Staff Summary Information Sheet

Subject: The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

1. Introduction

- The General Data Protection Regulation (GDPR) will come into force on the 25th May 2018. The GDPR clarifies and strengths the rules on processing personal information (known as personal data) as first set out in the Data Protection Act 1998.
- The GDPR is expanded upon in the Data Protection Act 2018 (DPA) which also came into force in May 2018 and replaces the Data Protection Act 1998. Both the GDPR and DPA need to be read side by side.
- The idea behind GDPR is to allow individuals to take back control of their personal data and to update the data protection laws due to global technological developments.
- The Information Commissioner's Office (ICO) will be able to fine organisations up to 20 million Euros for non-compliance or 4% of global turnover whichever the greater, for non-compliance.
- This is a significant increase on previous fine levels.
- There have been recent high-profile cases reported in the media, regarding the loss or mishandling of personal data. This has focused attention on ensuring that personal data is appropriately handled within public bodies, and that the requirements of the data protection laws are being met.
- The council, handles a considerable amount of data, and therefore most council staff have some degree of exposure to personal data about customers and others.
- The council and all its staff have responsibilities to comply with the requirements of the GDPR and DPA. Failure to do so, could result in the council and/or its staff being criminally prosecuted and/or fined, as well as legal claims for compensation. This could also result in substantial reputational damage for the council.
- It is therefore important that all staff are familiar with the requirements of the new laws and clearly understand what they need to do on a day-to-day basis in order to comply.
- Council staff are granted access to systems, records, data and information on a "need to know" basis. Your access rights are tailored to your operational needs. Systems will trail and log system activity to the User ID and this ensures that only authorised staff can create, amend or delete data. In order to protect the accuracy and integrity of personal and other data you should only use your designated ID and **not** share it with other colleagues.
- The council has a **General Data Protection Regulation and Data Protection Policy** which is available via the council's Intranet site, on the dedicated Data Protection Page.
- This sheet is not a comprehensive guide and only covers the basics – see Section 4 below for details of additional sources of guidance and advice. **If you are in doubt, seek advice.**

2. What does the Act cover?

- In summary, the GDPR and DPA relates to:

    - Paper and manual records, as well as computer-based and electronic records;
    - Personal data of living individuals (who are known as **Data Subjects**);
    - Any person or organisation (known as **Controllers**) that holds data, about living individuals and determines how the personal data is used.
    - 6 principles relating to the collection, use, processing and disclosure of data that must be complied with by the **Controllers and Processors** acting on behalf of the council, who must be instructed under a contract which is complaint with the new laws;
    - In order to protect the **Data Subjects** there are defined rules about what types of disclosure of their information are permitted and those that are prohibited and the council and its staff must rigidly comply in respect of disclosure;
    - The rights of **Data Subjects have been extended** in relation to access to their personal data (referred to as a **Subject Access Request**). The council can no longer charge a fee for this and can no longer insist on a written request, but can encourage requesters

to use the council's online form. The time limit to respond to these requests has reduced to one calendar month to in some case 28 days. The council can still insist on proof of the requester's identity.

- This information must be provided in a legible form, with interpretations provided for any codes used and if the request is made electronically the response should be given in a commonly used electronic format and if available through self-service by the **Data Subject** to a secure online system.
- If, upon receiving the requested information held by the **Controller**, the **Data Subject** feels that it contains errors, he/she has the right to apply to rectification, restriction of its processing and erasure (deletion) of the affected personal data. **The GDPR has extended these rights** to include a right to data portability (to move data between organisations freely), a right to be informed of how their data is being used (privacy notices), a right to object to its use and rights related to automated decision making (decisions made solely by computers).
- If the **Data Subject** suffers damage by reason of any contravention by the **Data Controller** of any requirement of the GDPR or DPA, then he/she has the right to receive compensation. DPA has expanded this to include compensation for any adverse effect which is likely increase the number of compensation claims.

3. What do I need to do?

- Firstly, you must read this **Summary** and the GDPR and Data Protection Policy available on the council's intranet. If you don't have access to the intranet it is the responsibility of your line manager to ensure you receive a copy of this.
- Become familiar with the 6 DPA principles of processing personal data. In summary these are;
  1) process the data lawfully, fairly and transparently
  2) use the data only for the purpose it was provided for
  3) limit the amount of data to only what is needed
  4) ensure the data is accurate and up to date.
  5) only keep the data for as long as necessary
  6) keep the data secure and only disclose it to those who need to know.
- Consider how, in the course of your duties, you either collect, process, analyse, disclose or otherwise deal with personal data;
- You should advise anyone enquiring about accessing their personal data that the council holds, to complete the **Subject Access Request Form** and to forward it and an approved form of identity, to the council's Legal Officer, Karan Shearwood, who logs all requests. The **Subject Access Request Form** is available from the council's website. GDPR also allows requests to be made orally and therefore requests can also be made by contacting the council's Legal Officer at legal@lincoln.go.uk or telephone 01522 881188.
- You should advise anyone with a query regarding data protection to contact our Data Protection Officer at dpo@lincoln.gov.uk or telephone 881188.
- Think carefully about disclosing information to others, irrespective of whether the request is in person, in writing (including emails and faxes) or via the telephone. Remember that the DPA applies to manual records and paper files as well as electronic records and systems;
- Protect your system user identity and related passwords so that no one can access systems in your name:
  - Do not share your ID and password
  - Do not use another colleague's ID to access systems
  - Do not write down your passwords
  - **Any breach of Information Security Policies is a disciplinary offence.**
  - Choose combinations of letters, numbers and characters to provide more secure password combinations, and do not use more obvious passwords such as your birthday, car registration number or a pet's name;
- Only collect the personal data required for a particular operational purpose;
- When asked to disclose information ensure that the enquirer is entitled to access the data:
  - Is the person making the request proven to be the data subject?

- Be certain that other colleagues working in your department and elsewhere in the council have the right to receive or view personal data **before** releasing any requested information. They may not share your level of access rights and may not "need to know". **If in any doubt consult with your line manager or team leader**;
- Be aware that there are people who will try and trick you in to giving out personal data so always ensure that the individual making the request is entitled to view such data, **before** such data is revealed. Be aware that unauthorised disclosure of personal data is an offence and you could be held liable;
- If in doubt about the identity and validity of the person making the request ask for the request to be made in writing and check that the request is not potentially bogus.

- Do not leave documents containing personal data exposed on your workspace where customers or other employees could read or remove them. Adopt a **'clear desk'** approach by securing and not displaying, hard copy personal data when it is not being used;
- Only dispose of confidential documents or information through the council's confidential waste paper service or by cross-cut shredding with the department;
- Lock your computer whenever you are leaving your desk ;
- Position your computer screen away from windows and corridors to prevent accidental disclosures of personal data;
- Use encryption on storage devices containing personal data that may be taken out of the office; and
- For computer systems not on the council network ensure that data is backed up and the copies are kept in a secure place.

4. Sources of Further Information

- **Information Commissioner's Website:** www.ico.gov.uk
- **The Data Protection Policies are available on City People**
- **Data Protection Officer:** Sally Brooks-ext. 3765
- **Freedom of Information Officer** and **Legal & Democratic Services Manager:** Becky Scott-ext 3441
- **Business Development & IT Manager:** Matt Smith-ext 3308