

## **General Data Protection Regulation (GDPR) Policy**

### **Introduction**

1. This policy explains to councillors, staff and the public about GDPR.
2. Personal data must be:
  - a) processed lawfully, fairly and transparently.
  - b) collected for specified, explicit and legitimate purposes.
  - c) be adequate, relevant and limited to what is necessary for processing.
  - d) be accurate and kept up to date.
  - e) be kept only for as long as is necessary for processing and
  - f) be processed in a manner that ensures its security.
3. This policy updates any previous data protection policy and procedures to include the additional requirements of GDPR which apply in the UK from 25<sup>th</sup> May 2018.
4. The Government has confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement.
5. This policy explains the duties and responsibilities of the Council and it identifies how the Council will meet its obligations.

### **Identifying the roles and minimising risk**

6. GDPR requires that everyone within the Council must understand the implications of GDPR and that roles and duties must be assigned.
7. The Council is the data controller and the Clerk is the Data Protection Officer (DPO). The administrative team are data processors working under the DPO.
8. It is the DPO's duty to undertake an information audit and to manage the information collected by the Council, the issuing of privacy statements, dealing with requests and complaints raised and the safe disposal of information. This will be included in the Job Description of the Clerk.
9. Appointing the Clerk as the DPO must avoid a conflict of interests, in that the DPO should not determine the purposes or manner of processing personal data.
10. GDPR requires continued care by everyone within the Council, councillors and staff, in the sharing of information about individuals, whether as a hard copy or electronically.
11. A breach of the regulations could result in the Council facing a fine from the Information Commissioner's Office (ICO) for the breach itself and to compensate the individual(s) who could be adversely affected.
12. Therefore, the handling of information is seen as high / medium risk to the Council (both financially and reputationally) and one which must be included in the Council's

Risk Register.

13. Such risk can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (an audit of potential data protection risks with new projects), minimising who holds data protected information and the Council undertaking training in data protection awareness.

### **Data breaches**

14. One of the duties assigned to the DPO is the investigation of any breaches.
15. Personal data breaches should be reported to the DPO for investigation. The DPO will conduct this with the support of the Executive Committee.
16. Investigations must be undertaken within one month of the report of a breach.
17. Procedures are in place to detect, report and investigate a personal data breach.
18. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage.
19. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will also have to notify those concerned directly.
20. It is unacceptable for non-authorised users to access IT using employees' log-in passwords or to use equipment while logged on.
21. It is unacceptable for employees, volunteers and members to use IT in any way that may cause problems for the Council, for example the discussion of internal Council matters on social media sites could result in reputational damage for the Council and to individuals.

### **Privacy Notices**

22. Being transparent and providing accessible information to individuals about how the Council uses personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR).
23. The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what a Council does with their personal information.
24. A privacy notice will contain the name and contact details of the data controller and Data Protection Officer, the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information.
25. Issuing of a privacy notice must be detailed on the Information Audit kept by the Council. The Council will adopt a privacy notice to use, although some changes could be needed depending on the situation, for example where children are involved.

### **Information Audit**

26. The DPO must undertake an information audit which details the personal data held, where it came from, the purpose for holding that information and with whom the

Council will share that information.

27. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the Council undertakes a new activity.
28. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted.

## **Individuals' Rights**

29. GDPR gives individuals rights with some enhancements to those rights already in place:

- a. the right to be informed
- b. the right of access
- c. the right to rectification
- d. the right to erasure**
- e. the right to restrict processing
- f. right to data portability**
- g. the right to object
- h. the right not to be subject to automated decision-making including profiling.

30. The two enhancements of GDPR are that individuals now have a right to have their personal data erased (sometimes known as the 'right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected, and data portability must be done free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.
31. If a request is received to delete information, then the DPO must respond to this request within a month. The DPO has the delegated authority from the Council to delete information.
32. If a request is considered to be manifestly unfounded then the request could be refused, or a charge may apply. The charge will be as detailed in the Council's Freedom of Information Publication Scheme. The Executive Committee will be informed of such requests.

## **Children**

33. There is special protection for the personal data of a child.
34. The age when a child can give their own consent is 13. Consent forms for children aged 13 plus, must be written in language that they will understand.
35. If the Council requires consent from young people under 13, the Council must obtain a parent or guardian's consent in order to process the personal data lawfully.

