New Forest DISTRICT COUNCIL

# DATA PROTECTION POLICY

**Dated: 10/2018**

**Lasted updated: 08/2022**

CONTENTS

## 1. INTRODUCTION

1.1 The purpose of this policy is to set out how the Council will comply with its obligations as a Data Controller in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and other applicable legislation and guidance ('the Data Protection Legislation').

1.2 This overarching policy is supported by a number of other appropriate policy documents which are listed in section 23 of this policy.

1.3 The policy forms part of the appropriate organisational measures which the Council has adopted in order to ensure that the rights and freedoms of natural persons with regard to the protection of their personal data.

1.4 The Council supports the accountability principle contained in the UK GDPR that data protection should be 'by design' and 'by default' and as such, the Council is committed is ensuring that data protection is embedded within the organisation and underpins everything it does.

## 2. SCOPE

2.1 This policy applies to employees, agency staff and Members ('employees') and third party contractors. It covers all personal data the Council processes.

2.2 Personal data is defined as '*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.'

2.3 The processing of personal data covers everything the Council does with any personal data, about a living individual, and can include collecting, recording, organising, storing, sharing, copying, using and destruction.

2.4 This policy applies to personal data in hard copy or electronic format and covers the Council's corporate databases, computer network and paper records. It covers videos and photographs, voice recordings, CCTV and mobile devices such as laptops, mobile phones, memory sticks and computerised hand held devices.

## 3. ROLES AND RESPONSIBILITIES

3.1 The Council is a data controller which means that it determines the purposes and means of processing personal data. Accordingly, the Council is accountable for its handling of personal data. The Council is registered as a data controller with the United Kingdom's supervisory body, the Information Commissioner's Office ('ICO').

3.2 There will also be instances where the Council is a data processor, because it processes personal data on behalf of another data controller.

3.3 **Executive Management Team ('EMT'):**

3.3.1 EMT is responsible for approving, endorsing and monitoring compliance with this policy.

3.3.2 The Executive Head with special responsibility for data protection is the Executive Head of Governance and Housing.

3.3.3 EMT will receive updates from the Council's Information Governance and Complaints Manager (and Data Protection Officer) ('DPO')) on data protection within the Council.

3.4 **Service Managers (including managers who report directly to EMT)**:

3.4.1 Each Service Manager will be responsible for ensuring compliance with this policy, and the Data Protection Legislation, within their Service. This will include:

a) Ensuring this policy is implemented in their Service and complied with;

b) Ensuring that all appropriate documents are prepared in accordance with the Data Protection Legislation including privacy notices, consent forms, data protection impact assessments ('DPIAs'), retention and destruction schedules and information sharing and processing agreements;

c) Ensuring data security breaches in their Service are reported to the DPO without delay and that any learning identified from breaches is implemented;

d) Identifying contracts within their Service which relate to the processing of personal data;

e) Making officers in their Service aware of the requirements of the Data Protection Legislation;

f) Identifying training needs within their Service and ensuring all employees undertake appropriate training in accordance with this policy;

3.5 **Data Protection Officer:**

3.5.1 The Council, as a public authority, is required to appoint a DPO. The DPO is the Information Governance and Complaints Officer and their duties include:

a) informing and advising employees about their obligations to comply with the Data Protection Legislation;

b) monitoring compliance with the Data Protection Legislation, including managing internal data protection activities; raising awareness of data protection issues, training employees and conducting internal audits;

c) advising on, and monitoring, DPIAs;

d) cooperating with the ICO; and

e) being the first point of contact for the ICO and for individuals whose data is processed.

3.5.2 The DPO is assisted by other employees in the Information Governance and Complaints Team including the Information Compliance and Complaints Officers and Information Governance and Complaints Assistant. The DPO, and other members of the team, can be contacted at data.protection@nfdc.gov.uk.

3.5.3 A central log of all compliance documentation should be kept by the Information Governance and Complaints Team.

3.5.4 The DPO will report to EMT twice per year on all information governance matters (including data protection).

3.6 **Data Protection Leads ('DPLs')**

3.6.1 All Service Managers are required to nominate a DPL for each of their business areas (or one DPL to cover multiple business areas).

