavily on the privacy of a person, an investigation or the commercial interests of a business or company.

Information that would cause only trivial harm would not require a restricted protective marking.

PROTECT

This is information that would, or would be likely to cause damage or prejudice to:

I. An individual, if it contains Special categories of personal data or other confidential information that may be detrimental to an individuals' privacy.
II. The Councils' or a third parties commercial interests.
III. The investigation or prosecution of a crime, or the apprehension of an offender
IV. The effective conduct of public affairs.
V. It would breach the proper undertaking to maintain a duty of confidence. This is not simply a document marked confidential. The information itself must also be confidential in nature.
VI. Breach a statutory restriction on disclosure.

Examples include: documents containing a large number of names and/or addresses; contracts; staff medical reports; independent living file notes.

INTERNAL USE ONLY

This is all other information not falling under any of the categories above. There are no requirements to mark other documents. However, to assist with operational efficiency documents that would not routinely be disclosed and are primarily for the use of staff only could bear a mark "**Internal Use Only**".

UNMARKED / PUBLIC

Documents unmarked or marked '**Public**' are unrestricted and require no security consideration. They can be freely shared and do not need to be securely destroyed. Information that is published, either on the Council's website, or in paper form, can remain unmarked. Examples include public facing policies, publications, public reports and web documents.

DESCRIPTORS

In order to provide an indication of why documents are marked in the manner that they have been, consideration should be given to marking the documents with a descriptor in addition to the protective marking.

A descriptor is an indication of the reason for the marking. This descriptor should be recorded next to the protective marking (for example **PROTECT - PERSONAL**).

The descriptors that can be used are:

PERSONAL – information that contains personal data of a natural person.

COMMERCIAL – information the release of which would, or would be likely to, prejudice the commercial interests of the Council or a third party.

POLICY/STRATEGY – information that forms part of a Council policy or strategy or procedure that is normally associated with internal use only.

INVESTIGATION – information that may prejudice a criminal investigation, prosecution or apprehension of an offender.

IN CONFIDENCE – information received under an air of confidence, the disclosure of which would be an actionable breach in law.

Examples
PROTECT – PERSONAL - likely to contain information that if it was comprised would cause distress to an individual.

RESTRICTED – IN CONFIDENCE - may be a whistleblowing statement where disclosure could damage the investigation but also cause distress and possible repercussion to the whistleblower (this would complement the fact that the whistleblower has additional legislative protection rights).

PROTECT – COMMERCIAL – document relates to the tender bid process and requires protection until the contract is awarded.

14 Disclosing data

Personal data must only be disclosed either:

a) following successful completion of approved data subject question checks* to confirm identity, or
b) to an individual in response to a Subject Access Request (SAR) (see part 5, section16), or
c) to other organisations and persons who are pre-defined as notified recipients within the Council's Data Protection Notification and with whom the Council has an active Data Sharing Agreement.

If you receive a request for personal data (SAR) you should in the first instance seek advice from the Data Protection Officer who will record and centrally manage under the request process detailed in section 16 and GDPR - Guidance Note 5A.

* When answering a call relating to an account or interaction with Council (such as a housing benefit claim or licence application) it will be necessary to check the identity of the caller before discussing the account with them. There are set questions that should be asked to ensure the caller is the account holder. You should record on the notepad that the DPA check has been carried out. If you are unsure please escalate the call to a more senior member of staff.

7th Golden DP Rule

Never disclose personal data without asking security questions to check a caller's identity before discussing personal account details. If unsure seek authorisation otherwise it may be a breach of data protection.

GDPR7

15 Data processing records

The Council's Data Protection Officer will maintain records of personal data processing as required by GDPR Article 30 and 32. These will include:

- A central copy of each department's personal data audit.
- A central copy of the departmental Personal data flow maps.
- A copy of all Departmental Privacy Notices.
- A central log of all Data Sharing and Processing Agreements.
- A log of all computer systems that hold and process personal data.
- A central log of all pseudonymised personal datasets.
- A record of all staff authorised to write encrypted files to mobile media devices.
- A corporate log of all hard drives over 250gb.

GDPR Guidance Note 4 - provides details and templates for the data processing records

Part 5

Data subject rights

The *GDPR* provides the following *rights* for individuals, most of which follow on from a subject access request. The *rights* below are hyperlinked to more detailed information about each one on the ICO website.

A12 - The *right* to be informed in respect of any of the rights Articles below;

- A13 - The *right* to be informed [Corporate Privacy Statement (CPS) and Departmental Privacy Notice (DPN)];
- A13 - The *right* to be informed of the use of 3rd party data;
- A15 - The *right* of access (to get copies of your data) [Subject Access Request];
- A16 - The *right* to rectification;
- A17 - The *right* to erasure (deleted) [be forgotten];
- A18 - The *right* to restrict processing (limit use) [manual intervention];
- A19 - The *right* to be notified [of change or erasure];
- A20 - The *right* to data portability [in a universally readable format, usually .pdf];
- A21 - The *right* to object;
- *A22* - The *right* to *be told* of automated decision making and profiling;
- A34 - The *right* to be informed in respect of a data breach.

Any request to take action against one or more of these rights must be passed immediately to the Data Protection Officer.