## **Summary**

The main actions arising from this policy are:

36. The Council must be registered with the ICO.

37. A copy of this policy will be available on the Council's website. The policy will be considered as a core policy for the Council.
38. The Clerk's Contract and Job Description (if appointed as DPO) will be amended to include additional responsibilities relating to data protection.
39. An information audit will be conducted and reviewed at least annually or when projects and services change.
40. Privacy notices must be issued.
41. Data Protection will be included on the Council's Risk Register.
42. The Executive Committee, with Terms of Reference, will manage the process.
43. This policy document is written with current information and advice. It will be reviewed at least annually or when further advice is issued by the ICO.
44. All employees, volunteers and councillors are always expected to comply with this policy to protect privacy, confidentiality and the interests of the Council.
45. This Policy is supported by the Terms of Reference for the Executive Committee responsible for GDPR (Appendix A).
46. This Policy is also supported by a GDPR awareness checklist (Appendix B) to help councillors comply with GDPR. Members will be asked to read and sign the checklist to demonstrate they understand their responsibilities as a Town Councillor for protecting personal data. This checklist will be incorporated into the councillor induction pack.

## **Appendix A**

### **EXECUTIVE COMMITTEE**

#### **ADDITIONAL TERMS OF REFERENCE FOR DATA PROTECTION**

##### **Name**

The Executive Committee will be responsible for managing the Data Protection requirements.

##### **Meetings**

The Committee will consider Data Protection at a minimum of one meeting annually. Minutes are presented to the next Full Council meeting by the Chairman of the Committee for adoption by the Council.

##### **Membership**

The Committee will be made up of a minimum of 6 councillors [including the Town Mayor and Council Leader]. The Committee and its Chairman will be appointed at the Annual Town Council meeting.

The Committee may set up a sub-group or working party to support its aims.

##### **Aims and Objectives**

The Committee aims:

- To determine the purpose and manner of processing personal data according to the law
- To ensure that the Clerk as Data Protection Officer (DPO) has no conflict of interest with this process
- To ensure that councillors and staff receive ongoing and appropriate training for Data Protection
- To conduct a survey of the Information Audit, Privacy Notices and any Risk Management to ensure compliance with Data Protection
- To receive any reports from the DPO of any manifestly unfounded requests and confirm action to be taken
- To receive reports from the DPO of any investigation of breaches which might need to be undertaken
- To make an annual review of the GDPR Policy and recommend any changes to Council which might be required
- To recommend to Council any changes which may be required in Standing Orders in respect of DP
- To recommend to Council any changes which may be required to the Job Description and Contract of Employment for the Clerk / DPO.

##### **Budget**

The Committee will recommend any budgetary needs to the Council in respect of the administrative and staffing costs to implement and maintain Data Protection requirements.

### General Data Protection Awareness Checklist for councillors

Individual Diss Town councillors need to ensure that they protect an individual's personal data whether it is stored electronically or as a hard copy. This applies only to living individuals (not the deceased, companies, other authorities and charities).

Personal data includes:

- Names and addresses
- Telephone numbers
- Email addresses
- IP addresses

The following measures are recommended to help councillors comply with GDPR:

Action	Noted (Please tick)
Each new councillor is set up with a separate diss.gov.uk email account for Town council correspondence separate from personal email	
Ensure that all devices (computers, laptops, phones) are password protected	
Do not forward on emails or email threads that may contain personal data	
Review any hardcopy information and if no longer relevant destroy using a suitable method (crosscut shredder or destruction service). Ensure Clerk is aware of actions before destruction.	
Where possible direct all correspondence to the Clerk who can obtain the necessary consent	
Where possible avoid holding an individual's information in a councillor's home or on a councillor's own PC. If a councillor has to hold any information containing personal data on behalf of the Town Council, it needs to be stored securely in a locked room or cabinet or if on a PC, in an encrypted folder or drive.	
Make sure your antivirus software and operating system is up-to-date	
Make sure your computers and router's firewall is turned on	
Ensure the Data Protection Officer of any breaches within 48 hours.	
Ensure that all hard copies of data held at home during homeworking is kept in a locked secure cupboard.	

I confirm that I have read the information above and understand my responsibility as a Town councillor for protecting personal data.

NAME:

Signed:

Date: