Data Protection Policy and UK GDPR Update

Date:	30 November 2022
Agenda Item:	Agenda Item 8
Officer Title:	Laura Brentnall, Compliance & Data Protection Officer
Local Ward Members	N/A

Audit and Member Standards Committee

1. Executive Summary

1.1 This report seeks to update the Data Protection Policy and to update members on recent changes to the resourcing of data protection activities and audit actions contained within the Internal Audit Report issued separately to Members of the Committee.

2. Recommendations

2.1 To approve the updated Data Protection Policy to meet (UK GDPR) regulations as set out at Appendix A (changes highlighted in yellow) .

2.2 The committee note the action plan (Appendix B) to ensure all actions highlighted in a recent audit of GDPR are delivered in a timely manner and reported at future meetings as appropriate.

3. Background

3.1 The council is fully committed to complying with the requirements of the General Data Protection Regulations and the Data Protection Act (2018) and has appointed a new Compliance and Data Protection Officer to ensure the Authority prioritizes and delivers on this commitment.

3.2 As part of the Target Operating Model and in discussion with the previous DPO it was clear that sufficient internal resources were not previously available to co-ordinate and manage all of the likely changes required as we restructure our teams, data and use of systems.

3.3 A recent audit of the Council's Data Protection and UK GDPR Compliance that was conducted in July 2022 (prior to the appointment of the new DPO) reported limited assurance, with three high priority recommendations, eight medium recommendations and five low recommendations.

3.4 The new Data Protection Officer role was formally appointed on the 1 October 2022 and has already made significant progress in resolving four of the recommendations in full and initiated a detailed programme of work to deal with the remaining recommendations and wider improvement initiatives.

3.5 Remaining recommendations which will be resolved by March 2023 are:

- Updating the Record of Processing Activity to confirm all data held and with whom it is shared – this needs full review in line with the changes brought about by the Target Operating Model and forming of new delivery teams.
- New processing of personal data and changes to existing processes not considering potential impacts on data subjects – a programme of Data Subject Impact Assessments is to be developed alongside the transformation plans, including a clear process and oversight of documenting these considerations to be implemented by the ICT/Digital team as new processes are developed or existing processes reviewed.

- Rights of individuals to be informed – clear processes are being developed and staff will be trained to consistently apply them with of one to one meetings with data processors and a suite of e-learning training being deployed on a regular basis to inform and check understanding.
- Updates to the

3.6 The Compliance and Data Protection Officer will provide further briefings on the progress of the plan to the Audit & Member Standards Committee in advance of both the February 2023 and March 2023 committee meetings, recognising that members will be keen to ensure all recommendations are resolved as swiftly as possible. The Compliance and Data Protection Officer will provide updates to each Audit and Member Standards Committee up until the completion of the approved action plan.

3.7 Consistent training and reminders of the requirements of the General Data Protection Regulations (2018) and the Data Protection Act will be available to all staff and members and information hubs will be available in due course.

Alternative Options	None, the council must comply with these regulations, however the committee can choose not to receive ongoing reports and instead have briefings.
Consultation	We have ongoing support from South Staffordshire District Council legal team regarding current advice and guidance and a strong auditor who specialises in this area to highlight areas for development. The updated policy has also been signed off by the Audit advisor.
Financial Implications	None – the role is now funded within the TOM as a permanent post on establishment.
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)
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 have been addressed.	Green Likelihood- low/ Impact -low
c)	Data Protection Officer capacity to develop and improve processes	New role appointed and action plan in place.	Green Likelihood – low/ impact - low

d)	Ongoing development of processes and practice during transformation work	Clear plan for digital transformation developed and regular review/compliance checks by DPO.	Green Likelihood – low/ impact - low
e)	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

Appendix A

Data Protection Policy
November 2022

Approved by:	**Leadership Team**
Approval date:	
Approved by:	**Audit & Member Standards**
Approval date:	
Author/owner:	**Laura Brentnall**
Review frequency:	**2 Years**
Next review date:	**November 2024**
Location:	**Governance**

Introduction

Lichfield District Council is committed to complying with the General Data Protection Regulation (UK GDPR). This policy sets 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.

Further information can be found at: https://ico.org.uk/

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. This is of particular importance now that data is stored electronically and available to officers who are homeworking as a result of the pandemic and continuing new ways of working.

1. Scope of policy

Both Officers and Members **must** comply with this policy when processing personal data on the Council's behalf.

Compliance with this policy is **mandatory.** Related policies and procedures/guidelines are available to assist Officers and Members 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 Officer and Member Codes of Conduct.

We primarily provide services for local communities and the people who live in them. We also collect data about people world-wide who contact us requesting information about Lichfield District Council.

In order to provide these services, we must collect and use data about the people we provide services to. Data is also collected and used where we have a statutory duty to do so.

