Your ref
Our ref
Ask for Wendy Johnson
Email wendy.johnson@lichfielddc.gov.uk

Lichfield district council
www.lichfielddc.gov.uk

District Council House, Frog Lane
Lichfield, Staffordshire WS136YU

Customer Services 01543 308000
Direct Line 01543 308075

Monday, 30 April 2018

Dear Sir/Madam

AUDIT AND MEMBER STANDARDS COMMITTEE SUPPLEMENT

Please find attached supplement papers for Audit and Member Standards Committee on **WEDNESDAY, 9TH MAY, 2018 at 6.00 PM IN THE COMMITTEE ROOM** District Council House, Lichfield.

Access to the Committee Room is via the Members' Entrance.

Yours Faithfully

Neil Turner BSc (Hons) MSc
Director of Transformation & Resources

SUPPLEMENT

7.	**Data Protection/GDPR**	3 - 26
	(Report of the Head of Legal, Property & Democratic Services (Monitoring Officer))	

This page is intentionally left blank

DATA PROTECTION ACT AND GDPR

Cabinet Member for Finance & Democratic Services

Date:	9 May 2018
Agenda Item:	7
Contact Officer:	Bal Nahal
Tel Number:	01543-308002
Email:	bal.nahal@lichfielddc.gov.uk
Key Decision?	**NO**
Local Ward Members	If any Wards are particularly affected insert the name of the Ward Members and their Ward. Ensure that the Ward Members have been consulted.

Lichfield district council
www.lichfielddc.gov.uk

AUDIT & MEMBER STANDARDS COMMITTEE

1. Executive Summary

1.1 To inform Members of progress made to date in respect of preparing for a change in data protection legislation, known as GDPR (General Data Protection Regulation).

1.2 To inform Members of Cabinet's decision on 1 May 2018 – see attached Cabinet Report **(Appendix 1).**

2. Recommendations

2.1 That Members note the actions to date and the planned measures to ensure compliance with the legislative requirements.

2.2 To approve the amended Data Protection Policy **(attached – Appendix 2**) and Individual GDPR Rights – Response Procedures **(Appendix 3).**

3. Background

3.1 Please see attached Cabinet Report **(Appendix 1).**

Alternative Options	None.
Consultation	Report to Audit Committee – 27 March 2017 Report to Cabinet – 1 May 2018
Financial Implications	The sum of £20,000 per year on GDPR has been included within the approved MTFS and is within budget.
Contribution to the Delivery of the Strategic Plan	Proposals will assist with compliance with the legal requirements and thus the Council's ability to deliver the services required and Fit for Future.

Equality, Diversity and Human Rights Implications	The new General Data Protection Regulations contain no specific reference to equality considerations, so at this stage there are no issues to consider beyond those associated with the current Data Protection Act provisions. However, analysis of the equality implications have been included as part of the wider project plan when considering the impact the regulations will have on each service. These will be included in future reports if necessary.
Crime & Safety Issues	No crime and safety issues.

	Risk Description	How We Manage It	Severity of Risk (RYG)
A	Non Compliance with Legislation	The Data Protection Policy is based on the current best practice. GDPR Training will be provided to all employees and members. The updated Data Protection Policy and Individual GDPR rights – Response procedures will be published on the Council's Intranet and Website once agreed. It will also be informed to all employees of the Council.	State if risk is Red (severe), Yellow (material) or Green (tolerable) as determined by the Likelihood and Impact Assessment. YELLOW
B			
C			
D			
E			

Background documents: Regulations (EU) 2016/679 of the European Parliament and of Council of 27 April 2016 and the Protection of Natural Persons with regard the processing of personal data and on the free movement of such data and repealing the direction 95/46/EC (General Data Protection Regulations).

Relevant web links: https://democracy.lichfielddc.gov.uk/mgCommitteeDetails.aspx?ID=134

DATA PROTECTION ACT AND GDPR

Cabinet Member for Finance & Democratic Services

Date:	1 May 2018
Agenda Item:	3
Contact Officer:	Bal Nahal
Tel Number:	01543-308002
Email:	bal.nahal@lichfielddc.gov.uk
Key Decision?	**NO**
Local Ward Members	If any Wards are particularly affected insert the name of the Ward Members and their Ward. Ensure that the Ward Members have been consulted.

