Data Protection Policy

Version:	1-3
Ratified by:	Senior Management Group
Date ratified:	
Name of organisation/author:	Dan Howarth
Name of responsible committee/individual:	Senior Management Group
Date issued:	
Review date:	
Target audience:	All employees

POLICY DOCUMENT CONTROL PAGE	
TITLE	**Title: Data Protection Policy** **Version: 1-2** **Date: 31 October 2019** **Reference Number:**
SUPERSEDES	**Supersedes: Data Protection Policy Version 1.1** **Description of Amendments:**
ORIGINATOR	**Originated by:** Dan Howarth – Data Protection Officer **Designation:** **Department / Service: Legal Services**
PROFESSIONAL GROUP APPROVAL	**Referred for approval by:** Data Protection Officer **Referred to (insert name of group/s):** Senior Management Group **Date of Referral: 31 October 2019** **Approved by:** **Date:** **Executive Signature:**
REVIEW	**Review Date: 31 October 2020** **Responsibility of: Data Protection Officer**
QUALITY CONTROL	**Date sent to: N/A** **Quality Control Check Completed:**

HCC STANDARDS LINK	

POLICY CONTROL PAGE (2)

IMPACT ON EMPLOYEES AND POPULATION GROUPS (Including children, vulnerable adults, black and minority ethnic groups, disabled people, men, women and transsexuals):

Equality Impact Assessment: Yes √ □ No □ N/A If N/A please state why:

……..

Date Assessed:

Manager/Group responsible:

Category High □ Medium □ Low □ N/A

Training/Awareness Raising required to fully implement policy: **Yes √ No □ N/A □**. If N/A please state why:

……..

Awareness raising to be conducted during: This will need to be developed as part of training in data protection.

Date:

Provided by:

Date……

1. Introduction

1.1 The General Data Protection Regulation (GDPR) has replaced the Data Protection Act 1998. This legislation tells organisations how to manage personal data that they hold, giving principles and rights that must be upheld. The GDPR encourages a balance between the individual's right to privacy and an organisation's need to conduct legitimate and appropriate operations with personal data.

1.2 Knowsley Council is committed to protecting the privacy of individuals and handles all personal data in a manner that complies with the GDPR. The council has established the following policy to support this commitment. It is the **personal responsibility** of all employees (temporary or permanent), Members, contractors, agents and anyone else using personal data on the Council's behalf to comply with this policy.

1.3 This policy explains what our expectations are when processing personal information. This policy should be read together with the Information Security Policy, Information Security Acceptable Use Policy, Protective Marking Scheme, and the Corporate Records Retention and Disposal Schedule.

2. The Data Protection Principles and Definitions

2.1 The GDPR is concerned with the use (processing) of personal data.

Personal data is information that either on its own, or when combined with other information, can be used to identify a living individual.

Examples of personal data include: - names, addresses, dates of birth, photographs, IP Addresses, Vehicle Registration Plates, CCTV footage.

The GDPR also defines personal data that is more sensitive and must be treated with a higher level of privacy and respect. This is called Special Category Data.

Special Category Data is any data that falls into the following categories: - racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data such as fingerprints, sex history or sexual orientation, any data relating to physical or mental health conditions.

Processing Data This means any use of the personal data. This includes collecting, disclosing, destroying, archiving and organising.

Data Subject is the person who the personal data is about. For example, the children named on a class register at a school are all data subjects of that register.

Data Controller is usually an organisation who dictates the reason and purpose for how data is processed. The Council itself is a Data Controller as it chooses how it collects, uses and shares its own data.

The Information Commissioner's Office (ICO) is the regulator for Data Protection and Privacy law in the UK. They have the power to enforce on organisations for breaches of the Data Protection Act 2018 or the GDPR.

Most notably, the ICO can issue a Monetary Penalty for serious and significant breaches. Under the General Data Protection Regulation this can be up to €20 Million or 4% of a company's global turnover.

2.2 The Principles

The GDPR contains a number of Principles that must be met in order to use personal data in line with the law.

Personal Data must be: -

1. Processed Fairly, Lawfully and Transparently
2. Processed for a Specified and Legitimate Purpose
3. Adequate, Relevant and limited to what is relevant
4. Accurate and up to date
5. Kept no longer than necessary
6. Stored securely using technical and organisational measures

Principle One – Fair, Lawful and Transparent

Fair and Transparent

When the Council collects personal data from an individual, we must tell them of what we intend to do with data once we have it.