3.6.2 DPLs are a point of contact for the Information Governance and Complaints Team.

3.6.3 DPLs are required to have good knowledge of the practices of their business areas/ Services, personal data processed, and records held.

3.6.4 DPLs will support Service Managers to ensure that personal data within their Service is handled appropriately.

3.7 **Elected Members:**

3.7.1 Elected Members must comply with the Data Protection Legislation and this policy in the exercise of their duties as Members of the Council.

3.7.2 Additionally, where Members represent the residents of their ward they will be data controllers in their own right. In this instance, the member must ensure that they comply with all of the obligations placed on them as a data controller.

3.7.3 Members may also process personal data as a representative of their respective political party.

3.8 **All employees:**

3.8.1 All employees have a responsibility to comply with the Data Protection Legislation.

3.8.2 All employees must read, be familiar with and comply with this policy and undertake the appropriate training.

## 4. PERSONAL DATA AND SPECIAL CATEGORIES DATA

4.1 The definition of personal data is contained in paragraph 2.2 of this policy. Personal data includes any information relating to an identifiable living person.

4.2 Examples of personal data include:

- Name, address, telephone number, personal email address;
- Financial information (eg, bank details, or information about a person's financial situation);
- A national insurance number/ account reference number;
- Vehicle registration number;

- CCTV images (where a person/ people can be identified from them).
- A photograph (where a person/ people can be identified it).
- A letter from or about an individual.
- IP address

4.3 Personal data can also include an expression of an opinion about the data subject and an indication of an intention regarding a data subject.

4.4 Special categories data is identified separately in the Data Protection Legislation because additional conditions need to be applied before it can be processed.

4.5 The UK GDPR defines special category data as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data (e.g DNA);
- biometric data (where used for identification purposes) (e.g. finger prints or eye scans);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

## 5. DATA PROTECTION PRINCIPLES

5.1 The Council applies the data protection principles in its processing of personal data. These principles are set out in the Data Protection Legislation. The seven principles are that personal data should be:

1. Processed lawfully, fairly and in a transparent manner ('lawfulness, fairness, transparency').
2. Collected for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes ('purpose limitation').
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
4. Accurate and, where necessary, kept up to date ('accuracy').
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation').
6. Processed in an appropriate manner to maintain security and ensure against unauthorised processing or accidental loss/damage Lawful basis of processing

personal data ('data security').

7. In addition, the Council *'shall be responsible for, and be able to demonstrate compliance with…*' all the above principles ('accountability')

## 6. LAWFUL BASIS OF PROCESSING PERSONAL DATA

6.1 There are different lawful reasons for processing personal data and special categories of personal data. The Council always uses at least one lawful basis for processing personal data and where there is processing of special category data an additional lawful basis will also be used.

6.2 The Council must always demonstrate it processes information with safeguards in place to protect the fundamental rights and interests of the data subject.

6.3 The six lawful bases for processing personal data are:

a) An individual has given **consent** for the processing of his or her personal data, and it is freely given, specific, informed, and there must be an indication signifying agreement;

b) The Council has a **contract** with a person and need to process their personal data to comply with its obligations under the contract; or we haven't yet got a contract with the person, but they have asked us to do something as a first step (e.g. provide a quote) and we need to process their personal data to do what they ask;

c) The Council is obliged to process personal data to comply with a **legal obligation**.

d) The processing of personal data is necessary to protect an interest essential to the life of the data subject or another person, known as someone's **vital interests**.

e) The processing of personal data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council; **public task**.

f) The processing of personal data is in the **legitimate interests** of the Council, where the Council uses personal data in ways that people would reasonably expect and that have a minimal privacy impact. However, as a public authority, the Council can only rely on the legitimate interests lawful basis if it is processing for a legitimate reason other than performing its tasks as a public authority**.**