16 Data Subject Access Request (SAR)

Article 15 of the GDPR provide every citizen with the right to request and be provided with copies of the personal data held by the Council about them.

All SAR's are recorded and managed centrally by the Information Governance team and the Data Protection Officer. You should forward any request to a member of the team on the day you receive it. Please note that SAR's can now be made orally such as over the phone or counter as well as in writing. In particular, staff should look for requests hidden in other correspondence such as an emailed complaint.

The Council does has a form (DSAR1) to assist individuals with the request process including a section on the suggested identity documents an individual can provide to prove they are entitled to receive copies of the personal data. Though it is not compulsory for individuals to submit their request on the form it is helpful to ensure all the information required to begin the request is provided.

Though making a request is free, the Council may consider charging for manifestly unreasonable, multiple or frequent requests. In addition, should the personal data be required in a format other than electronic copies on an optical disc (CD ROM, DVD etc.) the Council reserves the right to charge a fee equivalent to the time and resources it takes to respond in that format. (E.g. a charge of 12p per A4 copy will be made to cover the paper, printing and time to print, plus a postage charge at actual secure delivery cost plus £1.50 packaging).

GDPR Guidance Note 5A fully defines the Subject Access Request process including a copy of the request form DSAR1.2.

17 Exemptions to the non-disclosure provisions

At certain times it may be lawful that personal data held by the Council can be disclosed under one of the exemptions to non-disclosure within the Data Protection Act 2018. This section is in two parts. **Part A** relates to information that can be disclosed without the individual's consent, (see ***GDPR Guidance Note 5B – Non-disclosure Exemptions***) and **Part B** relates to information that may be exempt from disclosure following a subject access request.

Part A

There are several prescribed exemptions to the non-disclosure provisions within the DP Act 2018. The two main non-disclosure exemptions are copies below.

Schedule 2, Part 1, Section 2,

(1) *The listed GDPR provisions and Article 34(1) and (4) of the GDPR (communication of personal data breach to the data subject) do not apply to personal data processed for any of the following purposes -*

(a) the prevention or detection of crime,
(b) the apprehension or prosecution of offenders, or

(c) the assessment or collection of a tax or duty or an imposition of a similar nature,

to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).

Schedule 2, Part 1, Section 5,

(1) The listed GDPR provisions do not apply to personal data consisting of information that the controller is obliged by an enactment to make available to the public, to the extent that the application of those provisions would prevent the controller from complying with that obligation.

(2) The listed GDPR provisions do not apply to personal data where disclosure of the data is required by an enactment, a rule of law or an order of a court or tribunal, to the extent that the application of those provisions would prevent the controller from making the disclosure.

(3) The listed GDPR provisions do not apply to personal data where disclosure of the data—

(a) is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights,

to the extent that the application of those provisions would prevent the controller from making the disclosure.

The Council has control processes in place to ensure all such disclosures are managed by Information Governance and authorised by the DPO to ensure that they are legally permissible, recorded and auditable. Staff must not respond to any request for Personal data from anyone, not even the data subject, without first contacting the DPO for advice, no matter how genuine the request appears or how insistent or forceful the applicant may be.

NB.
It should be noted that the DP Act 2018 does not place a requirement on the Council to provide data following a non-disclosure request. It is for requesting organisations to put forward a strong lawful case. The final say is always with the Councils' DPO.

Part B

Under the DP Act 2018 there are some instances where personal data held about an individual are exempt from disclosure to that individual. The Council will review all such exemptions with a view to disclosing as much as is possible without causing harm.

The list is limited to those in the provisions found in the DP Act 2018, Schedule 2, Part 3 onwards. Below are the main reasons the Council may need to consider refusing to disclose personal data under the provisions;

- LPP (Legal Professional Privilege)
- Self-Incrimination
- Management forecasts
- Confidential references
- Exam marks

- Health and safety
- Exam results
- Medical records (subject to the harm test)
- Accreditation

All exemption disclosure requests are recorded and responded to centrally by Information Governance so that there is a full audit trail.

GDPR Guidance Note 5B – provides further guidance on processing exemption requests and compliant request forms.

Part 6

Sharing Data

18 Data Sharing and Processing Agreements (framework)

The Council follows the ICO Data Sharing Code of Practice. The aim of the code is to help organisations adopt good practice when sharing information and comply with requirements of GDPR and DP Act 2018.

The Council actively encourages the use of Data Sharing (or Processing) Agreements (DSA's) between organisations to formalise and define the way Personal data is shared. This approach ensures that personal data is shared lawfully, responsibly, appropriately and proportionally.

Though there is no one template, the Council uses the Crown Commercial Services (CCS) Framework as the basis for all DSA's (see GDPR Guidance Note 6). New agreements proposed by external organisations and partners must at least include all the points within the CCS framework.

DSA's must be approved and signed off by at least one of the following before they become active:

- Data Protection Officer.
- Monitoring Officer
- Chief Executive (Data controller)

A copy of all signed DSA's must be given to the Data Protection Officer (DPO) so that they can keep a corporate record of all approved DSA's. The DPO must be consulted in respect of any proposed changes to existing DSA's. Changes must be approved in the same way as a new DSA.

