CORPORATE AND COMMUNITY SERVICES

Data Protection Policy

DECEMBER 2019

North Kesteven
DISTRICT COUNCIL

Date of publication:	April 2018
Reviewed & updated:	December 2019
Next review:	December 2021

Alternative Formats

This document can be made available in large print, braille, audio tape, electronic formats such as CD, or in an alternative 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)

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

Contents

1. 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) and the Data Protection Act (DPA) 2018, which came into force on the 25 May 2018, and provided new rights to individuals concerning personal data.

The purpose of the GDPR and DPA is to regulate the way that personal information about living individuals is obtained, stored, used and disclosed. It grants rights to individuals to see data stored about them and to require modification if the data is incorrect and deletion of records (also known as 'the right to be forgotten'). These provisions amount to a right of privacy for the individual. Data protection legislation requires that all processing of personal data must be notified to the Information Commissioner's Office, who is the supervisory authority, and that personal data must be kept and used in accordance with the provisions of the GDPR and DPA.

The 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 data protection legislation. The Council is fully committed to compliance with the requirements of the GDPR and DPA and understands it is essential that it treats personal information lawfully and fairly.

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.

Purpose of the Data Protection Policy
The purpose of this Policy is to explain how the Council will ensure compliance with data protection legislation 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, elected Members, colleagues and partners) whilst ensuring transparency about how it stores and processes individuals' personal data.

Purpose of the General Data Protection Regulations (GDPR) and the Data Protection Act (DPA) 2018
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.

The Data Protection Act (DPA) 2018 also came into effect on that date, which is the UK implementation of the EU's GDPR legislation, codifying its requirements into UK law. However, the GDPR allows 'derogations' – limited opportunities to make provisions for how it applies in individual countries. However, these are generally kept within certain scenarios, for example, national security, crime and legal proceedings, but should still be in the spirit of the GDPR and define the purpose and scope of the processing, including safeguards, in relation to personal data.

The DPA 1998 was repealed and has been superseded by the DPA 2018. In addition, the GDPR will be retained in domestic law at the end of the transition period, however the UK will have the independence to keep the framework under review. Currently, the GDPR and DPA 2018 are read side by side when considering the application of data protection legislation.

2. Definitions

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

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 and DPA. Data protection legislation places additional emphasis on meeting contractual obligations with the processor to ensure they also comply with the GDPR and DPA.

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, data protection legislation 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 and DPA. 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 data protection legislation. In addition, it manages the notification process, handles queries and complaints and enforces the terms of the GDPR and DPA.

Personal Data
The GDPR and DPA make a distinction between personal data and special category 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. Please see 'Special Category Data' for more information.

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.

Special Category Data
Special category data is personal data that is subject to stricter conditions of processing. The GDPR and DPA define special category data as:

- Personal data revealing racial or ethnic origin
- Personal data revealing political opinions
- Personal data revealing religious or philosophical beliefs
- Personal data revealing trade union membership
- Genetic data
- Biometric data (where used for identification purposes)
- Data concerning health
- Data concerning a person's sex life
- Data concerning a person's sexual orientation.

The GDPR rules for special category data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures.

3. Data Protection Principles

The GDPR and DPA introduced six principles to replace the eight found in the Data Protection Act 1998, which relate to the collection, use, processing and disclosure of personal data. These Principles are listed below:

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

Under data protection legislation, a data controller is required to process the data fairly and lawfully. The GDPR and DPA also require the data controller to make available to the data subject certain specific information whereas, previously, there was no express obligation to process the data transparently. The inclusion of the principle of transparency is a new provision in the GDPR and DPA and 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 also provide details surrounding the data processing when requested by the data subject.

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')

These principles remain largely the same as under previous data protection legislation. However, the GDPR and DPA also permit 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 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 GDPR and DPA strengthen this requirement, as it raises the threshold from a data controller only being able 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 and, based on this principle, it will only store the minimum amount of data required for its purpose.

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

The GDPR and DPA requires the same standard as set under previous data protection legislation, 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 its processing activities.

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

The GDPR and DPA follows previous data protection legislation, however expands on the list of exemptions to this principle. The GDPR and DPA permit 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, which is in addition to the statistical or historical purposes covered in the previous 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 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 and DPA covers the same requirement held within previous data protection legislation with regards to technical and organisational measures needed to protect against any identified risks.