This is called a Privacy Notice.

The Privacy Notice must include information such as – what the personal data will be used for, who it will be shared with and how long it will be kept for.

The Privacy Notice must be given to the data subject as soon as possible when collecting their information and this can be done online, through the post or in the form of a recorded voice message. As long as the Privacy Notice is provided, it can take any form necessary.

The Privacy Notice template can be found on Bertha.

Lawful

To use personal data lawfully, the Council must ensure that no laws are broken when we use the data. This means we cannot use data to break any other laws within the UK or Europe.

As well as this, the Council must meet what is called a condition for processing when using the information. The conditions for processing are explained below. There are six of them and are all equally valid.

The Council can use information if we can meet one of the following conditions:-

- The data subject has consented to their information being used. This consent must be specific, informed and freely given. The data subject must know what they are consenting to and be given a genuine choice, before consent can be classed as appropriately obtained.

- The personal data is being used to perform a contract with the data subject or to undertake actions necessary for creating a contract with the data subject.

- The personal data has to be processed because legislation says that the Council has to. This also applies when the Council receives a court order that demands disclosure of information.

- The personal data is used in line with the vital interests of the data subject. This is usual a life or death situation.

- The personal data is used in line with a public function or legal power that the Council is meeting. For example, the Children's Act 1989 gives the Council the power to look after children at risk of harm. This power also allows the Council to use information to complete this function.

- The personal data is used in the legitimate interests of the Council and does not conflict the rights and freedoms of the data subject. When using this condition, it is best to consult with the Data Protection Officer.

When we use Special Category (sensitive) personal data, we must meet an additional condition. The Data Protection Officer can advise on this.

Principle 2 – Specified and Legitimate Purpose

The Council must only use, collect and share personal data for a specified and legitimate purpose. This purpose must be in line with the Council's aims and values and not contradict any laws or moral obligations.

Once we have collected personal data for a specific purpose, we must only use that personal data for purposes compatible with the original aim.

For example, if the Council collects personal data for a social care purpose, we can use it for other social care purposes such as evaluating the quality of the social care provided. However, we couldn't use social care personal data to inform bin collection timetables as this is not a compatible purpose because it so different to the original purpose for collecting the information.

Principle 3 – Adequate, Relevant and limited to what is necessary

The Council must only use, collect or share the personal data that we need in order to complete the purpose we are trying to achieve.

For example, if the Council only needs to collect a name and address in order to complete the purpose, only the name and address should be collected.

Principle 4 – Accurate and up to date

The Council must ensure that all of its information is as accurate as possible. This means that if we find out something new about a data subject such as a change of address, Council systems are updated as soon as possible to reflect this change.

Inaccurate personal data can lead to breaches, such as letters or emails being sent to wrong recipients or the wrong decisions being made about people.

Principle 5 – Kept No Longer Than Necessary

The Council has a responsibility to ensure that information is retained for the correct amount of time, and no longer. All of the Council's information has a date by which is should be securely deleted or archived. This is written into the Council's Retention Schedule which is available on Bertha.

More information about retention periods and records management can be found on the Records Management pages of Bertha.

Principle 6 – Stored Securely

The Council must take all appropriate technical and organisational measures to keep information secure and prevent it from being lost or put at risk of being seen by people who shouldn't have access to it.

This can take a variety of forms. Examples of technical and organisational measures can be found below.

Technical Measures

- Firewalls

- Anti-virus software
- Encryption
- Secure emails such as GCSX and Egress
- VPNs (Virtual Private Networks)

Organisational Measures

- Policies and Procedures in place to help staff understand their duties under data protection
- Training
- User guides on Bertha
- A more knowledgeable and open culture towards Data Protection

The aim of employing technical and organisational measures is to help staff keep information securely. This is by giving them the technology and the knowledge to know how to safely handle information. In line with this, if you identify any further training or equipment needs for your team, contact your line manager so that they can be arranged.

3. Access and use of personal data

3.1 Access and use of personal data held by the Council is only permitted to employees (temporary and permanent), Elected Members, contractors, agents and anyone delegated access as part of their official duties.

Council information is held on a need to know basis, meaning that unauthorised or inappropriate use of the information is strictly forbidden.

Council employees must only access personal data that they have a professional and legitimate need to see. Just because an employee has access to a specific system does not mean that the employee has the right to access all records within that system. Employees must only access cases or files within their caseloads, or those that are directly relevant.