Lichfield district council
www.lichfielddc.gov.uk

CABINET

1. Executive Summary

1.1 To inform Members of progress made to date in respect of preparing for a change in data protection legislation, known as GDPR (General Data Protection Regulation).

1.2 Members who process data on behalf of constituents whilst doing case work also need to comply with GDPR as they are data processors. The Council ensures that Members are registered with the ICO to undertake these duties.

2. Recommendations

2.1 That Members note the actions to date and the planned measures to ensure compliance with the legislative requirements.

2.2 To appoint Assistant Director Democratic & Regulatory Services at South Staffordshire Council as the Council's Data Protection Officer for 2 years effective from 2 May 2018.

3. Background

3.1 GDPR [the new data protection law] comes in to force on 25 May 2018. It replaces the European 'directive' that the current Data Protection Act 1998 is based on with a 'regulation'. GDPR needs to be read alongside the new Data Protection Bill. This Bill is currently going through the parliamentary process and when it comes in to effect [this must be at the same time as GDPR] it will replace the current Data Protection Act 1998.

The new law must be complied with by the Council as well as members of the Council in their own right as data controllers. Member training is scheduled for Thursday 19 April 2018. At that session members will be advised as to what support they will receive to help them comply with the new law.

Personal data is any information that relates to an identified or identifiable individual.

Data protection is regulated by the Information Commissioner's [Elizabeth Denham] Office.

The Commissioner has described GDPR [for those who currently comply with the law] as an "evolution" not a "revolution". She has also stated that she prefers the "carrot" rather than the "stick" which means that her approach is to encourage organisations to comply in the first instance.

It should be noted however that the new regime does include potentially much more severe penalties for data breaches and increased requirements to notify non-compliance to the ICO.

The ICO's guidance on the steps to be taken can be seen here.

3.2 **Action Taken**

The Council has a project team (consisting of one or more representatives from each service area) led by David Campbell - a Solicitor employed by South Staffordshire Council.

In order to become 'GDPR compliant' the Council needs to take the following steps (following the ICO guidance referred to above):

1. 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.

The Council has allocated a significant amount of officer time into preparation work to ensure compliance. Senior Officers have been kept informed throughout and this report will update Members in respect of steps taken and action needed.

2. Information you hold

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

Service teams have identified what personal data the Council processes, who has access, who it is shared with etc. This 'audit' has helped inform the project plan which is being implemented across the Council.

3. Communicating privacy information

Current privacy notes should be reviewed and a plan put in place for making any necessary changes.

This work has been scoped as part of the project plan. There are a number of privacy notices in place across the Council and these are being reviewed and refreshed as necessary to include the lawful basis for processing the data, data retention periods and the right to complain.

4. Individuals' rights

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

These rights are a mix of refinement of the old and (some) new such as (not exhaustive):

a) The right to access data
b) The right to have incorrect data rectified
c) The right to have data erased [new]
d) The right to data portability [new – but unlikely to be a concern to the council]

e) The right to restrict processing
f) The right to object to processing [limited effect on the council]
g) The right to object to marketing

The Council already has procedures in place to deal with the existing rights; possibly the most significant new right is the right to have data erased. This is not an absolute right and if there is a legitimate business need to retain data then this right can be overridden. However, the Council will need to have an appropriate procedure in place to deal with any such requests. This is being drafted and will be in place in time for May 2018.

5. Subject access requests

Procedures should be updated to allow for the new rules:

- *generally information should be provided free of charge (currently there is a standard £10 charge)*
- *Information should be provided within one month (currently this is 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.*

Whilst the Council does not receive a significant number of subject access requests, procedures and systems are being reviewed to ensure we can comply within the new shorter timescales.

6. Lawful basis for processing data

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

For the Council's statutory functions this will usually be that we are acting in the public interest or exercising official authority. For non-statutory function such as leisure the basis will typically be that the council provides services under a contract.

