Data Protection Policy

April 2018

districtnk
100 flourishing communities
North Kesteven District Council

Alternative Formats

This document can be made available in large print, Braille, audio tape, electronic formats such as CD, or in a different language. Our website is ReadSpeaker enabled. For a copy please contact the Corporate Information Team at the Council using the following options:

Phone: 01529 414155 (main switchboard)

Fax: 01529 413956

Web: www.n-kesteven.gov.uk

Email: equality@n-kesteven.gov.uk

Corporate Information Manager
North Kesteven District Council
Kesteven Street
Sleaford
Lincolnshire
NG34 7EF

Introduction
This document sets out North Kesteven District Council's policy regarding Data Protection and Incident Management; it is based on the General Data Protection Regulations (GDPR), which will come into force on the 25 May 2018. The GDPR is the new legal framework in the European Union. There will also be a new Data Protection Act 1998 (DPA), which is currently going through Parliament. This new Act will add to the GDPR and provide new rights to individuals concerning personal data.

The purpose of the GDPR is to regulate the way that personal information about living individuals is obtained, stored, used and disclosed. The Regulation grants rights to individuals to see data stored about them and to require modification if the data is incorrect. These provisions amount to a right of privacy for the individual. The Regulation requires that all processing of personal data must be notified to the Information Commissioner, who is the supervisory authority, and that personal data must be kept and used in accordance with the provisions of the GDPR.

As part of the organisation's obligations and duties relating to Incident Management, it must protect data using all means necessary by ensuring that any incident which could cause damage to the Council's assets and reputation is prevented and/or minimised. However, North Kesteven District Council needs to collect and use certain information about people to allow us to carry out our many and varied functions and responsibilities. This includes information on current, past and prospective employees, suppliers, clients, customers, service users and others with whom it communicates. The Council is required by law to collect and use certain types of information to fulfil its statutory duties and also to comply with the legal requirements of the Government. This personal information must be dealt with properly whether it is collected, recorded and used on paper, computer, or other material. The Council will ensure all employees, elected Members, contractors, agents, consultants, or partners of 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 duties and responsibilities under the Regulation. North Kesteven District Council is fully committed to compliance with the requirements of the GDPR and understands it is essential that it treats personal information lawfully and correctly.

The purpose of this Policy is to explain how the Council will ensure compliance with the GDPR and best practice relating to Incident Management. It includes organisational measures and individual responsibilities which aim to ensure that the Council complies with the Data Protection principles. The Policy exists to respect and protect the rights of individuals (which includes residents, employees and partners), whilst ensuring transparency about how it stores and processes individuals' personal data.

Purpose of the General Data Protection Regulations (GDPR)
The primary purpose of the GDPR is to provide a set of standardised data protection laws across all the Member countries of the European Union (EU). The intention is that this should make it easier for EU citizens to understand how their data is being used, and also raise any complaints, even if they are not in the country where it is located. In addition, the GDPR will:

- Increase privacy and extend data rights for EU residents
- Help EU residents understand personal data use
- Address the export of personal data outside of the EU
- Give regulatory authorities greater powers to take action against organisations that breach the new data protection regulations
- Simplify the regulatory environment for international business by unifying data protection regulations within the European Union
- Require every new business process that uses personal data to abide by the GDPR data protection regulations and Privacy by Design rule.

Definitions
To aid understanding of this Policy, certain words have specific meanings under the GDPR:

Anonymisation
Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

Data Controller
This is the organisation or individual(s) who hold and use (process) personal information. Data controllers are responsible for ensuring that data is processed within the principles of the GDPR. The GDPR places additional emphasis on meeting contractual obligations with the processor to ensure they also comply with GDPR.

Data Subject
Data subject is the individual about whom personal data is held. Data subjects have certain legal rights in relation to how, if at all, their personal data is processed.

Data Processor
Data processor means any organisation or person, other than an employee of the Council, who processes data on behalf of the data controller. For example, someone contracted to the Council to undertake work on its behalf. As a processor, the GDPR requires them to maintain records of all processing activities and personal data use, which increases the legal liability for processors in the event of a breach.

