APPENDIX A

FOREST HEATH DISTRICT COUNCIL

Data Protection Policy

Forest Heath

District Council

1. Executive Summary

1.1 This policy outlines the principles of the **Data Protection Act 1998 (DPA)** and identifies how Forest Heath District Council (the Council) complies with the Act. It aims to give guidance on how the requirements of the Act apply to the work of the Council.

1.2 This policy covers all personal data that the Council holds in either electronic or paper format, and applies throughout the life cycle of the data from the time it is created or arrives within the Council, to the time it is either destroyed or permanently preserved.

1.3 This policy applies equally to all staff on a contract, individuals who work for, or on behalf of, the Council including agency staff, contractors and also Members.

1.4 This policy also:

- Identifies responsibilities for data protection; and
- Gives more specific guidance on the following areas:
  - Notification to the Information Commissioner
  - Sensitive personal data
  - Staff records and monitoring
  - Use of CCTV
  - Retention and disposal of personal data
  - Subject access requests
  - Disclosure of data to third parties.
  - Fair processing notices
  - Data breach
  - Training and awareness
  - Security

1.5 Corporate data protection procedures have been developed from this policy which cover the main issues that are likely to arise for staff dealing with personal information under the Act. These procedures are stored on the intranet or can be obtained from Internal Audit.

2. Context

2.1 The DPA balances the legitimate needs of organisations to store and use personal data with the rights of individuals who are the subject of this data. Basically, if an organisation collects or holds information about an identifiable living individual, or if it uses, discloses, retains or destroys that information, it is likely to be processing personal data. The DPA is complex and, in places, hard to understand. However, it is underpinned by a set of eight straightforward, common-sense principles which, if followed will ensure compliance with the DPA.

2.2 Compliance with the DPA is monitored and enforced by the Information Commissioners Office (ICO). The ICO has the power to impose fines

of up to £500,000 for a serious breach of one or more of the data protection principles and where the breach was likely to cause substantial damage or distress. This is in addition to any penalties imposed by the courts against individuals who unlawfully breach the DPA.

2.3 The DPA uses many terms which have a specific meaning in the context of this Act, and therefore a glossary of these terms is included at the end of this policy.

2.4 The Council collects and uses certain types of data about people, in order to continue to provide the level of service expected by the public and to comply with the requirements of government departments. This data includes personal details about current, past, and prospective staff, suppliers, council taxpayers, benefits claimants, council housing and other tenants, residents in Forest Heath and others with whom it communicates.

2.5 As an organisation which deals with personal data the Council will ensure it:

- complies with both the law and best practice;
- respects the rights of individuals;
- is open and honest with individuals whose data is held; and
- provides support and training for those who handle personal data, so that they can act confidentially and consistently.

3. Achieving Compliance with the Data Protection Act

3.1 The main purpose of the eight principles of the DPA is to protect the interests of individuals whose personal data is being processed. They apply to everything the Council does with personal data, except where an exemption applies. The key to complying with the DPA is to follow the eight data protection principles.

3.2 Below is a summary of the eight principles and the ways in which the Council complies with them.

The First Principle – processing personal data fairly and lawfully

3.3 This first principle states that personal data shall be processed fairly and lawfully and in particular, shall not be processed unless:

- at least one of the conditions in Schedule 2 of the DPA is met; and

- in the case of sensitive data, at least one of the conditions in Schedule 3 of the DPA is also met.

3.4 In practice, this means that the Council must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how it intends to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure it does not do anything unlawful with the data.

Further information regarding the conditions for processing referred to above, including an explanation of what they mean in practice is available via the hyperlink to the Information Commissioner's Office (ICO).

Compliance is achieved by:

3.5 Abiding by the law in all activities;

3.6 Ensuring data subjects are aware of how their data will be used at the time they provide it and not using it for any purpose incompatible with the original stated purpose;

3.7 Ensuring the data has been provided by a person who is legally authorised, or required, to provide it;

3.8 Ensuring that any processing of personal or sensitive personal data meets one of the legitimising conditions listed in Schedules 2 and 3 of the DPA; and

3.9 Ensuring that all processing of personal data meets one of the following conditions:

- the data subject has consented to the processing;
- the processing is necessary for completion of a contract between the data subject and the data controller, or to investigate or set up a new contract between the data subject and the data controller;

- the processing is necessary because of a legal obligation which applies to the data controller;

- the processing is necessary to protect the individuals' vital interests;

- the processing is necessary for administering justice or for exercising statutory, governmental or other public functions; or

- the processing is necessary for the legitimate interests of the data controller.

