



## Draft/Staff Data Protection Training Policy

<b>Organisation Issue No:</b> 0001	<b>Organisation Issue Date:</b> / / 2020
<b>Author and Document Owner:</b> Data Protection Officer and Head of HR are the owners of this document and are responsible for keeping it up to date.	<b>Authorised by:</b> This policy has been approved by way of Executive Decision in xxx 2020

## Contents

1. Introduction.....	3
2. Responsibility .....	3
3. Scope.....	3
4. Purpose .....	4
5. Frequency of Training .....	4
6. Training for Data Users .....	4
7. Training for Non-Data Users.....	6
8. Publication.....	6

## 1. Introduction

- 1.1 This policy represents part of Hertsmere Borough Council (hereafter "The Council") overriding Data Protection Policy. It should therefore be read in conjunction with the Data Protection Policy and any sub-policies and documents listed within.
- 1.2 Everyone has rights with regard to the way in which their personal data is handled. During the course of The Council's activities we will collect, store and process personal data.
- 1.3 The Council is committed to providing adequate data protection training to its employees in order to help protect the rights and freedoms of individuals in accordance with the provisions of GDPR, Data Protection Act 2018 and best practice.

## 2. Responsibility

- 2.1 The responsibility for the production and maintenance of this document is with the Data Protection Officer and HR. They will also ensure that any substantive changes made will be communicated to all relevant personnel.
- 2.2 It is the responsibility of the Data Protection Officer and HR to ensure that Data Protection training is made available to all new employees as part of their induction program and employees are provided with regular refresher training to include any updates or changes.
- 2.3 It is the responsibility of all Service Heads that all new employees have completed the Data Protection training within 4 weeks of commencing their role and that all employees are complete refresher training which includes any updates or changes.

## 3. Scope

- 3.1 This policy applies to The Council's training and awareness programme relevant to the GDPR compliance and other matters relating to data protection and privacy.

3.2 This policy applies to all permanent, temporary, casual, work experience volunteers, agency or contracted employees (hereafter "Employees") of The Council.

## 4. Purpose

4.1 The purpose of this policy is to set out the training that staff will be provided with to ensure that all handling of personal data is compliant with the provisions of GDPR, Data Protection Act 2018 and best.

## 5. Frequency of Training

5.1 Training required by this policy should be provided to all new Employees as part of their induction program and must be completed within 4 weeks of commencing their role

5.2 All existing Employees shall also be provided with the training required by this policy unless this has been provided to them already.

5.3 All Employees shall receive a refresher of relevant training at least every twelve months or following a material change in GDPR, Data Protection Act 2018 and best data

5.4 HR shall keep a record of what training has been undertaken by each data user.

## 6. Training for Data Users

6.1 The Data Protection Officer assigns data protection responsibilities to Employees in relation to The Council's policies and procedures on personal data management.

6.2 The data Protection Officer and HR shall make available to all Employees training on their responsibilities under The Council's Data Protection Policy and all of its listed sub-policies and supporting procedures. This will include guidance on:

6.2.1 Data Protection Principles:

6.2.1.1 what data processing is;

6.2.1.2 how personal data must be handled in accordance with the data protection principles;

6.2.1.3 awareness that failure to comply with the information governance requirements contained in The Council's policies may result in disciplinary action; and

6.2.1.4 the possibility that they may commit criminal offences if they deliberately try to access, or to disclose, personal data without authority.

#### 6.3 Day to day office security:

6.3.1 personal desk and work area management;

6.3.2 implementation of a Clear Desk, Clear Screen Policy or the placing of personal data in a locked filing cabinet at the end of each day ;

6.3.3 the disposal of confidential waste;

6.3.4 password management and Password Policy;

6.3.5 how to access and exit the premises;

6.3.6 visitor security and management;

#### 6.4 Data Breach and Incident Reporting:

6.4.1 how to identify a possible data breach;

6.4.2 how suspected and actual security breaches affecting our systems should be dealt with;

6.4.3 how to report a possible data breach and comply with the Council's Security Incident Management Procedure; and

6.4.4 Specific training for those responsible for handling actual or suspected security breaches; ICO guidance on the handling of data security breaches and the notification of such breaches to the ICO.

#### 6.5 Email usage and document protection:

6.5.1 how all employees should use email;

6.5.2 where when and how encrypted email should be used;

#### 6.6 Data subject access requests:

6.6.1 understanding what a Subject Access Request (SAR) is; and

6.6.2 what action needs to be taken when a SAR is received.

6.7 tailored training will be given to those Employees who undertake investigation on understanding the lawful reasons for undertaking an investigation;

6.8 the purposes for which personal data can be processed;

6.9 the purposes for which sensitive personal data can be processed;

- 6.10 understanding why and where privacy impact assessments must be undertaken;
- 6.11 how to undertake a Privacy Impact Assessment and comply with the Council's Data Protection Impact Assessment Procedure;
- 6.12 additional training will be given to those who are responsible for marketing and communications on:
  - 6.12.1 what personal data The Council process;
  - 6.12.2 what consent is required to email a potential customer;
  - 6.12.3 how to obtain consent;
  - 6.12.4 when and how privacy notices need to be provided to data subjects; and
  - 6.12.5 what information should be included in a privacy notice.
- 6.13 Tailored training will be provided to those Employees at The Council who are responsible for advising The Council's staff and officers about compliance with employment law obligations or personnel management.

## 7. Training for Non-Data Users

- 7.1 The Data Protection Officer assigns data protection responsibilities to Employees in relation to The Council's policies and procedures on personal data management.
- 7.2 All Employees whose work does not ordinarily involve accessing personal data and all employees who do not have a work email account shall receive a copy of the Council's Data Protection awareness leaflet.

## 8. Publication

- 8.1 This policy will be published on The Council's intranet. All Heads of Service should ensure that Employees, understand their roles in implementing this Policy through trainings, communications, and team meetings.