Identifiable Natural Person
An Identifiable Natural Person is anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Information Commissioner
Each Member State has to have one or more independent public authority to be responsible for monitoring the GDPR. This is in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union. The Information Commissioner's Office is the supervisory authority for the United Kingdom and is the post established to oversee the implementation and enforcement of the GDPR. In addition, it manages the notification process, handles queries and complaints and enforces the terms of the GDPR.

Personal Data
The GDPR makes a distinction between personal data and 'sensitive' personal data. Personal data is any information, which relates to an identified or Identifiable Natural Person. In addition, it includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. The definition of personal data has been expanded to reflect the importance of the online element of many individuals' and includes online identifiers, device identifiers, cookie IDs and IP addresses.

Processing
Processing means obtaining, recording or holding the information or data, or carrying out any operation on the data (whether or not by automated means). This includes organisation, adaptation or alteration, retrieval, disclosure and destruction of the data.

Pseudonymisation
Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a 'key' that allows the data to be re-identified.

Relevant Filing System
Relevant filing system means any filing system which is structured and refers to identifiable individuals; the information relating to those individuals being readily accessible.

Sensitive Personal Data
Sensitive personal data is subject to stricter conditions of processing. The scope of personal sensitive data has been expanded to keep up with advances in medical technology, therefore sensitive personal data means personal data consisting of information in any of the following categories:

- Genetic data;
- Biometric data;
- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

Data Protection Principles
The GDPR introduces six principles to replace the eight found in the Data Protection Act 1998. These relate to the collection, use, processing, and disclosure of data, and the rights of data subjects to have access to personal data concerning themselves. These Principles are listed below:

1. Data processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')

Under the DPA, the data controller is required to process the data fairly and lawfully. The DPA also requires that the data controller make available to the data subject certain specific information, but there is no express obligation to process the data transparently. The inclusion of the principle of transparency is a new provision in the GDPR. The DPA does make some provision for the data controller to process data transparently, but this concept has now been enshrined as a core principle.

When the data is collected, the Council will be clear as to why that data is being collected and how the data will be used. The Council will provide details surrounding the data processing when requested by the data subject. For example, if a data subject asks what data the Council has about them, that information will be made available.

2. Data obtained for a specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')

The principle in the DPA places similar limitations on processing as those contained in the GDPR principle. Therefore, this principles remains largely the same as under the DPA. However, the GDPR also permits further processing for public interest and/or scientific purposes, widening the scope for further processing by data controllers.

This principle means that the Council will always have a lawful and legitimate purpose for processing the information in the first place. In essence, this means that the Council will not collect any piece of data that does not have a specific purpose.

3. Data processed is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

The DPA requires that processing shall not be excessive in relation to the purpose for which the personal data is processed, however the GDPR strengthens this requirement. The GDPR raises the threshold from the controller being limited to processing that is not excessive to only enabling the controller to process data that is necessary.

This principle instructs the Council to ensure the data it captures is adequate, relevant and limited. Therefore, the Council will not collect and compile every piece of data possible for various reasons, such as understanding customer buying behaviours and patterns. Based on this principle, the Council will be certain that it is only storing the minimum amount of data required for its purpose.

4. Data is accurate and, where necessary, kept up to date ('accuracy')

Under the DPA the data held shall be accurate and, where necessary, kept up to date. This is not an absolute and unqualified right and the data controller is only required to take reasonable steps to ensure the accuracy of the data. The GDPR requires the same standard as under the DPA, however the qualification of 'reasonableness' is now expressly contained within the principle.

This principle requires data controllers to make sure information remains accurate, valid and fit for purpose. To comply with this principle, the Council has privacy notices in place to address how it will maintain the data it is processing and storing.

5. Data not to be kept longer than is necessary for the purposes ('storage limitation')

The DPA requires that data is not held for longer than is necessary, but that data held for statistical or historical purposes can be kept indefinitely. The GDPR follows the DPA but expands on the list of exemptions to this principle. The GDPR permits the storage of data for longer periods than necessary where the data is being processed for archiving purposes in the public interest and/or scientific purposes, this is in addition to the statistical or historical purposes covered in the DPA.