Any deliberate or malicious access to systems or records will be dealt with in line with the Council's Disciplinary Procedures. There are also a range of criminal offences under the Computer Misuse Act 1990 and in Data Protection law for unauthorised use, obtaining or destruction of personal data. These offences can be punished by up to 12 months in prison or a fine of up to £1,000.

More information about how to handle personal data can be found on Bertha in the Acceptable Use Policy

You have individual responsibility for the way you handle personal data as part of your day to day work. As a Council employee, you are required to keep all information you use secure and confidential.

The general rule when using personal data is, treat it with the respect that you

expect your own personal data to be treated. All staff must ensure that their use of personal data is appropriate and respectful.

Staff Tips for using Personal Data

Handling and using personal data in line with the law is not complicated. The following tips are easy to follow, easy to implement and could make all the difference to your daily work in helping to avoid data breaches.

- Always lock your screen when you leave your desk. This avoids leaving your systems open to access and also stops those nearby reading any personal data you may have left onscreen.
- Clear documents away at the end of the day or when leaving your desk. This stops people who are walking past your desk from reading things they shouldn't.
- Always check for ID when holding doors open for people. It is everyone's responsibility to ensure the security of Council buildings and make sure only authorised staff have access to them.
- Double check when entering information into Council systems. Inaccurate information is the biggest cause of data breaches for the Council. Taking the time to check addresses and phone numbers is a vital part of data handling.
- Double check addresses when sending emails. It is easy to mistype or click the wrong name on Outlook. Once the email has gone, it can't be retrieved. Take the time to get the recipient right before you press send.
- When taking information out of the office, think about the most appropriate way to do so. Council tablets and laptops are encrypted and difficult to access if they are lost. Paper documents are not as secure as they can be read by anyone who finds them.
- If you don't need to print something, don't.
- If you are regularly sending personal information to organisations outside of the Council, check that you have an Egress account so you can send the information securely and view the guidance on BERTHA.
- Take care when working from home. Your family members don't have a right to see the information you use for work.
- Don't leave equipment or documents in your car overnight if you need to take them home. You wouldn't leave your own laptop on the front seat of your car, so don't leave your work on there either.

Using Council Systems

- Just because you have access to a system, this does not mean you have the right to access all of the information on it. Access is on a "need to know" basis.
- "Curiosity" checks are not permitted. You must have a genuine, legitimate work purpose to access information
- Never share passwords. If a colleague forgets their password, they need to have it reset by IT. Do not let them access a system under your username.
- Any information you access on a system will be logged. Do not let colleagues use your computer to retrieve information and do not undertake requests on their behalf.

- Always be professional when using Council systems. Do not input anything derogatory, inappropriate or rude about individuals.

Staff Responsibilities

Senior Management Team

To guide the Council's priorities and policy decisions, including ensuring all Council fucntions comply with relevant legislation, such as the GDPR.

Senior Information Risk Owner

To guide and where appropriate, make decisions with regards to the Council's compliance with the GDPR.

Data Protection Officer

To oversee the Council's compliance efforts with the GDPR. To train and provide advice to the Council's staff with regards to data protection. To monitor, audit and document all data protection measures taken within the Council.

All Staff

To understand the contents of this policy and to ensure they understand their own responsibilities when handling personal data. To take care and minimise mistakes made. To understand how what constitutes a data breach and how to report one.

4. Disclosing personal data

4.1 Personal data must only be shared when the staff member receiving the information is satisfied there is a clear and legal basis for sharing the information.

Knowsley Council staff must ask appropriate questions to ensure the requester (whether internal staff or an external partner) has the appropriate legal reason to see the information they are requesting.

Where necessary, staff members are encouraged to speak to their line manager to ask advice, or contact the Data Protection Officer on 0151 443 (4660)

4.2 When Council staff disclose personal data to another organisation, they must keep a record of what they have shared and why.

This should include;

- a description of the information given;

- the name of the person and organisation the information was given to;
- the date;
- the reason for the information being given; and
- the lawful basis.

4.3 If an Information Sharing Agreement (ISA) exists, this should be adhered to.

4.4 Where Council staff respond to a request for information from another organisation, they must ensure they only share relevant and accurate information.

4.5 When personal data is given internally or externally, it must be shared using a secure method.

- Egress can securely deliver emails to any email address, including Hotmail or Googlemail accounts.
- The Council has developed secure TLS connections with many organisations. A full list is available here.

