

# Data Protection Policy and GDPR Update

Cabinet Member for Regulatory, Housing & Health – Cllr Angela Lax

Date: 12 November 2020

Agenda Item: Agenda Item 9

Officer Title: Christie Tims – Head of Governance & Performance -  
Monitoring Officer

Local Ward: N/A

Members



**Audit and Member  
Standards Committee**

## 1. Executive Summary

- 1.1 The General Data Protection Regulation (GDPR) was introduced with effect from 25 May 2018. This is the third update members have had on the work undertaken to ensure the Council is compliant with the ongoing requirements of the act.
- 1.2 This report seeks to update the Data Protection Policy last reviewed in May 2018 with relevant links and ownership.

## 2. Recommendations

- 2.1 To receive the report and note the ongoing work to improve assurance of compliance with General Data Protection Regulations (GDPR).
- 2.2 To approve the updated Data Protection Policy at Appendix A and grant delegated authority to the Head of Governance & Performance to undertake minor changes such as job titles and links as necessary in future.

## 3. Background

- 3.1 Data Protection Act 2018 and General Data Protection Regulation 2016 ensure the safe and effective handling of personal data.
- 3.2 Both the Council and its individual Members are required to comply with the requirements, as data controllers. Member training was held in March 2018 and was part of new member induction in May 2019 where members were provided with a copy of the privacy notice they should be using. This was also shared with Parish Councils in January 2020 and reminders are due to go out to members shortly.
- 3.3 The Information Commissioner identified 12 areas to ensure compliance:

### **Awareness**

*Senior Officers and Members should be made aware of the changes under GDPR so that impact and key areas can be identified and managed.*

Refresher training has recently been undertaken by all staff via an on-line module and reports are sent to Leadership team. Regular training will continue to be provided in the future. Data Protection Officer (DPO) to attend Manager's Briefing later this year. This report will update members and an email reminder of the requirements and privacy notice will be sent shortly.

### **Information you hold**

*There is a need to undertake an information audit across the Council and have records of processing activities.*

The work to identify information held and to subsequently produce accurate and effective retention and disposal schedules is on-going and has suffered some disruption due to Covid 19 response.

### **Communicating privacy information**

*Privacy notices should be reviewed and a plan put in place for making any necessary changes.*

All privacy notices were reviewed and refreshed as part of implementation of GDPR to ensure they met the new requirements and are updated as our use of data changes over time. Any new forms of processing (for example tack and trace payments) have specific notices developed and signed off by the DPO.

### **Individuals' rights**

*Procedures should be checked and updated to ensure all the rights individuals have are included.*

These are operating effectively without issues. We have had one request to remove data.

### **Subject access requests**

*Procedures should be updated to allow for the new rules:*

- *generally information should be provided free of charge (there was a standard £10 charge)*
- *Information should be provided within one month (rather than 40 days)*
- *If refusing a request for access, we must tell the person why and set out their rights to complain and to judicial remedy; again there is a time limit of one month to do this.*

The Council does not receive a significant number of such requests. In the last 12 months (May 19 to May 20) 4 have been requested. 3 were responded to in the required timeframe, however a fourth request was not released as it was requested on behalf of the subject and the subject did not give authority to release this information to the third party.

### **Lawful basis for processing data**

*The lawful basis for processing data must be identified, documented and set out on a privacy notice.*

This information is included in each privacy notice and reviewed as our use of data changes over time.

### **Consent**

*How we seek, record and manage consent should be reviewed and refreshed as necessary.*

Where the Council relies on consent to process data (which is generally not the case), the consents have been reviewed and revised as necessary.

### **Children**

*GDPR brings in special protection for children's personal data and its use particularly for online services. The need for consent from either the child (if 16 or over) or the parent/guardian is explicit.*

The Council does not generally process large amounts of children's data (unlike unitary or county councils) but the special protection measures are followed when we do.