This principle discourages unnecessary data redundancy and replication and limits how the data is stored and moved. In addition, it requires the understanding of how the data subject would be identified if the data records were to be breached. To ensure compliance, the Council has control over the storage and movement of data, which includes implementing and enforcing the Records Management and Retention Policy and not allowing data to be stored in multiple places.

6. Appropriate technical and organisational measures against unauthorised or unlawful processing, loss, damage or destruction ('integrity and confidentiality')

The GDPR covers the same requirement as already held within the DPA with regards to technical and organisational measures needed to protect against any identified risks.

This principle protects the integrity and privacy of data by making sure it is secure (which extends to IT systems, paper records and physical security). The Council, when collecting and processing data, is responsible for implementing appropriate security measures that are proportionate to the

risks and rights of data subjects. To achieve compliance, please see the Council's Information Security Policy.

There is an additional section related to: accountability and liability ('accountability')

This focuses on compliance and being able to demonstrate that compliance. For example, GDPR requires the Council to respond to requests from data subjects regarding what data is available about them, which includes having a process in place to manage a request, but also the need to have a full audit trail to prove that it took the appropriate actions.

Incident Management
This applies to incidents affecting the Council's information assets or information systems. The Council is committed to effective information security management to protect the confidentiality and integrity of its information assets, to safeguard the reputation of the Council and to fulfil its legal and regulatory obligations.

These categories cover a range of incidents and breaches. For example:

- **Site Breach -** This could include unauthorised access to the site, with the intent to cause criminal damage.

- **Network Breach -** This could include network violation and/or breach of firewalls.

- **Security Hardware Incident** - This could include a failure with any site security hardware including cameras, gates, doors, failure of firewall, etc.

- **Building Incident** - This could include a problem within the offices, such as fire or flood.

- **Area Breach within the building -** This could include person or persons intentionally gaining access to areas within the building they are not authorised to be in.

- However, there are also many other incidents, which could affect security, such as, loss of ID badge/s, misplaced or missing USB sticks, mobile phones, password disclosures, computers left unlocked when unattended, etc.

Please see 'Reporting an Incident Management Breach' further in the Policy.

Roles and Responsibilities

Organisational Responsibilities
North Kesteven District Council is a data controller under the GDPR. The Council as an organisation is responsible for compliance with the GDPR.

Data Protection Officer
The responsibility for compliance with the GDPR and incident management is delegated to the Data Protection Officer (DPO). The DPO supports the implementation of this Policy and takes day to day responsibility for its operation. As part of the GDPR, the Council is required to appoint a DPO, who is responsible for the following activities:

- Keeping senior management informed on data protection matters
- Monitoring the Council's compliance
- Documenting, maintaining and developing policies and related procedures
- Educating employees on their responsibilities
- Providing advice on data protection impact assessments
- Embedding ongoing privacy measures into corporate policies and day-to-day activities

- Being the first point of contact for Subject Access Requests, deletion requests and queries from data subjects
- Checking and approving contracts (in conjunction with Procurement Lincolnshire) with third parties that process personal data to ensure they are compliant with GDPR before commencing the contract
- Working closely with ICT to ensure all systems, services and equipment used for storing personal data meet acceptable security standards
- Developing privacy notices to reflect lawful basis for fair processing, ensuring that intended uses are clearly articulated, and that data subjects understand how they can give and withdraw consent, or else otherwise exercise their rights in relation to the use of their personal data
- Co-operating wherever necessary with the relevant supervisory authority.

Heads of Service and Managers
Heads of Service and Managers, as data controllers for their Division and Teams, will retain a service responsibility for ensuring compliance with the provisions of the GDPR. Their main roles will be:

- Monitor compliance within their Division/Team
- Monitor compliance by external service providers who are processing personal data
- Ensure their Division/Team process and extract data in relation to subject access requests
- Ensure their Division/Team complies when there is a suspected data protection breach/incident management breach.