The Council is a signatory to a number of County-wide DSA's including the Northamptonshire Partnership Information Sharing Statement, which is available as part of the GDPR Guidance Note 6.

GDPR Guidance Note 6 – provides advice and guidance on Data Sharing and Processing Agreements. It should be read alongside current ICO guidance and A29 Working Party advice and opinions.

19 Tenders and Contracts

The Council's Contract Lawyer should be consulted whenever a contract includes the collection, holding or processing of personal data.

Though the Council does use some model data protection clauses, such as in the CCS procurement framework, it is often the case that clauses will require tailoring for each individual circumstance.

20 External Data Sharing Agreements

The Council will only consider drawing up a DSA with external partners and organisations that are ICO registered data controllers. To share otherwise would not provide the safeguards required to assure individuals that their personal data was being managed responsibly or in compliance with legal requirements.

Data sharing with external partners, organisations and individuals (such as consultants working for the Council) is controlled and defined through Data Sharing Agreements (DSA's). These can be separate agreements or combined within contacts. Where these are drawn up by a third party the Council's Data Protection Officer and Contract Lawyer should be consulted about the appropriateness and legality of the wording.

The process for agreeing externally drafted DSA's is the same as for NBC agreements. Without an approved DSA in place the Council **cannot** lawfully share Personal data except when there is a specific basis in law to do so.

21 Data Processing Agreements [DP Agreement]

Data Processors now assume direct accountability for the management of the personal data that they process on behalf of other data controllers such as the Council. GDPR Article 28 stipulates in paragraphs

1. '*Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.'*

3. *Processing by a processor shall be governed by a contract or other legal act under Member State law.*

Therefore the Council **must** have an agreement [contract] in place before any personal data can be passed to another data processor. That agreement must define;

- The specific data to be processed.
- The method of processing.
- The processing controls and security measures.
- The approved methods of secure data transfer.
- The audit and accountability procedures (quality assurance).
- Erasure / destruction process.
- Liability.

The data processor must be registered with the Information Commissioners Office.
A Data Processor cannot permit or use a third party subcontractor to further process that personal data without written authority from the Council and that change being incorporated into a revised DP Agreement.

22 Data Matching and Fraud Detection (National Fraud Initiative)

The Council is required by law to provide personal information data sets periodically to the Audit Commission to assist nationally with data matching exercises under section 68 of the Serious Crime Act 2007. This permits the disclosure of personal data for the specific purpose of the prevention and detection of fraud.

The data matching exercises are conducted as part of the National Fraud Initiative (NFI). There is a statutory Code of Practice and a model Privacy Notice providing further information about the lawful processing of citizens personal data for this purpose. Details of each exercise and the data sets required are available on the Audit Commission's website.

The Council supports the national data matching exercise. It provides all data required for each exercise and follows the relevant codes of practice to ensure the data is transmitted and processed securely at all times.

Part 7

Transmission and Transportation

23 Data movement, access and risk mitigation

The greatest single risk to the security of personal data is during transmission and transportation. Every time data is moved a risk of loss, theft or breach is created. Specific detailed departmental policies must be used to ensure that the security of Personal data is not compromised during the transmission and transportation process. Controls are considered further in sections 24 & 25 below.

GDPR Policy Statements

Risk assessment is fundamental to data protection compliance. Under the GDPR, consideration of risk underlies organisational accountability and all data processing.

The identification and classification of risks should include both material and non-material (tangible and intangible) harms. Material harms may require prioritisation over non-material harms, depending on context.

Table 2 below, though not intended to cover every conceivable risk, considers many of the more common 'data risk triggers' associated with data movements and some strategies that can be employed to significantly reduce the risk, and in some cases totally eliminate the risk of a data breach. You will need to complete a specific risk matrix as part of you DPIA.

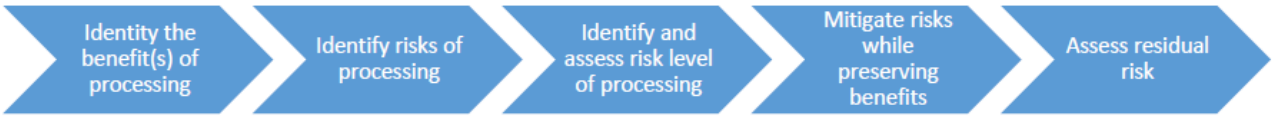

Table 2 – File movement risks

Areas of risk	Specific Risk	Suggested risk mitigation
Physical file movements		
File removed from an archive or store cupboard and cannot be traced. No records of who last had file.	Potential data breach but no evidence of loss. Staff unable to work or update case. File has to be recreated, potentially with new data gathered from individual.	Use markers such as coloured cards to sign and leave in place of file to indicate when it was removed, why and by who. Scan file [to EDRMS] and return/destroy.
Personal data file lost in office. No one knows where it is.	As above.	Use clear desk and office strategies suitable for you specific office environment. Employ file movement logs to track. Use EDRMS to remove the need for physical files.
File taken out of office to meeting.	Potential data loss. File left unattended. File misplaced / taken.	Employ Personal data file recording to sign out and back in. Make the file electronic and place on a secure device or make available via secure location. Send to print in new location; destroy copy after use.
Office move	Files lost in transit.	Log all files before move and check back in after move.
Home working	Transport of physical files. Access to non-staff in the home environment. Burglary.	Only access secure online files from home. Use secure email and password protected files.