6.4 There are ten lawful bases for the processing of special category data:

a) An individual has given **explicit consent** to the processing of personal data for one or more specified purposes, except where limited by law;

b) The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Council or the data subject under **employment, social security and social protection law** or a collective agreement under law;

c) The processing of personal data is necessary to protect the **vital interests** of a person where the person is physically or legally incapable of giving consent;

d) The processing of personal data is in the legitimate interests of the Council, where it uses personal data in ways that people would reasonably expect and that have a minimal privacy impact. However, public authorities are more limited than private organisations in their ability to rely on this basis for processing personal data;

e) The processing relates to personal data which are manifestly made public by the data subject;

f) The processing is necessary for the establishment, exercise or defence of **legal claims** or whenever courts are acting in their judicial capacity

g) The processing is necessary for reasons of **substantial public interest** under law;

h) The processing is necessary for the purposes of **preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional and subject to the duty of confidentiality;

i) The processing is necessary for reasons of **public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, subject to the duty of confidentiality;

j) The processing is necessary for **archiving** purposes in the public interest, scientific or historical research purposes or statistical purposes.

6.5 For more information see the Council's Protecting Special Category Data Policy which is the '*appropriate policy document'* required by the Data Protection Legislation for this processing.

## 7. CONSENT

7.1 The Council must ensure that where it relies on consent or explicit consent as the lawful basis for processing, it should do this by offering individuals real choice and control. The Data Protection Legislation defines consent as *'any freely given, specific, informed and unambiguous indication of the data subject'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'.*

7.2 The following is a guide which should be followed when obtaining consent:

- The Council should avoid making consent to processing a precondition of a service.

- Any requests for consent should be clear and concise and they should be separate from other terms and conditions.

- The Council must demonstrate consent was given. It should be a clear indication via affirmative action so, for example, pre-ticked boxes not permitted.

- The Council should ensure that consent is specific and 'granular' so that separate consent is obtained for separate things.

- Any third parties (i.e. other groups or organisations) who will rely on the consent should be named.

- Consent can be withdrawn at any time and must be as easy to withdraw as it was to give. Data subjects must be made aware of this right.

- The Council will keep evidence of consent (who, when, how, and what the data subject was told). Consent should be kept under review, and updated if anything changes.

- The Council cannot make performance of a contract conditional upon consent.

- Consent may not be valid if there is a substantial power imbalance between parties. The Council, as a public authority (and in its capacity as an employer), will need to take extra care to demonstrate that consent is freely given and there should not be an overreliance on consent.

- For explicit consent the Council will ensure the individual provides a very clear and specific statement of consent.

## 8. LEGITIMATE INTERESTS

8.1 In the limited instances where the Council can rely on the legitimate interests lawful basis (processing for a legitimate reason other than performing the Council's tasks as a public authority), a Legitimate Interests Assessment ('LIA').

8.2 For the LIA, the Council must:

- identify a legitimate interest - this may be the Council's own interests, or the interest of a third party and can include commercial interests, individual interests or broader societal benefits.

- show that the processing is necessary to achieve it - If the Council can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.

- balance it against the individual's interests, rights and freedoms – if the data subject would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override the Council's legitimate interests.

8.3 For more information and guidance, please see the Council's internal LIA guidance.

## 9. DUTY OF CONFIDENTIALITY

9.1 All Council employees abide by a common law duty of confidentiality. This means that personal information that has been given to an employee by an individual, or otherwise in the course of their role, should not be used or disclosed further, except as originally understood by that individual, or with their permission.

## 10. CRIMINAL OFFENCE DATA

10.1 The UK GDPR gives extra protection to *'personal data relating to criminal convictions and offences or related security measures*; criminal offence data.

10.2 This covers a wide range of information about offenders or suspected offenders in the context of:

- criminal activity;
- allegations;
- investigations; and
- proceedings.

10.3 It includes not just data which is obviously about a specific criminal conviction or trial, but may also include personal data about:

- unproven allegations; and
- information relating to the absence of convictions.