All Employees and Elected Members
Every employee and elected Member must comply with this Policy when using personal data controlled by the Council. All employees and elected Members are individually responsible for ensuring that their collection, storage, processing and destruction of data are in accordance with the GDPR. All employees should ensure paper files and other records or documents containing personal, confidential and sensitive data are kept in a secure environment. All employees are responsible for being aware of, and complying with, the disposal of confidential waste in the area in which they work. For further information on disposal of confidential waste, please see the Council's Confidential Waste Policy.

Personal data held on computers and computer systems are protected by the use of secure passwords and individual passwords should be such that they are not easily compromised. It is a criminal offence to access personal data held by the Council for other than Council business, or to procure the disclosure of personal data to a third party. It is a further offence to sell such data.

Employees who experience or discover a data loss are responsible for reporting it as soon as possible to their line manager and DPO. As previously detailed, the DPO will work with the line manager to assess the risk and will have primary responsibility for investigating the incident and ensuring that steps are taken to address this for the future. All relevant employees will be responsible for assisting the DPO during this investigation. Relevant employees play an important role in providing information about the data which has been lost.

Contractors/Partners
All contractors, partners and other agents of the Council must ensure that they and their employees who have access to personal data held or processed for or on behalf of the Council are aware of this Policy and are fully trained in and are aware of their duties and responsibilities under the GDPR.

Data Subject Rights
The GDPR grants citizens certain rights in relation to their personal data. The rights are:

1. Right to be informed

Under the GDPR, each data subject has the right to be given information about how their data is being processed and why. When the data controller is asking for a data subject's consent, the data subject needs to understand all the details regarding the processing. All information supplied to a data subject should be concise, intelligible, easily accessible, free of charge and written in plain language.

2. Right of access

Under the GDPR, data controllers must, on request, confirm if they process a data subject's personal data, provide a copy of that data and provide supporting (and detailed) explanatory materials. The request must comply without undue delay and, at the latest, be met within one month (with extensions for some cases) and any intention not to comply must be explained to the individual.

3. Right to rectification

Under the GDPR, data subjects can require a data controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data is incomplete, a data subject can require the Council to complete the data or to record a supplementary statement.

4. Right to erasure

Data subjects have the right to have their data 'erased' in certain specified situations (often known as 'the right to be forgotten'). The right can be exercised against data controllers, who must respond within one month, although this can be extended in difficult cases. This can used when data is no longer necessary for the purpose for which it was collected or processed. In addition, it can be used if a data subject withdraws consent to processing (and if there is no other justification for processing).

5. Right to restrict processing

Data subjects have the right to 'block' or suppress the processing of their personal data. When processing is restricted, the data controller is permitted to store the personal data, but not further process it. For example, when a data subject contests the accuracy of the personal data, the data controller should restrict the processing until it has verified the accuracy of the personal data.

6. Right to data portability

Data subjects can demand that their personal data be ported to them in a machine readable format. This allows data subjects to obtain and reuse their personal data for their own purposes.

7. Right to object

Three rights to object are provided within the GDPR and all relate to processing carried out for specific purposes. Therefore, there is no right for a data subject to object to processing in general. Data subjects have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

8. Rights to automated decision making, including profiling

Data subjects have the right not to be subject to a decision based solely on automated processing which significantly affect them (including profiling). Such processing is permitted where:

- it is necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.

The Data Protection Officer has overall responsibility for ensuring that the rights of data subjects are respected.

Transfer of Data

Transfer of personal data to recipients outside of the European Economic Area (EEA) continue to be regulated and restricted in certain circumstances. The EEA includes EU countries and also Iceland, Liechtenstein and Norway. In addition, the US safe Harbor Scheme is no longer valid. However, in July 2016, the European Commission formally adopted a decision confirming the adequacy of its replacement, known as the EU-U.S. Privacy Shield.

Data Protection on a Day to Day Basis

On a day to day basis, there are a number of things which all employees and Members should be aware of when dealing with personal data:

• When personal data is collected, the form used for collecting should clearly state who the data controller is; what purpose(s) the data is being collected for; and if the data is to be passed to a third party and who that is

• Data should never be used for a purpose it was not collected for without seeking the consent of the individual.

• The Act covers paper-based records as well as those held on computer and extends to other media, such as, CCTV.