Post	Data lost in post. Wrong data posted. Post incorrectly addressed.	Signed for does not make the postage any more secure, though it does give assurance that someone at the other end has received the information. Courier, particularly same day door-to-door, is about the most secure way to post.
Electronic file movements		
File not found on server	Moved or deleted. Time wasted recovering from back up.	Improve file management controls and training. Consider EDRMS.
Access across network drives	Personal data placed in unsecure shared area	Use secure folders and password protected files in departmental J drives to hold Personal data. Consider EDRMS.
Home working	Particular risks include the storage of data on removable drives such as USB sticks, the holding of data on a laptops and taking files home. Accessing data over insecure network.	Only use encrypted storage devices (NBC enforced policy). Remove rights to access insecure online storage.
FTP e.g. Dropbox	Insecure access. Poor accountability of access. No corporate control or file back up.	Use SFTP (Secure File Transfer Protocol) sites over insecure ones. Virtual Data Rooms provide a high level of secure storage. Huddle and other similar file share sites have secure areas. Beware of where the data is held, particularly in the cloud.
Email	Often overlooked as a transmission risk. Standard email is not a secure way to send Personal information.	Consider password protection. encryption, or secure email such as GCSX depending on the level of risk identified

GDPR Guidance note 7 - provides further advice on how to identify and mitigate Personal data risks and can be used alongside Guidance Note 9 – Data Protection Impact Assessments.

24 Physical personal data file movements

Lack of control measures used to manage personal data files within the office environment and during archive deposit and retrieval are the biggest single cause of data loss within an organisation nationally. It causes time lost searching for a missing file, delays dealing with customers and can result in embarrassment recreating the file from new data. Under GDPR it also creates a reportable data loss.

Control measures are therefore essential to the smooth running of a modern efficient office and to provide the assurance to members of the public and the regulator that personal data management is a high priority.

There are 4 key areas of risk:

1. Between staff (same department and between departments).
2. Transportation - site visits including client visits.
3. Archive deposit and retrieval.
4. File destruction.

Departments should analyse the tangible and intangible risks in these 4 areas and put in place mitigation procedures. The DPIA can assist you to identify your key risk areas. The Data Protection Officer can assist you to develop and implement your mitigation strategy.

Departments should consider EDRMS as a permanent solution to mitigate the risk of lost physical files.

25 Electronic personal data file transmission

Transmitting personal data inherently creates a risk of data loss. As soon as data moves out of the Council's secure internal network the potential for loss increases exponentially. It is therefore essential that the additional control measures are utilised to reduce or eliminate both the tangible and intangible risks associated with data transmission.

Password protecting – All documents containing personal data should already be password protected with a unique not generic passcode. The passcode should be unrelated to the file name, Data Subject, date of creation, author, department or organisation.

Encryption – In addition to the passcode to open a personal data document, electronic files containing Special categories of Personal data **must** be encrypted or held behind an encryption layer when being transmitted either by email or via online storage.

Emailing – Password protection **must** be used on all email file attachments containing Personal data. GCSX or similar secure email network **must** be used to transmit special categories of personal data or share data with other central and local government departments and agencies.

Online public cloud file storage – This media is only suitable for non-personal data transmission. Personal data **must not** be shared using cloud solutions without explicit permission from the data subject and the Data Protection Officer. Unless cloud based storage for any electronic files and particularly Personal data can be proven to exist only in the UK or wider EEA then its use is strictly forbidden.

Secure File Transfer Protocol Sites (SFTP) and Virtual Data Rooms (VDR's) – Provided that it can be shown the personal data will be held within the UK or wider EEA then the use of SFTP sites and VDR's is encouraged as a relatively secure way to transfer password protected personal data files.

Part 8

Encrypting personal data

26 Removable media (USB)

To completely remove the risk of personal data breach from the loss, theft or unauthorised access to any data held on a removable media device (RMD) the Council enforces McAfee Endpoint Encryption at user level. All computers and laptops block the downloading of data to all removable drives including hard drives, USB's, memory cards and optical media.

Endpoint encryption initialises a 256 bit AES encryption layer in front of all files and folders on the device. A copy of the software is also installed so that the device can be accessed from any machine. The user creates a unique password which secures the device and protects all data placed on the device behind the encryption layer.

Employees can request permission to use the encryption software where there is a demonstrable corporate need.

i. Employees complete a request form which is countersigned by their Head of Service who agrees the corporate need.
ii. The form is then reviewed by the Data Protection Officer (DPO) who uses the DPIA process to evaluate the risk and need.
iii. If approved endpoint encryption is enabled and training provided to the user.
iv. Access is reviewed annually and employees not using encryption regularly are contacted and access revoked if the need has changed.

Access can only be provided to PC and Laptop users. Wyse users will need to ask ICT or the DPO to create their drive and download their data. Alternatively departments could nominate their own super user responsible for all encryption in their area.

GDPR Guidance note 8 – details the Council's Endpoint Encryption policy and approval process (commonly called the USB Encryption Policy).