5. Accuracy and relevance

5.1 It is the responsibility of the staff who receive personal information to make sure so far as possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to make sure that it is still accurate. If the information is found to be inaccurate, steps must be taken to correct it. Individuals who input or update information must also make sure that it is adequate, relevant, clear and professionally worded.

6. Retention and disposal of information

6.1 Knowsley Council holds a large amount of information. The GDPR requires that we do not keep personal data for any longer than is necessary. Personal data should be checked at regular intervals and deleted or destroyed when it is no longer needed, provided there is no legal or other reason for holding it.

6.2 The Corporate Records Retention and Disposal Schedule must be checked before records are disposed of, to make sure that the retention period for the information in question, has been served.

6.3 For specific information regarding retention and disposal of personal data, consult the Council's Records Management page or contact the Council's Records Manager – Liz Diack on 0151 443 3794.

7. Rights of the Data Subject

7.1 Individuals have a number of Rights under the GDPR and they are able to enact them against any organisation at time they choose.

The Rights include: -

- **The Right of Subject Access** – the right to request a copy of data held about them by an organisation and find out how it is used.
- **The Right of Rectification** – the right to ask for inaccurate or incorrect information to be corrected or removed.
- **The Right of Data Portability** – the right to move data from one organisation to another. This could apply when moving bank accounts or energy suppliers.
- **The Right to Be Forgotten (Erasure)** – the right to ask for data to be removed by the organisation that holds it.
- **The Right of Restriction** – the right to stop information being used whilst a complaint is made.
- **The Right of Objection** – the right to ask an organisation to stop using their data. This is particularly used with regards to direct marketing.

7.2 The council has 30 days (one month) to respond to an individual's request to enact their Rights. This is provided the applicant has put their request in writing and suitable identification has been supplied.

7.3 Further information about the rights of the individual can be found in the Council's Information Rights Policy.

8. Reporting security incidents

8.1 As a Data Controller (organisation that owns data), Knowsley Council has a responsibility to monitor and investigate all incidents that occur within the organisation that involve any of the GDPR Principles being breached.

All incidents need to be identified immediately, reported using the Data Breach Report Form which is available on Bertha. All incidents will be investigated by the Information Governance Team.

Where an incident occurs, staff must inform the Data Protection Officer as soon as possible. The Council has a responsibility to report all serious incidents to the Information Commissioner's Office within 72 hours of discovery. This will be done by the Data Protection Officer.

Staff are advised to contain all incidents as quickly as possible, either by retrieving information sent in error, locking down erroneous access or asking accidental recipients of Council data to confirm it has been deleted.

All relevant incidents and risks that are identified should be reported to the Data Protection Officer, regardless of how trivial they may seem. The Council must constantly evaluate and improve its data protection and information security practices to address the new risks it uncovers. This is to stop breaches from occurring or reoccurring as the case may be.

8.2 Specific procedures have been developed for the reporting of all information security incidents and weaknesses. It is designed to make sure that all relevant information is communicated correctly so that timely corrective action can be taken. The following are links to:

- Guidance for employees in reporting an information security incident; and
- Actions for Heads of Service or other senior managers in reporting an information security incident.

8.3 All employees (permanent, temporary and external users) must be aware of the procedures and obligations in place for reporting the different types of incidents and weaknesses which may have an impact on the security of the council's information assets.

9 Data Protection by Design

9.1 The Council will meet the requirements of the GDPR by building data protection into all new projects from the start and employing appropriate technical and organisational measures to keep personal data secure. This will be achieved through completing Data Protection Impact Assessments (DPIAs)

9.2 The Council has installed DPIAs into the Procurement Pipeline, meaning that all new projects must be subject to a DPIA before they can be put out to tender. This step is mandatory and must not be ignored.

9.3 A DPIA is a process of assessing the risks to privacy and to personal data in a project. A DPIA enables the Council to identify risks and problems at an early stage in the project, meaning that changes can be made quickly and without incurring expenses.

9.4 Further information regarding DPIAs can be found on BERTHA.

10 Contact

The Council's Data Protection Officer is available for advice and guidance regarding all aspects of data protection and GDPR. Please contact: -

Dan Howarth
Data Protection Officer
Legal Services
Municipal Buildings
Archway Road
Huyton
L36 9YU

Tel – 0151 443 4660
Email – dan.howarth@knowsley.gov.uk
Data.protection.officer@knowsley.gov.uk