This is important as the lawful basis impacts on a person's rights under GDPR; if using consent as a basis for processing data then an individual has greater rights to have that data deleted.

Again, officers are working through this in each service team to ensure the lawful basis for processing data is clear and documented.

7. Consent

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

Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in.

Where the Council relies on consent to process data, the consents given will be reviewed as part of the preparation work and if necessary (this will be on a case by case basis) revised and renewed.

8. 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.

9. 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 should also be notified to the individual concerned.

The Council currently has a procedure in place to deal with data breaches and this is being reviewed to ensure compliance with GDPR requirements. It is not anticipated that any significant changes will be necessary.

10. 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 Privacy Impact Assessments (or Data Protection Impact Assessments as they will be known) in certain circumstances.

11. 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 DPO must have access to information across the Council and have the support of the leadership to carry out their role. The Council has approached three neighbouring Councils for quotes for the provision of a shared DPO. Two were not interested and only South Staffordshire Council has quoted and has been assisting in the preparation of compliance towards GDPR. It is proposed that the Assistant Director Democratic & Regulatory Services from South Staffordshire Council is designated as a shared DPO for Lichfield District Council and will be invited to attend Leadership Team meetings/Legal & Democratic team meetings as and when required. The Council will receive a designated Solicitor for 1 day per week who is trained in GDPR. The team at South Staffordshire Council which consists of 4 solicitors will also provide advice and assistance on day to day GDPR issues and on Information Governance as and when required.

12. International

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

In order to ensure the Council is GDPR compliant, the following actions are also being taken:

a) **A Service Level Agreement is currently being drafted;**

b) **Review any contracts it has with 'data processors' i.e. external organisations who process personal data on behalf of the Council.** GDPR requires the Council as a controller of data to ensure that any processor complies with new legal requirements;

b) **Review the existing 'organisational' and 'technical' measures it has in place and ensure that personal data is kept 'safe';**

c) **Review and update its incident management plan and formulate procedures setting out when and how to notify the Commissioner and affected individuals if there was a breach of security i.e. unauthorised or unlawful processing, loss, damage or destruction of personal data**.

3.3 Next Steps

Whilst preparation work has been underway for some time, there is still a significant amount of work to be undertaken over the coming months.

Meetings are now being arranged with representatives of service teams to provide the necessary training/information in the drafting and giving of 'fair processing notices' to all individuals from whom the Council collects information from.

The meetings will also identify any data processor contracts that need to be looked at.

It is anticipated that these meetings will have all taken place by the end of April 2018. It will then be for service teams to draft the appropriate notices (with guidance and support) and to liaise with any current processors of data that the Council controls. Revised contract provisions, to take account of the new GDPR requirements are being finalised and will be made available to all service teams and incorporated into the Council's Standard Terms and Conditions.

Procedures to assist when people exercise rights have been drafted and the revised data protection policy is being finalised and will come forwards for approval shortly.

Discussions will take place with ICT re: any technical changes that may need to take place to keep data safe. These discussions will also inform the revision of the Council's current incident management plan. It is planned to complete the revision of the Council's information security policy/incident management plan by the end of April 2018.

A number of staff have already received training on the changes brought about by GDPR via team training sessions provided in-house. All those staff who regularly handle personal data will have received face-to-face training before the coming into force of the GPDR and those who do not will have undertaken an appropriate form of e-learning. The training programme will be risk-based with those service teams that handle the most/most sensitive data being targeted first; these areas will receive face-to-face training. It is envisaged this will include Revenues and Benefits, Human Resources, Elections, Development Management and Local Plans. Records will be kept of all training undertaken.

Conclusion

The Council is on track to meet the requirements of the new data protection rules. There will be a substantial amount of work between now and 25 May 2018, however, we are confident that we will be compliant with the new rules on the go-live date.

Regular updates will be given to Members on preparation for the changes to the data protection rules.

Alternative Options	The Council could have appointed an In-house DPO, but the costs including overheads would have been much greater. Having a shared service with South Staffordshire Council brings resilience as they have a team of experts on data protection issues/information governance as well as providing the services of a DPO.
Consultation	Report to Audit Committee – 27 March 2017
Financial Implications	The sum of £20,000 per year on GDPR has been included within the approved MTFS and is within budget.