27 Local drive storage

Citizens personal data **must not** be stored on:

- A local PC device drive or memory,
- A laptop,
- Any unencrypted removable media device,
- Any device or storage media not owned by the Council e.g. your own personal devices or that of another person, organisation or partner.

Anyone found to be storing citizens personal data on any of the above will be subject to the Council's gross misconduct procedure.

GDPR Policy Statements

Part 9

Personal Data Impact Assessments

28 Data Protection Impact Assessments (DPIA)

Ensuring personal data is processed correctly from the very beginning is critical to the Council's ongoing compliance with its obligation to safeguard personal data.

GDPR Article 35 sets out for the first time in legislation the requirement that all processing activities, particularly new processes and changes to existing processes, **MUST** be subject to a DPIA.

GDPR Article 35 states:
1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of Personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a DPIA.

Therefore, and with due regard for the GDPR, ICO Code of Practice and Article 29 Working Party guidance, the Council has produced a DPIA toolkit . This provides a step-by-step approach to evaluate the risks and identify mitigation strategies associated with proposed, new or existing personal data systems to ensure they are GDPR complaint.

Its use is mandatory for the following:

- Any change to an existing manual personal data collection process
  E.g. Consultation, survey, petition, membership/contact list

- Any proposed new process that involves the collection of personal data
  E.g. Consultation, survey, petition, membership/contact list
- All system upgrades where the system holds any personal data
  E.g. Planned software version upgrade
- All proposals for a new or replacement software solution that will hold personal data. *E.g. Implementation of a new case management system or Document Image Processing (DIP) solutions such as EDRMS*

The DPIA toolkit provides help to identify weaknesses or risks in respect of personal data losses or breaches and consider action that needs to be taken to ensure compliance where such compliance is not yet achieved. DPIA applies equally to paper as well as electronic data processing systems.

Suppliers/contractors must give all reasonable assistance to the Council in the preparation of any DPIA before starting any installation or upgrading process, including:

- A systematic description of the expected processing or change and its purpose.
- The necessity and proportionality of the processing operations.
- The risks to the rights and freedoms of individuals.
- The intended measures to address the risks, including safeguards, security measures and mechanisms to protect personal data.
- The supplier must also put in place appropriate protective measures to protect against a data loss event during the installation.

DPIA has been integrated into the project initiation process and has been embedded into the ICT Governance Board's approval process. From 25th May 2018 no new system that holds or processes personal data will progress until a DPIA has been completed and signed off by the Data Protection Officer and ICT Governance Board as part of the project initiation process. Major issues may mean changes to the project to ensure compliance. Minor issues identified in the DPIA will become part of the project risk register for resolution before project sign off.

GDPR Guidance Note 9 contains the Councils Data Protection Impact Assessment (DPIA) Toolkit

Part 10

Retention, destruction and decommissioning

29 Data retention

GDPR Data Principle (e) – Storage limitation, requires the Council to only keep personal data for only as long as is necessary.

How long data has to be retained will depend on the higher of one of the following factors:

1. **Statutory Requirement**; such as most finance records which are kept for CFY+6FY (current financial year plus 6 financial years).
2. **Best Practice;** Examples may include a Code of Practice issued by a Commissioner or Regulatory or an industry body such as CIPFA.
3. **Business Need;** the need to retain data may be specific to the organisation or the department. Provided the rationale for retention is justified, not excessive and is not less than 1 or 2 above there is no reason why you cannot set your own retention period.

A retention schedule will contain details of how long specific record types should be kept for. Your departmental retention schedule may well be different to another department's for exactly the same data type. This is perfectly acceptable and not unusual. Information

Governance and the Data Protection Officer can advise on how long information should be kept.

GDPR Guidance Note 10 includes a copy of the Corporate Retention Schedule and a template for departments to add their own specific retention periods.

30 Reviewing data

Previously, advice under DPA98 was that personal data should not be kept on active files for more than a maximum of 6 years without being refreshed. GDPR brings in the requirement to keep the retention of personal data under constant review for example, a consultation database. At each new consultation individuals must be asked if they wish to remain on the database. Those that do not and those who are undeliverable should be removed. The database remains current and compliant with the GDPR Data Principle.

There are of course exceptions such as Council Tax where a person can remain liable for many years or even decades. Their billing address never changes so the account will only need changing when there is a change of circumstances.

Ideally, as a minimum, data should be reviewed every couple of years.

- Privacy notices state how long personal data will be held for. There must be processes in place to ensure the personal data is erased /securely destroyed at the end of this period. E.g. records of disciplinary action, consultation responses, monitoring data etc..
- Departments must have in place procedures to ensure personal data (such as contact details) are updated regularly. Some departments, such as HR, may do this annually; others will do it as a rolling process such as Housing Tenancy and Planning while some will just note the date the details were put onto the system such as Council Tax.

There is no requirement to update personal data on closed files such as ex-tenant files, though it is good practice to set review periods where data no longer relevant can be destroyed. GDPR compliant EDRM Systems can allocate different retention and deletion rules to each document type indexed and can be used to delete some indexed files in a case whilst leaving others.

Department retention schedules must include review periods where necessary to ensure Personal data is not held longer than necessary.

31 Destroying paper documents and files

Secure destruction of all personal data, special categories of (Sensitive) personal data, confidential, commercial and financial information held by the Council is mandatory.