10.4 It also covers a wide range of related security measures, including:

- personal data about penalties;
- conditions or restrictions placed on an individual as part of the criminal justice process; or
- civil measures which may lead to a criminal penalty if not adhered to.

10.5 The Council, as a public body, has the power to process criminal offence data in limited circumstances, for example, in accordance with its legal obligations and because it has legal authority in certain areas for enforcement including, for example, preventing fly-tipping, upholding food hygiene and the licensing of taxi and private hire vehicles, pubs and clubs.

10.6 For more information see the Council's Law Enforcement (Data Protection) Policy which is the '*appropriate policy document'* required by the Data Protection Legislation for this processing.

## 11. SURVEILLANCE

11.1 The Council operates CCTV for public safety. The Council has a CCTV policy which confirms that the Council will comply with the 'Guidance on Video Surveillance' issued by the ICO and the requirements of the Data Protection Legislation.

11.2 The Council can use the Regulation of Investigatory Powers Act 2000 ('RIPA') to conduct covert surveillance involving directed surveillance or the use of a covert human intelligence source ('CHIS'). When these powers are used the Council complies with the Codes of Practice that are overseen by the Investigatory Powers Commissioner's Office.The surveillance must be authorised by a Magistrate. The Council's Audit Committee receives an annual update and monitors the use of such powers.

## 12. HOW THE COUNCIL HANDLES PERSONAL DATA – PRIVACY NOTICES

12.1 The Council provides privacy notices, which are statements to data subjects about the collection and use of their personal data. This is an automatic right, in accordance with the right to be informed in the Data Protection Legislation and does not need to be requested. This is important for transparency.

12.2 Data subjects must be provided with a privacy notice which sets out specific information regarding the use of their personal data, either at the point the data is collected or as soon as possible after. Where the Council obtains personal data from other sources, individuals are provided with the privacy information within a reasonable period of obtaining the data and at the very least, within one month.

12.3 Each of the Council's privacy notices should:

- Be concise;
- Be transparent;
- Be intelligible;
- Be easily accessible; and
- Use clear and plain language.

12.4 The privacy notices should include:

- The name and contact details of the Council.
- The contact details of the DPO
- The purposes of the processing.
- The lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations (if applicable).

- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with the ICO.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

12.5 The Council has a corporate privacy notice which is supplemented by additional privacy notices relevant to each Service/ business area of the Council. This information is on the Council's website, and individuals are referred to it at the time personal data is collected from them.

12.6 Each Service within the Council is responsible for the preparation of their privacy notice(s).

12.7 For more information and guidance, please see the Council's internal Privacy Notice Guidance.

## 13. INDIVIDUAL RIGHTS

13.1 Individuals whose data is processed by the Council have a number of rights in law. These are as follows:

- The right to be informed – privacy notices.
- The right of access – the right to copies of personal data.
- The right to rectification – the right to correct errors in personal data.
- The right to erasure – the 'right to be forgotten'.
- The right to restrict processing – the right to have personal data quarantined in an area where we no longer are processing it but it is still accessible.
- The right to data portability – the right a copy personal data in a commonly used electronic format or to request that it is provided directly to another organisation.
- The right to object – the right to object to certain reasons we are relying on in order to process personal data.
- Rights in relation to automated decision making and profiling.

13.2 It is important that all employees recognise when an information rights request is made to them. Requests do not have to state what they are or reference data protection. Requests can be made verbally or in writing.

13.3 Requests should, ordinarily, be dealt with within one month.

13.4 All requests should be logged with the Information Governance and Complaints Team.

13.5 For more information see the Council's Information Rights Policy.

## 14. INFORMATION SHARING

14.1 The Council believes that the duty to share information can be as important as the duty to protect information. However, all personal data sharing must be in compliance with the Data Protection Legislation.

14.2 The Council complies with the ICO's 'Data sharing: Code of Practice'. This provides that:

- Data Protection Legislation facilitates data sharing when it is approached in a fair and proportionate way.
- Data Protection Legislation is an enabler for fair and proportionate data sharing, rather than a blocker. It provides a framework to help make decisions about sharing data.
- Data sharing has benefits for society as a whole.
- Sometimes it can be more harmful not to share data.

14.3 When considering sharing personal data it is good practice to have a data sharing agreement in place. Each Service within the Council is responsible for the preparation of their sharing agreements.

14.4 A DPIA can be used to assess the risks of the data sharing and measures required to be put in place to mitigate those risks.

14.5 When sharing personal data, the Council must follow the key principles in the Data Protection Legislation:

- The accountability principle means that the Council is responsible for compliance, and must be able to demonstrate that compliance.
- personal data must be shared fairly and transparently.
- There must be at least one lawful basis for sharing data before any sharing commences.
- The Council must process personal data securely, with appropriate organisational and technical measures in place.

14.6 It is possible to share personal data in an emergency, as is necessary and proportionate. Examples of an emergency situation are the risk of serious harm to human life, or the immediate need to protect national security. Personal data can also be shared for safeguarding requirements in accordance with the Council's Safeguarding Policy.

14.7 For more information see the Council's internal guidance on Data Sharing.

## 15. TRANSFERS TO OTHER COUNTRIES

15.1 The Council shall only process personal data in the UK, save for in exceptional circumstances.

15.2 However, when personal data is transferred outside of the UK, the Council will assure itself that there is a level of adequacy in the data protection arrangements of that country.

## 16. DATA PROTECTION BY DESIGN AND BY DEFAULT

16.1 The Data Protection Legislation requires the Council to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is '*data protection by design and by default'*.

16.2 In essence, this means the Council should integrate or '*bake in'* data protection into its processing activities and business practices, from the design stage right through the lifecycle.

16.3 Data protection by default requires the Council to ensure that it only process the data that is necessary to achieve its specific purpose. It links to the fundamental data protection principles of data minimisation and purpose limitation.

## 17. DATA PROTECTION IMPACT ASSESSMENTS

17.1 The Council requires all employees to consider whether it is necessary to conduct a DPIA if they propose to introduce new technologies, or commence a new project or changes to the processing of personal data.

17.2 A DPIA must be carried out for processing that is likely to result in a high risk to individuals. It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

17.3 Each DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

17.4 The DPO should be consulted on DPIAs at an early stage and the DPIA process should be built into the Council's Project Management Guidance.

17.5 The Council's DPIAs are living documents to be revised and updated whenever necessary.

17.6 For more information see the Council's internal DPIA Guidance and template.

## 18. DATA PROCESSORS

18.1 In accordance with the Data Protection Legislation all data processors used by the Council will be subject to a written contract. Where the Council has a contractual

relationship with another organisation or individual, we will ensure we are clear about the contractor's role, responsibilities and accountability in relation to personal information.

18.2 Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the Council.

18.3 Contracts must also include as a minimum the following terms, requiring the processor to:

- only act on the written instructions of the Council;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the Council and under a written contract;
- assist the Council in providing subject access and allowing data subjects to exercise their rights under the UK GDPR;
- assist the Council in meeting its data protection obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections and provide the Council with whatever information it needs to ensure compliance with the Data Protection Legislation.

18.4 The Council has model data processing agreements to be used a) where there is a principal contract in place and b) where there is no principal contract in place. Where a contract includes data processing provisions, these should be checked by the Information Governance and Complaints Team.

18.5 For more information see the Council's internal Data Processing Agreement Guidance and Templates.

## 19. RETENTION AND DESTRUCTION AND RECORD OF PROCESSING ACTIVITIES ('ROPA')

19.1 The basis for the Council's approach to the retention and destruction of all records is that records should be kept for as long as they are needed. There are a number of factors to take into consideration in setting retention periods for records. These include:

- Whether there is a requirement for retention for the purposes of reference or accountability;
- Regulatory and statutory retention requirements;
- The protection of legal rights and interests;
- Ensuring the Council's storage and electronic storage systems are efficiently utilised; and

- Importantly, where records contain personal data, ensuring that personal data is not kept for longer than is necessary.