• There is a requirement for robust records management with appropriate retention schedules for different record types.

• Data should never be disclosed to a third party without seeking the consent of the individual.

• The principles should always be adhered to when processing personal data.

• The police and other organisations may use exemptions to access data the Council holds.

Personal Data

This Policy applies to all processing of personal data held by the Council. This includes:

- Personal data processed by the Council
- Personal data controlled by the Council, but processed by another organisation on the Council's behalf
- Personal data processed jointly by the Council and its partners.

Personal data may be held in many forms including:

- Database records
- Computer files
- Emails
- Paper files
- CCTV and video recordings
- Sound recordings
- Photographs
- Microfiche and film
- Corporate website.

Data subjects may include:

- current, past and prospective employees
- suppliers

- clients
- customers
- service users
- others with whom the Council communicates.

Deceased individuals are not classified as data subjects under the GDPR, therefore processing of this type of data is outside the scope of this Policy (please see the Freedom of Information Policy).

Controls and Procedures
The Council needs to ensure that appropriate controls and procedures are in place to ensure compliance with the GDPR:

Collecting and Processing Personal Data
The General Data Protection Regulations increases individuals' rights on personal data meaning the Council will need to have consent, or one of five other specific legitimate reasons to hold and process individuals' data. The Council will collect and process personal data only to the extent that it is needed to fulfil operational needs or to comply with legal requirements. GDPR also stipulates the right of citizens as detailed previously in this Policy.

The central aim of the GDPR is to ensure individuals are able to control their own personal data. Therefore, the GDPR stipulates that any individual the Council holds data on must give their explicit and 'informed' consent for their data to be retained for a set period of time and processed. This means the individual must be made aware of how their information is protected, what it is being used for, and what the risks are. Valid consent has to be specific, informed, unambiguous and freely given, which means that individuals cannot be chased or unduly pressed for their consent. The GDPR makes it clear that consent must be a positive indication of the individual's agreement to process their personal data and consent cannot be inferred from pre-ticked boxes or inactivity. In addition, the individual must have the right to withdraw consent at any time. This is not a new obligation under the GDPR, but the quantity of information that needs to be provided has increased, which includes:

- the legal basis for processing the data
- the period for which the data shall be retained
- that the individual has a right to complain to the Information Commissioner's Office
- whether there is a statutory or contractual requirement to provide the data
- the consequence of not providing the data.

When sensitive data is collected, the Council will need explicit and specific consent for the exact purpose or purposes for which any of the sensitive personal data will be used the individual's explicit consent for this processing.

Data Protection by Design and Default
To ensure that all Data Protection requirements are identified and addressed at the start of each project or process and/or when reviewing or expanding existing services, each of them must go through an approval process before continuing. This approval process consists of the completion of a Data Protection Impact Assessment (DPIA). This is a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy, and protect against the risk of harm through use or misuse of personal information. A DPIA will enable the Council to identify issues at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. The subsequent findings of the DPIA must then be submitted to the DPO for review and approval.

Privacy Notice
The Council aims to ensure that individuals are aware that their data is being processed. The GDPR aims to ensure privacy notices will be:

- Concise, transparent, intelligible and easily accessible
- Written in clear and plain language, particularly if addressed to a child
- Free of charge.

These requirements are intended to ensure privacy information is clear and understandable for data subjects. The explicit emphasis on adapting privacy notices for children goes beyond what is currently required by the DPA.

Data Quality and Retention
Personal data held will be relevant to the stated purpose and the Council will ensure that the information held is accurate and up-to-date. The Council's use of personal data will comply with the Records Management and Retention Policy and information will only be held for as long as is necessary after which the details will be deleted or destroyed. Where details of individuals are stored for long-term archive or historical reasons, and where it is necessary to retain the personal detail within the records, it will always be done within the requirements of the GDPR.

Data Protection Officer
Under the GDPR, the Council must have a named Data Protection Officer who is responsible for data protection matters. Within North Kesteven District Council, the Data Protection Officer is the Corporate Information Manager.