Contribution to the Delivery of the Strategic Plan	Proposals will assist with compliance with the legal requirements and thus the Council's ability to deliver the services required and Fit for Future.
Equality, Diversity and Human Rights Implications	The new General Data Protection Regulations contain no specific reference to equality considerations, so at this stage there are no issues to consider beyond those associated with the current Data Protection Act provisions. However, analysis of the equality implications have been included as part of the wider project plan when considering the impact the regulations will have on each service. These will be included in future reports if necessary.
Crime & Safety Issues	No crime and safety issues.

	Risk Description	How We Manage It	Severity of Risk (RYG)
A	Non Compliance with Legislation.	The Data Protection Policy is based on the current best practice. GDPR Training will need to be provided to all employees and members. The updated Data Protection Policy will be published on the Council's Intranet and Website once agreed. It will also be informed to all employees of the Council.	State if risk is Red (severe), Yellow (material) or Green (tolerable) as determined by the Likelihood and Impact Assessment. YELLOW
B			
C			
D			
E			

Background documents: Regulations (EU) 2016/679 of the European Parliament and of Council of 27 April 2016 and the Protection of Natural Persons with regard the processing of personal data and on the free movement of such data and repealing the direction 95/46/EC (General Data Protection Regulations).

Relevant web links: https://democracy.lichfielddc.gov.uk/mgCommitteeDetails.aspx

Lichfield District Council

Data Protection Policy

Opening statement

Lichfield District Council ('the Council') is committed to complying with both the General Data Protection Regulation ('GDPR') 2016/679 and the Data Protection Act 2018. This policy sets out the Council's approach (through its Officers and Members) to the handling of 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.

Protecting the confidentiality and integrity of personal data is something that the Council takes extremely seriously. The Council is exposed to potential fines of up to EUR20 million (depending on the nature and severity of the infringement) for failure to comply with the provisions of the GDPR.

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.

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.

[more information is given below]

(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.

Further information

Leadership Team are responsible for ensuring that this policy and the related documents are complied with. However, if you have any questions about the policy or any other data protection documentation please speak with the Data Protection Officer.

Changes to this policy

The Council reserves the right to change this policy at any time. If it does it will draw any changes to the attention of Officers.

Approved by

May 2018

Persons responsible for compliance – Leadership Team

Version 1 Review date 1 June 2019

This page is intentionally left blank

Individual GDPR rights

Response procedures

Note: requests ought generally be responded to within one month of receipt. The Council may be the subject of a financial penalty if it fails to comply with the deadline.

CONTENTS

CLAUSE **PAGE**

1. About these procedures

1.1 Individuals have certain rights in respect of *their* personal data. These procedures provide a framework for responding to requests to exercise those rights. **If you are at all uncertain as to what to do you must speak with the Council's Data Protection Officer.**

1.2 For the purposes of these procedures, "personal data" means any information relating to an identified or identifiable individual. An identifiable Individual is one who can be identified, directly or indirectly, by reference to an identifier, such as their name, identification number or online identifier. "Processing" means any operation or set of operations that is performed on personal data, such as collection, use, storage, dissemination and destruction.

2. Responding to requests to access personal data

2.1 Individuals have the right to request access to their personal data processed by us. Such requests are called subject access requests (SARs). When an Individual makes a SAR, we shall take the following steps:

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

(b) [Very Important] **confirm** the identity of the Individual who is requesting access to their personal data;

(c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held; and

(d) **confirm** to the Individual whether their personal data is being processed. **For the avoidance of doubt processing includes where the information is simply being stored by the Council.**

2.2 If personal data of the Individual is being processed, we must provide them with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means:

(a) the purposes [why we are] of the processing;

(b) the categories of personal data concerned (for example, name, contact details, DOB, requests for service etc.);

(c) the recipients or categories of recipient to whom the personal data has been or will be disclosed in particular any recipients overseas (for example, US-based cloud service providers);

(d) where possible, the envisaged period for which their personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of their right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing;

(f) the right to lodge a complaint with the Information Commissioner's Office (ICO). **Individuals ought to be advised to speak to the Data Protection Officer in the first instance [this may resolve matters] but they are not under an obligation to do so.**

(g) where the personal data are not collected from the individual, any available information as to their source;

(h) (where applicable) the existence of any automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for them; and

(i) where personal data are transferred outside the EU, details of the appropriate safeguards to protect the personal data.