19.2 Common Practice and Local Government Guidance will be used as guidance for retention periods but will not be binding.

19.3 The Council has a Corporate Retention and Destruction Schedule which identifies whether a record contains personal data.

19.4 The Council also maintains a ROPA which documents the following information, as a minimum for all processing that the Council undertakes:

- The name and contact details of the Council and the DPO.
- The purposes of processing.
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of any transfers to third countries including documenting the transfer mechanism safeguards in place, where applicable.
- Retention information.
- A description of the technical and organisational security measures in place.

## 20. INFORMATION SECURITY

20.1 The Council has an Information, Communications and Technology Security Policy and Guidance. The Council also has a Human Resources Management Advice Note on Acceptable Use of ICT. The purpose of these policies is to take appropriate technical and organisational measures to protect personal data.

20.2 The Council obtains independent assurance of its information security and complies with the information security standards of the Public Service Network.

20.3 The Council has Cyber Essentials Accreditation.

20.4 The Council meets the standards of PCI-DSS, which is the standard for protecting credit and debit card payments.

## 21. PERSONAL DATA BREACHES

21.1 A personal data breach means '*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes'.*

21.2 The Council aims to prevent personal data breaches, but when these occur, there is a Data Security Breach response plan. Breaches should be reported to the DPO, or another member of the Information Governance and Complaints Team in their absence. All employees must ensure that they recognise when a breach has occurred and report it without any delay.

21.3 If a breach results in a risk to the rights and freedoms of an individual, it will be reported to the ICO within 72 hours.

21.4 If a breach is likely to result in a high risk to the rights and freedoms of an individual, the Council must inform those data subjects concerned directly and without undue delay.

21.5 The Council will maintain a central log of data security breaches, identifying the relevant Service, how the breach occurred, any action taken and any learning identified as a result of the breach.

21.6 Where it is not considered that the threshold to report a breach to the ICO has been met, the Council will prepare an internal report.

## 22. TRAINING

22.1 The Council is committed to ensure that all employees are trained on their responsibilities for data protection.

22.2 All employees with access to the Council's IT systems are required to undertake a Data Protection eLearning module which can be accessed on Forestnet.

22.3 The module must be carried out by all employees as part of their induction programme and then every two years.

22.4 Operational employees who do not have access to the eLearning module will be given appropriate training through alternative methods, at the same time intervals.

22.5 Training will be provided to Members by the Information Governance and Complaints Team on election and then midterm, with the opportunity for additional training as required.

22.6 DPLs will also be required to attend additional training every two years.

22.7 Completion of training will be monitored.

22.8 The DPO and other members of the Information Governance and Complaints Team are available to support employees with their training needs and group training sessions can be arranged at the request of each Service.

## 23. RELATED POLICIES AND DOCUMENTS

23.1 This policy is supported by a number of other policies/ documents which relate to the Council's overall approach to information management.

23.2 These other policies/ documents include the following:

- Protecting Special Category Data Policy;
- Law Enforcement (Data Protection) Policy;
- Corporate Retention and Destruction Schedule;
- Information Rights Policy;
- Breach response Plan;

- ROPA
- Access to Information Policy;
- Internal guidance documents:
    - Privacy notices
    - Data sharing
    - Data processing
    - LIAs
    - DPIAs

## 24. FOR FURTHER INFORMATION

- Regulation (EU) 2016/679 (General Data Protection Regulation)
- Data Protection Act 2018
- Information Commissioner's Office: www.ico.org.uk
- Forest Net: Data Protection Guidance Page

## 25. REVIEW OF POLICY

25.1 EMT is responsible for approving this policy.

25.2 This policy will be reviewed annually by the DPO.

25.3 Changes to the supporting policies, relevant legislation or guidance may require further reviews within this period.

25.4 Where minor changes are required to this policy, or supporting policies/ guidance/ documents, these will be made by the DPO in consultation with the Executive Head of Governance and Housing.