From August 2018 secure destruction receptacles will be placed on every floor and must be used unless you have a departmental shredder. They must only be used for secure destruction waste.

For larger destruction requirements, such as your yearly archive file destructions, you will need to book and pay for additional receptacles through the Data Protection Officer.

32 Deleting electronic files

The rules for deleting electronic files are no different to that of paper records; the retention periods are exactly the same for both. It is easy to forget about electronic documents as they do not clutter the desk or fill a cupboard. They do however require considerable ICT resource to continually back up and store on archive tape.

It is good practice to have electronic files such as old reports, reference material, old Journals etc. that are no longer accessed regularly to be archived to a drive or an encrypted departmental hard drive. They remain accessible to you but corporately the Council is not spending time and resource constantly backing them up. ICT should be advised and a copy of the drive taken and archived for recovery purposes.

You must advise the Data Protection Officer of any new hard drive so that it can be recorded on the hard drive log for audit purposes. The DPO and ICT can advise

33 ICT decommissioning

Wherever possible the Council's ICT Services (currently provided by LGSS) will seek to reuse ICT hardware to maximise the return on investment and minimise waste. Where prudent to do so, ICT Services will look to sell ICT hardware as an alternative to disposal. However where this is not possible the Council will manage the secure disposal of all redundant hardware through specialist decommissioning and destruction companies who comply with both the Waste Electronic & Electrical Equipment (W.E.E.E.) Regulations as well as data protection requirements.

ICT Services clear down and wipe all PC's of user profile data. No corporate data should have been stored on the PC's 'C' Drive (hard drive) however this is also checked and cleared. Printer and other hardware hard drives are wiped before being decommissioned.

Redundant items are then stored and are batch collected and securely destroyed by a special company with all of the relevant haulage and environmental certification. Certificates of secure destruction and WEE Regulation compliant disposal are retained by the Data Protection Officer for a period of 7 years.

Part 11

Non Compliance

8th Golden DP Rule

You must notify the Data Protection Officer immediately if you identify or suspect any personal data misuse. You may also want to consider raising the issue through the Council's Whistleblowing procedure.

GDPR8

34 Breaches

The Council is required to proactively report significant data breaches to the Information Commission. To do this, anyone who suspects or finds that a data breach, data loss, data theft or misuse of personal data has occurred should inform the Data Protection Officer (DPO) at the earliest opportunity, preferably on the same day. You should not wait to inform your manager, the DPO will do this as part of the investigation.

Types of suspected data breaches include, but are not restricted to:

- Accidental disclosure of personal data to another person or organization.
- Emailing of personal data to the wrong recipient.
- Inappropriate access to or use of personal data.
- The theft of personal information, either paper based or electronic.
- Accidental loss of personal data.
- Personal data that has not arrived at its destination.
- Fraudulent acquisition of (or attempt to acquire) personal data (blaggers).
- Near misses.

The DPO must investigate the suspected data loss at the earliest opportunity. Each reported breach will receive a unique breach log reference number and will be recorded on a REACTER report and log. Within 3 working days of the suspected breach being notified the DPO will complete the initial investigation and draft report. If the report identifies a significant breach, and after consulting with the Chief Executive and / or Monitoring Officer, the DPO will inform the Information Commissioners' Office of the breach and provide a full report to them within 5 working days. Where appropriate, particularly in respect of theft, the police will also be notified.

Where a breach is shown to have originated from a member of staff it will be dealt with in accordance with the Council's procedure for dealing with poor performance and misconduct. Managers will need to decide what action is appropriate based on the circumstances and may wish to seek advice from HR, the DPO and if necessary Legal Services, (particularly in the case of criminal offences). This will be in addition to the breach report to the ICO.

35 Consequences of non-compliance including data breach

The Information Commissioner (ICO) has a duty to monitor and enforce compliance with GDPR. This includes the power to conduct audits to assess whether an organisation's processing of personal data follows good practice. Following such an audit the Information Commissioner has the power to issue the following notices.

Information notice
Sections 142 – 145 of the DPA 2018. An information notice would require the Council to provide certain information within set time limits to the ICO. It would usually be served to assist the ICO determine if further notices and or action was necessary.

GDPR Policy Statements

Assessment notice
Would require the Council or one of its processors to permit the ICO to carry out an assessment (audit) to ascertain if it is complying with the data protection legislation.

Enforcement notice
If the Information Commissioner decides that there had been or is a failing, he may serve the Council with an enforcement notice (Sections 149 – 153 of the DPA 2018). Failings fall into 4 types, 3 could be applied to the Council.

149(2) The controller or processor has or is failing to comply with the principles, individuals rights, obligations, breach reporting or restricting international transfers.

149(4) The controller does not meet the accreditation requirements, certification or any other GDPR requirement.

149(5) The controller has failed to comply with DPA 2018 section 137 (pay an annual fee).

Penalty notice
Sections 155 – 159 of the DPA 2018. The ICO has the power to issue monetary penalties under GDPR Article 58 if they are satisfied the controller as or is failing or has failed to comply with any of the notices in this section.

The ICO can prosecute those (personally and corporately) who commit criminal offences under GDPR Article 83.4 and 5 or sections 170 – 173 of the DPA 2018. The maximum penalty for such a failing is the sterling equivalent of €10,000,000 (or 2% of annual turnover).