2.3 We shall also, unless there is an exemption (see paragraph 9 below), provide the Individual with a copy of the personal data processed by us in a commonly used electronic form (unless they either did not make the request by electronic means or they have specifically requested not to be provided with the copy in electronic form) within **one month** of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding, we MUST inform the Individual within one month of receipt of the request and explain the reason(s) for the delay.

2.4 Before providing the personal data to the Individual making the SAR, we shall review the personal data requested to see if they contain the personal data of other Individuals. If they do, we may redact the personal data of those other Individuals prior to providing the Individual with their personal data, unless those other Individuals have consented to the disclosure of their personal data. **For further guidance on this please consult the ICO website – *www.ico.gov.uk* where you will find a Code of Practice. Please also speak with the Data Protection Officer.**

2.5 If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request.

2.6 If we are not going to respond to the SAR, we shall inform the Individual of the reason(s) for not taking action and of the possibility of lodging a complaint with the ICO.

3. Responding to requests to rectify personal data

3.1 Individuals [this may arise when they have been provided with a copy of their information] have the right to have any inaccurate personal data rectified. Rectification can include having incomplete personal data completed, for example, by the Individual providing a supplementary statement regarding the data. Where such a request is made, we must, unless there is an exemption (see paragraph 9 below), rectify the personal data without undue delay.

3.2 We shall also communicate the rectification of the personal data to each recipient to whom the personal data have been disclosed (for example, any third-party service providers who process the data on our behalf) unless this is impossible or involves disproportionate effort. We shall also inform the Individual about those recipients if the Individual requests it.

4. Responding to requests for the erasure of personal data

4.1 Individuals have the right, in certain circumstances, to request that we erase their personal data. Where such a request is made, we shall, unless there is an exemption (see paragraph 9 below), erase the personal data without undue delay if:

(a) the personal data are no longer necessary **[consider if we need it for a continuing purpose]** in relation to the purposes for which they were collected or otherwise processed;

(b) the Individual withdraws their consent to the processing of their personal data and consent was the basis on which the personal data were processed and there is no other legal basis for the processing;

(c) the Individual objects to the processing of their personal data on the basis of our legitimate interests which override their interests or fundamental rights and freedoms- unless we either can show compelling legitimate grounds for the processing which override those interests, rights and freedoms, or we are processing the data for the establishment, exercise or defence of legal claims; **[Please speak with the Data Protection Officer if this situation arises]**

(d) the Individual objects to the processing of their personal data for direct marketing purposes;

(e) the personal data have been unlawfully processed, or;

(f) the personal data have to be erased for compliance with a legal obligation to which we are subject.

4.2 When an Individual makes a request for erasure in the circumstances set out above, we shall, unless there is an exemption (see paragraph 4.5 and paragraph 9 below), take the following steps:

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

(b) confirm the identity of the Individual who is the subject of the personal data. We may request additional information from the Individual to do this;

(c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held and erase such data within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding, we shall inform the Individual within one month of receipt of the request and explain the reason(s) for the delay;

(d) where we have made the personal data public, we must, taking reasonable steps, including technical measures, inform those who are processing the personal data that the Individual has requested the erasure by them of any links to, or copies or replications of, those personal data; and

(e) communicate the erasure of the personal data to each recipient to whom the personal data has been disclosed unless this is impossible or involves disproportionate effort. We shall also inform the Individual about those recipients if the Individual requests it.

4.3 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of erasure, or refuse to act on the request.

4.4 If we are not going to respond to the request, we shall inform the Individual of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.

4.5 In addition to the exemptions in paragraph 9 below, we can also refuse to erase the personal data to the extent processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by law and to which we are subject; or

(c) for the establishment, exercise or defence of legal claims.