### **Data breaches**

*Procedures should be in place to detect, report and investigate a personal data breach.*

Only certain breaches have to be notified to the ICO; where it is likely to result in a risk to the rights and freedoms of individuals e.g. discrimination, damage to reputation, financial loss etc. These breaches are also notified to the individual concerned.

In the last 12 months (May 2019 to May 2020) the council has had 5 recorded breaches, none have been reportable to the ICO. Where issues have occurred we have ensured training has been given and procedures tightened to ensure future breaches are prevented.

## Data Protection by Design and Data Protection Impact Assessments

*It will be a statutory requirement to adopt a privacy by design approach and to use Data Protection Impact Assessments in certain circumstances.*

Guidance on when and how a Data Protection Impact Assessment is needed is available.

### Data Protection Officers

*It will be a statutory requirement to designate someone to take responsibility for data protection compliance, known as the Data Protection Officer (DPO).*

The Director for Legal & Governance at South Staffordshire Council is currently designated as the DPO for the Council and works closely with the Head of Governance & Performance to ensure Data Protection is managed effectively.

### International

There are provisions for those organisations operating in more than one EU state but these are not applicable to the Council.

Even though the UK formally exited the EU on 31 January 2020 we will still adhere to all the EU standards and regulations until new regulations are made. Interim guidance for local authorities in preparedness in the event that the EU decides against providing sufficient GDPR adequacy status to the UK, would make the UK a 'third country' for data protection purposes. Further legal advice is being sought on this issue and how it might affect us.

- 3.4 An audit was undertaken by an external computer auditor in April 2019 which highlighted a number of areas for improvement. The audit highlighted some key areas of ongoing work that will need to be embedded to ensure ongoing compliance. The recommendations were agreed by senior management and a compliance audit tool has addressed a number of the issues raised which included ongoing training, awareness and recording of information assets and processing activity. The original project plan for this has been impacted by Covid response and resources are being identified to improve the pace of this work.
- 3.5 In order to ensure the Council remains GDPR compliant, the following actions were also taken:
- a) A review and update of the Data Protection Policy (Appendix A). These changes relate to the ownership of the document and the links to other documents and policies. There are no substantive changes to the policy.
  - b) Existing 'organisational' and 'technical' measures to ensure that personal data is kept 'safe' are reviewed and revised as necessary.
  - c) Cyber updates are given to leadership team on a quarterly basis identifying issues and progress.
  - d) The Head of Governance & Performance holds the position of Senior Information Risk Owner (SIRO) and completed relevant training in September 2020.

Alternative Options	None, the council must comply with these regulations, however the committee can choose not to receive ongoing reports.
Consultation	We have ongoing support from South Staffordshire District Council legal team regarding current advice and guidance. The DPO has been consulted on this report and update to the policy.

Financial Implications	Resources are currently being identified to allow the ICT team to improve the pace of information audits and support information owners to establish good data housekeeping routines.
Contribution to the Delivery of the Strategic Plan	Data protection contributes to the sound running of the council.
Equality, Diversity and Human Rights Implications	None
Crime & Safety Issues	None
Environmental Issues	None
GDPR/Privacy Impact Assessment	Not required for this report. This policy ensures ongoing compliance and the processes to underpin such assessments.

	Risk Description	How We Manage It	Severity of Risk (RYG)
			State if risk is Red (severe), Yellow (material) or Green (tolerable) as determined by the Likelihood and Impact Assessment.
a)	Legal challenge if no process is in place	Ensure process is in place and regularly reviewed.	Green Likelihood – low / Impact -low
b)	Assurance of processes in place	Issues highlighted in the audits are being addressed. Information Audit resources being sought.	Yellow Likelihood- med/ Impact -low
c)	Data Protection Officer not an LDC employee – opportunity to miss key activities	Ensure that clear agreement exists for the provision of the role and processes in place.	Green Likelihood – low/ impact - low
d)	Data Protection Policy no longer fit for purpose	Regular review of the policy and updated guidance from suitably qualified DPO.	Green Likelihood – low/ impact - low

Background documents

Relevant web links

<https://www.lichfielddc.gov.uk/downloads/file/713/data-protection-policy> current policy

## Data Protection Policy November 2020

Approved by:	AMS
Approval date:	November 2020
Author/owner:	Christie Tims
Review frequency:	2 Years
Next review date:	November 2022
Location:	Governance

# Introduction

Lichfield District Council is committed to complying with both the General Data Protection Regulation (GDPR) 2016/679 and the Data Protection Act 2018. This policy set out the framework Officers and Members must abide by when handling personal data.