We collect data in a number of ways; verbally, paper, telephone, email, online forms, website cookies as well as other forms of image and voice recordings. This data may be collected from the data subject or may be gathered from other sources, we may need to occasionally ask other agencies or organisations for relevant data about the data subject to fulfil our legal responsibilities or to provide services. All data we obtain will be captured and stored in appropriate systems for the purpose or purposes specified.

2. How this policy relates to/underpins our strategic ambitions

Once of our fundamental ambitions is to be a better council that is responsive and resident centric. 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.

3. Policy details

3.1 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.

Data Protection Officer (DPO) is the designated person within an organisation that has responsibility for ensuring 'legal' compliance with GDPR, which relates only to personal data.

3.2 Commitment to the (General Data Protection) Principles

The Council is legally obliged to comply with data protection principles set out in the GDPR when handling your personal data. We will ensure we:

(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.

(g) Officers are accountable 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.

3.3 Member Responsibility

Members will receive, consider and share the personal data of residents as necessary during the course of their duties. Further guidance on how to do this safely and effectively can be found from the Information Commissioner. You may also receive information about individuals as part of your role as a member of a committee or the cabinet. You may also receive information about local residents e.g. an extract of the electoral roll for the purposes of canvassing for your political party.

You MUST when dealing with personal data uphold the data protection principles as set out at 3.2.

3.4 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 the processing is necessary to protect someone's life , this is called **vital interests**
(e) 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;
(f) 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****

3.5 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****

3.6 Crime/offence data

To process personal data about criminal convictions or offences, the Council must have a lawful basis under article 6 (at 4.5 above) and legal authority or official authority. For further advice speak with the Data Protection Officer.

3.7 Your Rights

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

a. **The right to be informed**
You have the right to be informed about the collection and use of your personal data. We will normally do this by way of privacy notices on forms or on our website.

b. **The right of access**
You have the right to request access to the information we hold about you. The information requested will be provided free of charge, however, we may charge a reasonable fee if the request is considered "manifestly unfounded" or "excessive". We may also charge a fee if you request further copies of information we have already provided to you

c. **The right to rectification**
You have the right to request that inaccurate personal information be rectified and incomplete personal information updated.

d. **The right to erasure**
You have a right to ask us to erase information about you. This right will only apply where:

- The personal data is no longer necessary for the purpose which we originally collected it for
- We are relying on consent as the lawful basis for holding the data and you withdraw that consent
- We are processing the data for direct marketing purposes and you object to that processing.
- The majority of processing carried out by the council is governed by legislation, which usually includes how long we have to keep your information. The right of erasure won't apply where we have a lawful reason to process your data and it is kept in accordance with our retention schedule.
- Where your information has been shared with others, we will endeavour to ensure they are aware of your request for erasure.

e. **The right to restrict processing**
You have the right to restrict the processing of your personal data where:

- you contest the accuracy of your personal data and the council needs to verify its accuracy before further processing takes place;
- the data has been unlawfully processed and you oppose erasure of the data and request restriction of its use instead;

f. **The right to data portability**
You have the right to ask for your personal information to be given back to you or another service provider of your choice in a commonly used format. This is called data portability. However, this only applies if we're using your personal information with consent (not if we're required to by law) and if decisions were made by a computer and not a human being. It's likely that data portability won't apply to most of the services you receive from the Council.

g. **Automated Decision Making**

You have the right to not be subject to a decision based solely on automated processing. You can ask to have any computer made decisions explained to you, and details of how we may have 'risk profiled' you.

h. **The right to object**
You have the right to object to the processing of your personal information.

The right to object only applies in certain circumstances.

Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, a data subject should be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the Council to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

Please note that the above rights are not absolute. The Council can say no to your request. For full details of the rights, ground to exercise them and the exemptions available to the Council please see articles 12 to 23 of UK GDPR. If you wish to exercise a right please put your request in writing to our Data Protection Officer.

To exercise your rights to access information we hold about you please use our subject access request form or for any other queries, please email dpo@lichfielddc.gov.uk

3.8 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.

3.9 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. ****

3.10 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.

3.11 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.**

3.12 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****

3.13 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.

3.14 Data Protection Officer (DPO)

The Council's designated DPO is Laura Brentnall, Compliance & Data Protection Officer available via dpo@lichfielddc.gov.uk . 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.

3.15 Data Breaches

The Council does all it reasonably can to keep your personal data confidential, available for us and intact. However, if there should be a breach of your personal data such as its destruction, loss, alteration etc. then, if there is a risk of harm to you, the Council will report matters to the Information Commissioner's Office. We will tell them what has happened; how many people are affected; what the likely consequence s are and what we are doing to make things better. In certain circumstances we will also provide this information to you.

5.Related policies and procedures

- Retention of documents schedule
- Subject access request
- ICT Security Policies