5. Responding to requests to restrict the processing of personal data

5.1 Individuals have the right, unless there is an exemption (see paragraph 9 below), to restrict the processing of their personal data if:

(a) the Individual contests the accuracy of the personal data, for a period to allow us to verify the accuracy of the personal data;

(b) the processing is unlawful, and the Individual opposes the erasure of the personal data and requests the restriction of their use instead;

(c) we no longer need the personal data for the purposes we collected them, but they are required by the Individual for the establishment, exercise or defence of legal claims; and

(d) the Individual has objected to the processing, pending verification of whether we have legitimate grounds to override their objection.

5.2 Where processing has been restricted, we shall only process the personal data (excluding storing them):

(a) with the individual 's consent;

(b) for the establishment, exercise or defence of legal claims;

(c) for the protection of the rights of another person.

5.3 Prior to lifting the restriction, we shall inform the Individual of the lifting of the restriction.

5.4 We shall communicate the restriction of processing of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort. We shall also inform the Individual about those recipients if the Individual requests it.

6. Responding to requests for the portability of personal data [this is unlikely to apply to the Council]

6.1 Individuals have the right, in certain circumstances, to receive their personal data that they have provided to us in a structured, commonly used and machine-readable format that they can then transmit to another organisation. Where such a request is made, we shall, unless there is an exemption (see paragraph 9 below), provide the personal data without undue delay if:

(a) the legal basis for the processing of the personal data is consent or pursuant to a contract; and

(b) our processing of that data is automated.

6.2 When an Individual makes a request for portability in the circumstances set out above, we shall take the following steps:

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

(b) confirm the identity of the Individual who is the subject of the personal data. We may request additional information from the Individual to confirm their identity; and

(c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held and provide the Individual with such data (or, at their request, transmit the personal data directly to another company, where technically feasible) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding, we shall inform the Individual within one month of receipt of the request and explain the reason(s) for the delay.

6.3 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing or transmitting the personal data, or refuse to act on the request.

6.4 If we are not going to respond to the request, we shall inform the Individual of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.

7. Responding to objections to the processing of personal data

7.1 Individuals have the right to object to the processing of their personal data where such processing is on the basis of our legitimate interests unless we either:

(a) can show compelling legitimate grounds for the processing which override the individual 's interests, rights and freedoms; or

(b) are processing the personal data for the establishment, exercise or defence of legal claims.

7.2 Individuals also have the right to object to the processing of their personal data for scientific or historical research purposes, or statistical purposes.

7.3 Where such an objection is made, we shall, unless there is an exemption (see paragraph 9 below), no longer process the individual's personal data.

7.4 Where personal data are processed for direct marketing purposes, Individuals have the right to object at any time to the processing of their personal data for such marketing. If an Individual makes such a request, we shall stop processing the personal data for such purposes.

8. Responding to requests not to be subject to automated decision-making

8.1 Individuals have the right, in certain circumstances, not to be subject to a decision based solely on the automated processing of their personal data, if such decision produces legal effects concerning them or similarly significantly affects them. Where such a request is made, we shall, unless there is an exemption (see paragraph 9 below), no longer make such a decision unless it:

(a) is necessary for entering into, or the performance of, a contract between us and them;

(b) is authorised by applicable law which lays down suitable measures to safeguard their rights, freedoms and legitimate interests; or

(c) is based on their explicit consent.

8.2 If the decision falls within paragraph 8.1(a) or paragraph 8.1(c), we shall implement suitable measures to safeguard their rights, freedoms and legitimate interests, including the right to obtain human intervention, to express their point of view and to contest the decision.

9. Exemptions

9.1 Before responding to any request, officers must check whether there are any exemptions that apply to the personal data that are the subject of the request. These may apply where it is necessary and proportionate not to comply with the requests described above to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general national public interest, an important national economic or financial interest, including monetary, budgetary and taxation matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in paragraph 9.1(a) and paragraph 9.1(g) above;

(i) the protection of the Individual or the rights and freedoms of others; or

(j) the enforcement of civil law claim

If you believe that a restriction may apply then you should speak with the Data Protection Officer.