As a Council we recognise that the correct and lawful treatment of people's personal data will maintain their confidence in us and will provide for successful business operations.

## 1. Purpose of policy

Protecting the confidentiality and integrity of personal data is something that the Council takes extremely seriously. The Council is exposed to large fines (depending on the nature and severity of the infringement) for failure to comply with the provisions of the GDPR.

## 2. Scope of policy

Both Officers and Members **must** comply with this policy when processing personal data on the Council's behalf, however for ease of reading only Officers will be referred to in the rest of the policy.

Compliance with this policy is **mandatory**. Related policies and procedures/guidelines are available to assist Officers and in complying with GDPR and the new Data Protection Act.

Any breach of this policy or the related policies and procedures/guidelines may result in disciplinary action or action under the Council's Code of Conduct.

## 3. How it relates to/underpins our strategic ambitions

One of our fundamental ambitions is to be a good council that is responsive and customer focused. This policy facilitates a unified and GDPR compliant framework for all Members and Officers when managing and processing customer data. The policy itself is publicly available and will facilitate a high level of confidence for customers whose data we collect, manage and process.

## 4. Policy details

### Common terms and application

**Personal data** - this is any information relating to an identified or identifiable (from information in the possession of the Council or when put together with other information the Council might reasonably access) living individual.

This policy applies to all personal data the Council processes regardless of the media on which that data is stored.

The law (and this policy) applies to:

- 1) personal data processed by automated means such as computers, phones, tablets, CCTV, swipe cards etc. or,
- 2) (structured) personal data held in a 'relevant filing system' for example an employee's personnel file or it is intended to form part of such a file or,
- 3) unstructured personal data.

**Special** personal data is that about an individual's race/ethnicity, political opinions, religious or philosophical beliefs, membership of a trade union, their genetic/biometric data (if used to identify them), health information or information about their sex life or sexual orientation.

**Processing** includes receiving information, storing it, considering it, sharing it, destroying it etc. The Council recognises that the law applies to all processing activities.

A **processor** is a third-party individual/organisation who process personal data on the Council's behalf - to our instructions.

The Council is the **controller** of people's personal data as we determine what is collected, why and how it is used.

The individual who is the focus of the information is known as the **data subject**.

**Consent** means any freely given, specific, informed and unambiguous indication of a person's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

A **data breach** means a breach of Council security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

### **Commitment to the (General Data Protection) Principles**

The Council (through Officers) MUST:

- (a) process personal data **fairly, transparently** and only if there is a **legal** basis to do so.

To comply with this Officers *must* inform individuals when collecting their personal data (concisely and using clear and plain language so that they understand) of the following:

- 1) that the Council is the "data controller";
- 2) our contact details;
- 3) why we are processing their information and in what way the law allows it;
- 4) if we [this will be rare] rely on our 'legitimate interests' for processing personal data we will tell them what those interests are;
- 5) the identity of any person/organisation to whom their personal data may be disclosed;
- 6) whether we intend to process their personal data outside the European Economic Area;
- 7) how long we will store their information, and;
- 8) their rights.

- (b) only collect personal data for **specified, explicit and legitimate** purposes. Officers must not further process any personal data in a manner that is **incompatible** with the original purposes; Officers should be clear as to what the Council will do with a person's personal data and only use it in a way they would reasonably expect.