The maximum penalty for a serious and significant data breach is the sterling equivalent of €20,000,000 (or 4% of annual turnover).

The maximum fine for failure to comply with DPA 2018 section 137 is 150% of the annual charge applicable at the time.

In addition, in relation to computer processed personal data, the following offences remain under the Computer Misuse Act 1990:

- Unauthorised access to computer
- Unauthorised modification to contents of computer, and
- Unauthorised access with intent to commit / facilitate the commission of further offences.

36 Corporate responsibility

The data controller for the purposes of GDPR is Northampton Borough Council's Chief Executive. His deputy is The Monitoring Officer.

The person responsible for the day-to-day management of data protection at the Council is the Data Protection Officer, David Taylor, who has a direct reporting line to the data controller in respect of the statutory obligations set out in the General Data Protection Regulation 2016, the Data Protection Act 2018 and detailed in Part 12 of this policy.

GDPR Policy Statements

Part 12

DPO duties & responsibilities

37 The Data Protection Officer

The Council has, under GDPR Article 37 paragraph 1 and DP Act 2016 s69 – s71, appointed David Taylor as the Council's Data Protection Officer (DPO).

The DPO's duties are aligned to those as set out in GDPR Article 39 and the 29 Working Party Guidance (A29WP) on the role and responsibilities for the position.

a) Ensure the Council's Data Protection Notification accurately reflects the activities of the Council and is renewed each year (see policy statement 40).
b) Maintain the Corporate Data Protection Policy and related guidance by ensuring it reflects current legislation and best practice.
c) Inform, advise and provide guidance and assistance to the data controller, the processor, employees, elected Members, contractors, agents, partners or consultants who have access to any personal information held by or on behalf of the Council in the practical application of the obligations pursuant to the GDPR, to other Union or Member State data protection provisions and this policy and associated guidance.
d) Monitor compliance.
e) Provide induction and ongoing corporate training to ensure all data handlers and processors understand, and continue to understand, their responsibilities with regard to all data protection obligations.
f) Investigate personal data breaches, losses, inappropriate use, theft and malicious cyber incursions and where necessary report such incidents to the data controller, the Information Commissioner and the Police.
g) Record and manage all requests for access to personal information including subject access and DPA 2018 Sch2, Part 1, (2) & (5) requests.
h) Keep a log of electronic and manual databases and to review their use periodically for compliance.
i) Maintain corporate records of data processing processes include data flow maps and a change log.
j) Provide a Data Protection Impact Assessment (DPIA) toolkit, advise where requested on its use and monitor DPIA performance pursuant to Article 35.
k) Keep a log of, and regularly review, the continued appropriateness and compliance of all Data Sharing and Data Processing Agreements in place and approve all new agreements in consultation with Legal Services.
l) Cooperate and liaise with the Information Commissioners Office and act as the contact point for the ICO on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

In order to assist the Data Protection Officer, Council staff must inform the DPO if their department: -

- plans to create a new database, or relevant manual filing system; or plans to purchase or use a third party database to hold Personal information, or
- discovers an unexpected data loss or any potential security breaches.

Departments should identify a departmental 'Data Champion' to assist the DPO manage data compliance in their service area.

38 The Notification process

The Council maintains, and will continue to maintain, regular notification of its data processing activities to the Information Commissioners Office (ICO) under section 134 of the Data Protection Act 2018.

Its current registration number for such purposes is Z5256045.

It is the responsibility of the Council's DPO to ensure the Council:

- renews its annual Data Protection Fee on or before the last day of February each year,
- at least annually review its data protection notification to ensure that it reflects the use of personal data within the authority and,
- promptly (within 28 days) updates notified changes to its notification to the ICO.

It may mean that a notification amendment is needed if:

- personal data is no longer needed for an activity,
- new data is to be used for a new activity, or
- changes are made to the way personal data are used in an existing activity.

To enable this process to begin you will need to supply the following information in writing to the Data Protection Officer:

- why (for what **data purpose)** are personal data being processed?
- who is it about (the type of **data subject**)?
- what personal information (**data classes**) is being held?
- who has it come from and who does it go to?
- is information to be sent abroad, and if so where to?

It is your responsibility to ensure changes to the way you collect, hold or process personal data is reported to the DPO. Only after you have supplied written notification of changes can the notification be reviewed and amended if required. You are breaking the law if you knowingly process personal data in contravention of the Council's Notification and the GDPR.

9th Golden DP Rule

Under no circumstances can you begin collecting personal data for a new or amended purpose until the Council's notification has been checked and amended if required by the Data Protection Officer.

GDPR9

39 Data complaints & investigations

Individuals expect the personal data the Council holds to be processed and destroy in a safe and secure environment and in compliance with the GDPR, DP Act and its ICO notification.

Occasionally individuals may have cause for concern that their Personal data has not been managed as they would expect and have the right to complain. All such complaints, whether directed at the Council or one of its data processors, must immediately be passed to the DPO who will investigate and respond in the first instance using, wherever possible the timescales in the Council's Corporate Complaints Policy; that is 3 days for an initial response and 10 days to provide a formal written response.