This principle protects the integrity and privacy of data by ensuring it is secure (which extends to ICT 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 also see the Council's Information Security Policy, which is available on the corporate website.

There is an additional section within the GDPR and DPA related to: accountability and liability ('accountability')

This focuses on compliance and being able to demonstrate that compliance. For example, adopting and implementing data protection policies, maintaining documentation of processing activities, implementing appropriate security measures, recording (and where necessary reporting) personal data breaches and carrying out data protection impact assessments.

4. Data Subject Rights

The GDPR and DPA grants citizens certain rights in relation to their personal data. The rights are:

a. Right to be informed
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.

b. Right of access
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 potentially detailed) explanatory materials. The request must comply without undue delay and, at the latest, be met within one calendar month (with extensions for some cases) and any intention not to comply must be explained to the individual.

c. Right to rectification
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.

d. 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 calendar 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).

e. 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.

f. 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.

g. Right to object
Three rights to object are provided within the GDPR and DPA 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.

h. 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.

5. Data Protection on a Day to Day Basis

a. Overview
On a day to day basis, there are a number of areas which colleagues and elected Members should be aware of when processing 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.
• This includes paper-based records, as well as information held electronically, and extends to other media, such as, CCTV.
• There is a requirement for robust records management with appropriate retention periods for different record types.
• Data should never be disclosed to a third party without seeking the consent of the individual (however this could depend on whether an information sharing agreement and/or contract is in place)
• The data protection principles should always be adhered to when processing personal data.

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

b. 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 and DPA, therefore processing of this type of data is outside the scope of this Policy (please see the Freedom of Information Policy, which is available on the corporate website).

c. Data Protection Impact Assessment

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. Please see the DPIA Guidance, which is available on the corporate website.

d. Collecting and Processing Personal Data

The GDPR and DPA increases individuals' rights on personal data meaning the Council will need one of six lawful bases 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. The GDPR and DPA also stipulates the right of citizens, as detailed previously in this Policy.

Organisations must have a valid lawful basis in order to process personal data. There are six lawful bases under the GDPR and DPA:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests.

e. Privacy Notice

The Council aims to ensure individuals are aware that their data is being processed. The GDPR and DPA 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 to data subjects.

f. Data Quality and Retention

Personal data held will be relevant to the stated purpose and the Council will ensure that the information 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 and DPA (please see the Records Management and Retention Policy, which can be found on the corporate website).

g. Data Security

i. Access

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. Further information can be found in the Records Management and Retention Policy and Information Security Policy.

ii. 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 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.

iii. 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 and mobile phones, password disclosures, computers left unlocked when unattended, etc. Please see the Data Breaches and Incidents Policy for detail on the breach reporting process, which is available on the corporate website or by contacting the DPO at: dataprotection@n-kesteven.gov.uk.

6. Information Sharing

Data sharing across and between organisations can play a crucial role in providing a better, more co-ordinated and efficient service to customers. The Council recognises the importance of sharing information with appropriate third parties in order to

maximise public service delivery and to meet its statutory responsibilities. In addition, sharing information about individuals between public authorities is often essential when it is needed to keep people safe or ensure they receive the best services.

However, this sharing must only happen when it is legal and necessary to do so and adequate safeguards need to be in place to protect the security of the information. The Council understands that it is important that residents' remain confident that their personal information is kept safe and secure and that Council employees maintain the privacy of individuals.

The 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.

The DPO will retain a central repository of all Council ISAs and a log will be kept of all decisions to share personal data, including the reasons for the decision and legal basis.

Data sharing, giving personal data to a third party, can form an essential part of service delivery and meeting people's needs. It may be 'systematic', occurring as a routine process, or 'ad hoc', including one off emergency situations. If the information to be shared does not include personal data then the GDPR and DPA do not apply, with sharing only requiring approval from the relevant Manager. However, in all instances, the sharing of personal data must be legal, fair, transparent and in line with the rights and expectations of the individual whose data is being shared (please see the Information Sharing Policy, which is available on the corporate website, and the DPO for further information).