- (c) ensure that the personal data we collect is **adequate, relevant and limited** to what is **necessary** to carry out the purpose(s) it was obtained for;

Officers should think about what the Council is trying to achieve in collecting personal data. Officers must only collect the personal data that they need to fulfil that purpose(s) and no more. Officers must ensure that any personal data collected is adequate and relevant for the intended purpose(s).

- (d) ensure that the personal data we process is **accurate** and, where necessary, **kept up to date**.

Officers must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Officers must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

- (e) keep personal data in a form that identifies individuals for **no longer than is necessary** for the purpose(s) that it was obtained.

Officers should periodically review what personal data is held and erase/destroy or anonymise that which is no longer needed.

- (f) process personal data (whatever the source) in a manner that ensures **appropriate** security of the same including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

This is elaborated upon in the Council's information security policy/ procedures/guidelines.

### **Accountability**

The Council is responsible for and must be able to demonstrate that it complies with all the above principles. Officers should, always, be mindful of the need to be able to prove that processing is in accordance with the above principles.

### **Legal basis for processing ordinary personal data (article 6)**

The Council (through its Officers) must generally process personal data ONLY if one or more of the following circumstances exist:-

- (a) Where an individual has given [valid- see definition] **consent**;
- (b) Where necessary to **perform a contract** to which the individual is a party or **to take steps** at their request prior to entering into a contract;
- (c) Where processing is necessary for the Council to comply with our **legal obligations**;
- (d) Where processing is necessary for the performance of **a task carried out in the public interest** by the Council or it is in the **exercise of official authority** vested in us;
- (e) To further the Council's [this will be rare] **legitimate interests or those of a third party** except where such interests are overridden by the privacy interests of the individual who is the subject of the information especially if they are a child.

**\*\*Officers must always ensure that they have a lawful basis to process personal data on behalf of the Council before they process it. No single basis is 'better' or more important than the others. Officers should consider and document what basis they are processing under. If an Officer is unsure as to what basis they can rely upon or indeed whether they can lawfully process personal data, then the advice of the Data Protection Officer should be sought\*\***

### **Special personal data (article 9)**

The Council (through Officers) MUST only process this kind of information where circumstances exist such as:

- a) the individual has given **explicit** consent for one or more **specified** purposes;
- b) it is necessary for **employment/social security/social protection law** purposes;
- c) it is necessary in relation to **legal claims**, or,
- d) it is necessary for reasons of **substantial public interest**.

Other grounds are potentially available.



**\*\*Again, if an Officer is unsure as to how to lawfully process special personal data then the advice of the Data Protection Officer should be sought\*\***

### **Crime/offence data**

To process personal data about criminal convictions or offences, the Council must have a lawful basis under article 6 (above) and legal authority or official authority. For further advice speak with the Data Protection Officer.

### **Rights**

Individuals have rights when it comes to how the Council handles their personal data. These include rights to:-

- (a) withdraw consent to processing at any time;
- (b) receive certain information when the Council collects their information or receives it from a third party;
- (c) request access to their personal data;
- (d) have the Council correct inaccurate information;
- (e) ask the Council to erase their personal data;
- (f) restrict the way the Council uses their information;
- (g) be notified about any recipients of their personal data when they have asked for rectification, erasure or restriction;
- (h) object to any processing undertaken by the Council in the public interest/exercise of official authority or in our legitimate interests or those of another;
- (i) object to direct marketing by the Council, and, to
- (j) be notified by the Council of a personal data breach where it is likely to result in a “high risk” to their rights and freedoms.

Procedures exist (which should be followed) if a person seeks to exercise any of the above rights.

### **Restrictions**

In certain circumstances we are permitted to restrict the above rights and our obligations as well as depart from the principles. Any restriction will be in accordance with the law. For further advice speak with the Data Protection Officer.

### **Data protection by design and default**

Taking into account available technology, the cost of implementation of it and the nature, scope, context and purposes of the processing as well as the privacy risks to individuals the Council **MUST** both **at the time we decide how to process personal data and at the time of the processing itself**, implement appropriate technical and organisational measures (such as pseudonymisation) so as to minimise the amount of personal data processed in order to protect the privacy of individuals.