Data Security
The Council will endeavour to implement appropriate technical and organisational security measures so that unauthorised employees and other individuals are prevented from gaining access to personal information. An employee must only access personal data they need to use as part of their role. All employees will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

Types of Breach
Security is more than a Data Protection issue because it covers the wider security of all Council facilities. There are direct linkages with the Council's Information Security Policy, as it relates to all Council facilities and systems. The Council is required to take all reasonable measures to ensure the personal information is held securely. Security in some instances may involve encrypted and password protected devices or files. In other instances, it may require paper files to be kept in locked cabinets. In addition, personal information should not be left on an unattended desk or overnight.

A data breach is any incident involving the loss of personal information that could have an impact on individuals. The data breach includes electronic, media and paper records and it can also mean inappropriate access to information.

Data protection breaches could be caused by a number of factors. Some examples are:
- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Human Error;
- Unforeseen circumstances such as fire or flood;
- Hacking;
- Offences where information is obtained by deception.

Reporting a Data Protection and/or Incident Management Breach:
By adopting a standardised consistent approach, we aim to ensure that breaches and/or incidents are:
- Reported in a timely manner and can be properly investigated

• Are handled appropriately by authorised personnel (namely the DPO)
• Are recorded and documented
• The impact is understood and action taken to prevent further damage
• Data subjects and/or external parties are informed as required
• Are dealt with in a timely manner and are reviewed to identify future improvements.

Throughout the breach management process, records will be kept of what action has been taken and by whom. In addition, a data breach log will be utilised to record this information, including any copies of correspondence.

As a corporate approach, when a breach occurs, the following steps are to be followed (please see Appendix 2A for examples of breaches/incidents):

Initial Reporting
The person who discovers a breach must inform their line Manager and the Data Protection Officer (DPO) immediately. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable. All relevant employees must co-operate promptly with their line manager and DPO to avoid any unnecessary delays, which includes completing the Breach/Incident Report Form at Appendix 2B as quickly as possible. This will also help determine whether a data breach has occurred and the urgency of response required. If in doubt, it is better to report a suspected incident by contacting dataprotection@n-kesteven.gov.uk.

The information in the form will provide key details of the breach/incident, including a description of what happened, when it occurred and any immediate action taken. The DPO will be able to provide advice and assistance when completing the form and, once received, the breach will be logged corporately.

As part of the initial reporting process, the line Manager and DPO must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant employees.

Assess Risks
All data and incident breaches must be managed according to their risk, and the 'Data Protection Incident Levels' found in Appendix 2C should be utilised to help determine this. However, an incident level may change once the full facts and impact has been determined, therefore the status of the breach will be kept under review accordingly.

In addition, Appendix 2C provides the line manager with further questions that can be used to assess the risk level, whilst providing further information to the DPO to understand the sensitivity of the data and the number of individuals whose data has been compromised. As above, the DPO will provide guidance and assistance when reviewing the data protection incident level and associated risks.

Managing the Breach
If it is concluded that a breach has occurred, the line Manager and DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

- Attempting to recover lost equipment
- Contacting the Council's Contact Centre, Benefits or other relevant Council Departments, so that they are prepared for any enquiries asking for further information
- Contacting the Communications Team so that they can be prepared to handle any press enquiries
- The use of back-ups to restore lost/damaged/stolen data
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use

- If the data breach includes any entry codes or passwords, then these codes must be changed immediately, and the relevant agencies and employees informed
- Use of backup equipment to restore lost or damaged data or ensuring that employees recognise when someone tries to use stolen data to access accounts
- Where appropriate, inform the police.

The DPO will also contact ICT, particularly if there is an actual or potential security risk arising from an incident involving IT systems or equipment. For example, this could include lost or stolen IT equipment or devices, or unauthorised access to data or systems. In addition, data loss incidents may occur as a result of, or in connection with, major IT incidents (please see the Cyber Resilience Policy). Appendix 2D will also be completed at this stage, which includes actions, such as, identifying whether the breach has been controlled and determining whether anything can be done to recover losses and limit damage caused.

Breach Reporting
Data controllers are required to report a personal data breach to the ICO without undue delay and, where feasible, no later than 72 hours after becoming aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. If a notification is made after the 72 hour period has expired, the Council must explain the reasons for the delay.