7. Subject Access Requests

Under the GDPR and DPA, an individual has a right of access to information held about them by any organisation and to receive a response within one calendar month (which can be extended in some circumstances) and is known as the Right of Subject Access. The Council will ensure that the right of subject access to information held by the organisation 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 can be made verbally or 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. 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.

Until the identification has been received, the Council will not process a request. However, 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 be able to withdraw their consent and, in some circumstances, 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 it cannot legitimately delete, however 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 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.

a. Making a Request

SARs should be submitted to the Corporate Information Team via:

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

b. 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. Legal advisers 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.

c. 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 DPO or by emailing dataprotection@n-kesteven.gov.uk. Reviews relating to requests will usually be dealt with within 20 working days of a written request being received by the Council. The Information Commissioner is unlikely to investigate any complaint about the Council's handling of a request unless the internal review procedure has been exhausted. After the Council's internal review procedure has finished, further reviews about the same information request would be directed to the Information Commissioner for adjudication.

8. Monitoring

a. Demonstrating Compliance

Meeting the obligations of the GDPR and DPA is an ongoing process, however the Council is 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 colleagues on privacy and data protection matters.

9. Roles and Responsibilities

a. Organisational Responsibilities

North Kesteven District Council is a data controller under the GDPR and DPA. The Council as an organisation is responsible for compliance with data protection legislation.

b. Data Protection Officer

Under the GDPR and DPA, the Council must have a named Data Protection Officer (DPO) who is responsible for data protection matters. Within North Kesteven District Council, the Data Protection Officer is the Corporate Information Manager. The DPO supports the implementation of this Policy and takes day to day responsibility for its operation. The DPO is responsible for the following activities:

- Keeping senior management informed on data protection matters
- Monitoring the Council's compliance
- Monitor compliance by external service providers who are processing personal data
- 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 Information Commissioner's Office.

c. Heads of Service and Managers

Heads of Service and Managers will retain a service responsibility for ensuring compliance with the provisions of the GDPR and DPA. Their main roles will be:

- Monitor compliance within their Division/Team
- 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.

d. All Employees and Elected Members

All employees and elected Members must comply with this Policy when using personal data controlled by the Council. All employees and elected Members are individually

responsible for ensuring their collection, storage, processing and destruction of data are in accordance with the GDPR and DPA. All employees and elected Members should ensure paper files and other records or documents containing personal, confidential and sensitive data are kept in a secure environment. All employees and elected Members 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, which is available on the corporate website.

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 Manager and DPO. As previously detailed, the DPO will work with the Manager and employee 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.

The GDPR and DPA also applies when working from any location outside the District Council offices, whether it is on an ad-hoc or permanent basis. Therefore, it is recommended all employees ensure they have a suitable workspace with adequate security and storage (if required). Therefore, if you have any concerns, please discuss these with your Manager and DPO as to whether it is appropriate to work from these locations.

In addition, the GDPR and DPA must continue to be complied with in relation to the security of information. When processing personal information the same measures apply to remote working as working in the office. Employees should continue to work electronically, where possible, to minimise the risk of information being compromised. Furthermore, employees should continue to lock laptops so that information is hidden when away from a workstation, and information should not be saved on personal hardware.

If employees work with hard copy information (for example, printed forms, plans, notebooks), please ensure the following:

- Ensure information is secured whilst away from a workstation or overnight (including the consideration of using a lockable draw or briefcase)
- Ensure your colleagues know you have removed the information from the District Council offices to a remote workstation and ensure this is recorded
- Ensure that a workstation is not at risk of being overlooked, including angling your workstation so that your laptop screen cannot be seen from outside
- If making amendments to personal information, ensure other service providers are aware so that the Council is only using up to date information

- Never dispose of paper that is work related through normal domestic rubbish. Any personal, confidential and sensitive documentation must be returned to the office for disposal or shredding (when it is possible to do so)
- Ensure if you are discussing personal information in a Teams meeting or telephone call you cannot be overheard from outside your location or place of work. Consider closing windows or moving to another room whilst you make the call.

e. 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 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 and DPA.

10. 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.

North Kesteven
DISTRICT COUNCIL

District Council Offices, Kesteven Street, Sleaford, Lincolnshire NG34 7EF
Telephone Number: (01529) 414155
180912-JA2