An appeal to the outcome can be made within three months and will be responded to within 20 working days by the data controller. If the matter is still not resolved the final step is to ask the Information Commissioner to review the case.

If a complaint relates to an alleged data breach the Council will investigate according to its data breach procedure.

40 Training

Data protection training is a crucial element of staff awareness. Staff, both permanent and temporary, need to be aware of their obligations relating to all Personal data they process as part of their Council duties. Failure to adhere to the eight data protection principles can lead to possible disciplinary action and prosecution.

It is the Council's Policy that all staff who hold or process Personal data receive the appropriate training.

Basic data protection training is provided to staff via their induction process departmentally and corporately. Additional training will be provided for all who have access to Personal information to ensure that they know how to:

- Identify and manage personal data and Special categories of personal data
- Keep Personal data safe and secure
- Seek advice in respect of Data Protection queries and complaints

Further in-depth data protection training will be provided for all staff whose main or core function is to process personal data.

- Collect, process and store personal data
- Record keeping, free text and identifying individuals rights
- Reporting a data breach

In addition staff are expected to read this Corporate Data Protection Policy.

41 Policy review

This policy is subject to an annual review including its accessibility to staff and all related advice and guidance.

The review will include tests on the continuing appropriateness of the safeguards and controls already in place.

In addition, changes to legislation, national guidance, codes of practice or supervisory body advice may trigger individual policy section reviews and updates.

10th Golden DP Rule

When you think about data protection remember that we are all data subjects. Think about how appropriately and securely you would like your personal details to be handled and then manage the personal details of others in the same way.

GDPR10

Part 13

Annexes

Annex 1 - Compliance Related Legislation

Computer Misuse Act 1990
Data Protection Act 2018
Disability Discrimination Act 1995
Disability Discrimination Act 2005
The Environmental Information Regulations 2004
Freedom of Information Act 2000
General Data Protection Regulations 2016
The Human Rights Act 1998

Annex 2 - Links to other associated legislation

Civil Contingencies Act 2004
Copyright, Designs and Patents Act 1988
Criminal Justice and Immigration Act 2008
Defamation Act 1996
Electronic Communications Act 2000
Public Interest Disclosure Act 1998
Regulation of Investigatory Powers Act 2000
The Re-Use of Public Sector Information Regulations 2005
Serious Crime Act 2007

Annex 3 - References

The Information Commissioners Guide to Data Protection
Legal guidance on Data Protection
Article 29 Working Party Guidance
Article 29 Working Party Opinions

GDPR Policy Statements

Annex 4 - Contact details

At Northampton Borough Council	The Data Protection Regulator
David Taylor Data Protection Officer Northampton Borough Council The Guildhall St Giles Square Northampton, NN1 1DE	The Information Commissioner's Office Wycliffe House Water Lane Wilmslow SK9 5AF
Telephone : 01604 83 8536 Email: djtaylor@northampton.gov.uk	Tel: **0303 123 1113** **Live Chat:** ICO live chat Website: https://ico.org.uk/your-data-matters/raising-concerns/

Annex 5 - Guidance Notes to this Policy

The following GDPR Guidance Notes support this policy and provide further information, useful tips, implementation information, templates and forms.

GDPR-GN01 – Corporate Privacy Statement and Departmental Privacy Notices (templates).

GDPR-GN02 – How and where to hold Personal data and Version Control Policy.

GDPR-GN03 - Clear Desk and Secure Office Environment Policy.

GDPR-GN04 – The Protective Markings Policy and details and templates for the data processing records.

GDPR-GN05A – Subject Access Requests including a copy of the request form DSAR1.2.

GDPR-GN05B – Guidance on processing exemption requests and compliant request forms.

GDPR-GN06 – Data Sharing and Processing Agreements including DSA & DPA templates.

GDPR-GN07 - Identifying and mitigating Personal data risks.

GDPR-GN08 – The Council's Endpoint Encryption (USB) policy and approval process.

GDPR-GN09 – Data Protection Impact Assessments Toolkit

GDPR-GN10 - Retention Schedules and Destruction Guidance

Annex 6 – GDPR Golden Rules

THE 10 GOLDEN DATA PROTECTION RULES

1. **Treat others data as though it was your own.**
2. **Only collect the minimum amount of personal data**
3. **Publish your Departmental Privacy Notice**
4. **Only write what you'd want recorded about you**
5. **Treat all personal data as provided 'in confidence'**
6. **Only use personal data for the purpose it was collected for**
7. **Never disclose personal data without asking security questions**
8. **Notify the DPO immediately if you suspect misuse or a data breach, loss or cyber attack**
9. **The DPO must approve all new personal data collection**
10. **Manage others data as you would want you data managed**

Annex 7 - The Information Commissioners Personal Information Promise (PIP)

I (name and title),
on behalf of (name of organisation)
promise that we will:

1. value the personal information entrusted to us and make sure we respect that trust;
2. go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
3. consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
4. be open with individuals about how we use their information and who we give it to;
5. make it easy for individuals to access and correct their personal information;
6. keep personal information to the minimum necessary and delete it when we no longer need it;
7. have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
8. provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;
9. put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and
10. regularly check that we are living up to our promises and report on how we are doing.

Signed

(name and title)

Date

Annex 8 – Think Privacy