As part of the notification to the ICO, this must include:
- a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned;
- the name and contact details of the DPO (or alternative contact);
- the likely consequences of the data breach; and
- measures taken or proposed by the Council to address the breach and/or mitigate its effects.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the Council must communicate the breach to individuals' without undue delay. The communication of any data security breach must be handled with care and sensitivity and must describe in clear and plain language the nature of the breach and at least provide the following information:
- the name and contact details of the DPO (or alternative contact);
- the data involved, plus the likely consequences of the data breach
- advice on what steps they should take, for example, contacting their bank;
- measures taken or proposed by the Council to address the breach and/or mitigate its effects and how the Council will keep them informed.

However, the DPO and line manager will review whether notification to the data subject is necessary, particularly where any of the following conditions have been met:
- technical and organisational measures have been applied to the personal data which will render it unintelligible to unauthorised persons (such as encryption);
- the Council has taken steps to ensure the originally high risk is no longer likely to materialise; or
- to notify each individual would involve disproportionate effort, in which case a public communication or other method of information is used which would inform the affected data subjects in a similarly effective manner.

Where a breach is reported to the ICO and not to the data subjects, the ICO may require the Council to notify affected individuals anyway.

Please see Appendix 2E for a more detailed form to be completed with regards to breach reporting.

Breach Investigation
In most cases, the next stage would be for the DPO to fully investigate the breach, which will consider the following (of which most will have been documented throughout this process):

- How many people are affected and who (e.g. residents, suppliers, tenants)
- Type of data
- Sensitivity of the data
- Potential effect on the individual
- What protections/safeguards are already in place (e.g. encryption)
- What happened to the data
- Whether the data could be put to any illegal or inappropriate use
- Whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as soon as possible. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Review, Evaluation and Lessons Learned
The DPO should fully review both the causes of the breach and the effectiveness of the response to it. The breach may highlight remedial action required in relation to procedures, additional training requirements, IT systems and so on. Any agreed actions and target dates for completion will be recorded on Appendix 2F. If systemic or ongoing problems are identified, then an improvement action plan must be drawn up.

To view the data breach process, please see Appendix 2G.

It should be noted that there could be the recommendation of the pursuance of the relevant disciplinary procedure for employees where the circumstances of a particular incident make it appropriate to do so. Any such recommendation will be made to the Human Resources Team.

Breach Reporting Obligations on Data Processors

Data processors are required to notify data controllers of a personal data breach without undue delay.

Sanctions for Non-Compliance
Failure to comply with breach reporting requirements under the GDPR will result in regulator scrutiny, negative PR and, possibly, loss of business (dependent on the role of the Division and loss of data). There are also financial penalties, including up to 2% of annual global turnover or 10 million Euros, whichever is higher.

Subject Access Request
Under the GDPR, an individual has a right of access to information held about them by any organisation and to receive a response within one month, which is known as the Right of Subject Access. North Kesteven District Council will ensure that the right of subject access to information held by the Council can be fully exercised by everyone. However, a Subject Access Request (SAR) only relates to personal data, and not to information relating to other people.

A SAR must be made in writing and enough information must be provided to judge whether the person making the request is the individual to whom the personal data relates. This is to avoid personal data about one individual being sent to another, accidently or as a result of deception. However, until the identification has been received, the Council will not process a request. The

Council has one month (which we can extend in some circumstances) to respond to the request. A person will be required to confirm their identity and will usually be asked to provide the following:

- Full Name
- Address
- Date of Birth
- One Photographic piece of Evidence, such as, Passport, Driving Licence with photograph, Travel Pass with photograph

and

- One Other piece of Evidence, such as, Council Tax Bill, Utility Bill, Bank/Building Society Statement, Birth Certificate.

If a request is submitted to the Council, the individual is entitled to be told free of charge whether the Council holds any data about the person. If the Council does, the individual has the right:

- To be given a description of the data, the purposes for which the data are being processed, and those to whom the data may have been disclosed;
- To be given a copy of the data in an intelligible form enabling them to port the data to another provider, with any unintelligible terms explained;
- If there is a specific request, to be given an explanation as to how any decisions taken about an individual solely by automated means have been made;
- To have more power to withdraw their consent and have their data amended or deleted, known as the 'right to be forgotten'.