The Council must also implement appropriate technical and organisational measures to ensure that, by default, only personal data which are **necessary** for each specific purpose of the processing activity are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

**\*\*For any new projects that involve the processing of personal data the advice of the Data Protection Officer must be sought, no later than the commencement of the project planning stage, so that the above principles can be put built in at the earliest opportunity. \*\***

## Joint controllers

Where the Council and another controller jointly determine why and how personal data should be processed the Council will be regarded as a 'joint controller'. If this is the case, then the appropriate Officer must work with the 'opposite number' to determine the respective responsibilities of the controllers for compliance with GDPR about the exercise of any rights by an individual and the controllers' respective duties to provide a privacy notice. The arrangement must reflect the respective roles and relationships of the joint controllers towards the individual(s). The essence of the arrangement shall be made available to any individual.

## Council use of data processors

These are external people/organisations who process personal data on our behalf to our order.

Officers MUST ensure that any processor we use:

- a) has provided **sufficient guarantees** of having implemented appropriate technical and organisational measures to satisfy us that personal data will be safe.
- b) **do not engage another processor** without our written authorisation.

In addition, any processing MUST be governed by a **contract** that is binding on the processor. It should set out the **subject-matter and duration of the processing, the nature and purpose of the processing and the type of personal data and categories of individuals**.

The contract MUST set out that:

- a) the processor will only process the personal data on **documented instructions** from us.
- b) any person or organisation authorised to process personal data have **committed themselves to confidentiality**.
- c) that the processor puts in to place **appropriate security measures**.
- d) assists us in complying with our obligations about requests by people to **access their data**.
- e) **assist us in complying with our security obligations, notifications to the ICO and to affected individuals and privacy impact assessments**.
- f) the processor **deletes or returns** all personal data to us after the end of the provision of the processing services.
- g) the processor **makes available to us all information necessary** to demonstrate compliance with the above and to **allow for and contribute to audits, including inspections etc**.

## Records of processing activities

The Council is obliged to maintain a record of our processing activities. The record will contain, amongst other matters, information about:

- (a) why we process personal data;
- (b) describe the categories of individuals and the categories of personal data;
- (c) state the categories of recipients to whom personal data has been or will be disclosed to;
- (d) where possible, state the envisaged time limits for erasure of the different categories of data;
- (e) where possible, give a general description of the technical and organisational security measures that the Council has in place.

**\*\*If Officers are aware of any changes in the above they should inform the Data Protection Officer who will make the required changes to the record\*\***

## Data protection impact assessments

Where a type of processing of personal data, using new technology, and considering the nature, scope, context and purposes of the processing, is likely to result in a **high risk** to the privacy of individuals then Officers MUST

**prior to the processing**, carry out an assessment of the impact of the envisaged processing operations on the individuals. **As part of this process Officers MUST seek the advice of the Data Protection Officer.**

Further guidance exists as to when an impact assessment should be undertaken and how. In certain circumstances the Information Commissioner may need to be consulted.

### **Data Protection Officer (DPO)**

The Council's designated DPO is Lorraine Fowkes. The DPO MUST be involved, properly and in a timely manner, in all issues which relate to the protection of personal data. The Council will support the DPO in performing her [this list is not exhaustive] tasks:

- (a) to inform and advise the Council of its legal obligations under all data protection laws;
- (b) to monitor the Council's compliance with GDPR and other data protection laws and the Council's compliance with our internal policies and procedures and to assign responsibilities, awareness-raising and training of staff involved in processing operations, and related audits;
- (c) to provide advice where requested about any data protection impact assessment and monitor its performance;
- (d) to cooperate with the Information Commissioner;
- (e) to act as the contact point for the Information Commissioner on issues relating to the processing of personal data, including privacy impact consultations and where appropriate, any other matter.

## 5. Related policies and procedures

- [Retention of documents schedule](#)
- [Subject access request](#)