However, it must be noted that some records cannot be deleted, even if the data subject has asked to 'be forgotten'. This might be for reasons of financial regulatory compliance, or because the Council can show it has 'legitimate' reason for retaining and processing the data. In this instance, the Council may need to pseudonymise or anonymise the data the Council cannot legitimately delete to be compliant, but these will be reviewed on a case by case basis.

These rights apply to electronic data and to data in 'manual' (i.e. non-electronic) formats. If a request is for information other than information about themselves, such as information about decisions or actions by the Council, these cannot be submitted as a Subject Access Request. This would be a request under Freedom of Information legislation or Environmental Information Regulations.

The Council has a duty to protect the Data Protection rights and other legal rights of other individuals when we respond to SARs. Information which does not relate to the individual who submitted the request may be redacted, particularly if it relates to other individuals. Sometimes the Council may not be able to release data relating to the individual who submitted the request because doing so would also reveal information about other persons who have not consented to their data being released, and it would not be reasonable in the circumstances to release the data without their consent. In such cases, the individual who submitted the request will be informed that data about them has been withheld and the reasons for doing so.

Making a Request

SARs should be submitted to the Corporate Information Team via:

- FOI@n-kesteven.gov.uk or
- North Kesteven District Council, Corporate Information Team, Kesteven Street, Sleaford, NG34 7EF.

Disclosure and Sharing

Third Party Access to Information

Where a request for personal data is made by a third party on behalf of an individual it shall be treated as a SAR. Evidence is required that the third party is entitled to act in this way, such as a written statement from the individual or an enduring power of attorney. Appropriate professionals may need to be consulted before a decision to release the personal data is made.

When there is a specific reason for requesting the information, an exemption under the Act may apply. Examples are where information is required for the prevention or detection of crime; apprehension or prosecution of offenders; or assessment or collection of tax or duty. If an appropriate exemption under the Act applies so that the Data Protection principles will not be breached, the Council will usually comply with the request. However, without a Court Order there is no obligation on the Council to disclose the information.

Information Sharing
Information sharing is the sharing of sensitive and/or personal information in a closed way, between or within organisations. In instances of sharing, in order to comply with the GDPR and other relevant legislation, the Council are responsible for giving individuals' clear and adequate information about how their information will be protected.

Council will give consideration to the following before sharing personal data with third parties:

- whether the Council has the power to share the information, for example, where consent is the basis for sharing, the DPO will review how this has been obtained and recorded;
- whether the sharing can be justified;
- whether the sharing is to be carried out on an ad hoc or systematic basis;
- whether an information sharing agreement should be created; and
- how to ensure the security of information being shared.

A log of Information Sharing Agreements involving Council services will be maintained by the DPO.

Appeals and Complaints
Where a requester is dissatisfied with a decision or the handling of their SAR they are entitled to an independent internal review of the decision by contacting the Corporate Information Team or by emailing foi@n-kesteven.gov.uk. Reviews relating to requests will be dealt with within 20 working days of a written complaint being received by the Council. The Information Commissioner is unlikely to investigate any complaint about the Council's handling of a request unless the complaints procedure has been exhausted. After the Council's internal review procedure has been exhausted, further reviews about the same information request must be directed to the Information Commissioner for adjudication.

Demonstrating Compliance
Meeting the obligations of the GDPR will be an ongoing process, however the Council will be implementing a range of measures to demonstrate compliance, including:

- Maintain documentation/evidence of the privacy measures implemented and records of compliance
- Regularly test the privacy measures implemented and maintain records of the testing and outcomes
- Use the results of testing, other audits, or metrics to demonstrate both existing and continuous compliance improvement efforts
- Keep records showing training of employees on privacy and data protection matters.

Policy Review

This Policy will be formally reviewed on an annual basis to ensure it continues to be relevant and current. In some circumstances it may be necessary to review this Policy more frequently in response to specific events.