Further information regarding the conditions for processing referred to above, including an explanation of what they mean in practice is available via the hyperlink to the Information Commissioner's Office (ICO).

3.10 Further conditions are in place for sensitive personal data, see section 6 for further guidance.

The Second Principle – processing personal data for specified purposes

3.11 This second principle states that personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3.12 In practice this means that the Council must:

- be clear from the outset about why it is collecting personal data and what it intends to do with it;

- comply with the DPA's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;

- comply with what the DPA says about notifying the Information Commissioner; and

- ensure that if the Council wishes to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

Compliance is achieved by:

3.13 Ensuring that the Council's annual notification to the ICO is up to date and includes all the purposes for processing.

3.14 At the time data is obtained the data subject will be informed of the purpose for which the data is being collected.

3.15 If the Council wishes to use or disclose the data to a third party for any purpose other than that for which the data was obtained, the Council will ensure a data sharing agreement between the two parties is in place beforehand ensuring the data is processed fairly in accordance with the first principle.

3.16 As well as creating a framework for collecting and using personal data, the DPA sets standards that personal data must meet before it can be used. The standards are set out in the third, fourth and fifth principles which are that personal data should be:

3rd principle: adequate, relevant and not excessive;
4th principle: accurate and, where necessary, kept up to date; and
5th principle: kept for no longer than necessary.

The Third Principle – personal data shall be adequate, relevant and not excessive

3.17 This third principle states that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

3.18 In practice, this means the Council shall ensure that it:

- holds personal data about an individual that is sufficient for the purpose for which it is being held in relation to that individual; and
- does not hold more information that the Council needs for that purpose.

<u>Compliance is achieved by:</u>

3.19 Collecting only the minimum amount of personal data required to fulfil legitimate operational needs or to comply with legal requirements. Additional unnecessary data will not be collected and data will not be held on the off-chance that it might be useful in the future.

The Fourth Principle – personal data shall be accurate and, where necessary kept up to date

3.20 This fourth principle states that personal data shall be accurate and, where necessary, kept up to date.

Compliance is achieved by:

3.21 Taking reasonable steps to ensure the accuracy of any personal data ensuring that the source of any personal data is clear; carefully considering any challenges to the accuracy of information; and considering whether it is necessary to update the information.

The Fifth Principle – personal data shall not be kept for longer than is necessary

3.22 This fifth principle states that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

3.23 In practice this means the Council will need to:

- review the length of time it keeps personal data;
- consider the purpose or purposes it holds the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

Compliance is achieved by:

3.24 The Council will hold personal data only as long as it is necessary for the legitimate Council purpose it has been provided/obtained.

3.25 If personal data is collected for a specific project it shall be disposed of as soon as the project comes to an end.

3.26 Compliance with the Council's data retention arrangements. Guidance in this respect is available from Internal Audit.

The Sixth Principle – the rights of data subjects

3.27 The sixth principle states that personal data shall be processed in accordance with the rights of data subjects under the DPA.

3.28 The rights of the data subjects that this refers to are:

- A right of access to a copy of the information comprised in their personal data;
- A right to object to processing that is likely to cause or is causing damage or distress;

- A right to prevent processing for direct marketing;
- A right to object to decisions being taken by automated means;
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- A right to claim compensation for damages caused by a breach of the DPA

Compliance is achieved by:

3.29 The Council will ensure that individual rights are protected in relation to the processing of personal data by the Council. In order to achieve this staff should have sufficient knowledge of data protection to recognise and act on subject access requests (SAR).

3.30 If the Council intends to process personal data for direct marketing, the prior consent of the individuals being marketed must be obtained.

The Seventh Principle- information security

3.31 This seventh principle states that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

3.32 In practice this means the Council must have appropriate security to prevent the personal data it holds being accidentally or deliberately compromised. In particular, the Council will need to:

- design and organise its security to fit the nature of the personal data it holds and the harm that may result from a security breach;
- be clear about who in the Council is responsible for ensuring information security;
- make sure the Council has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

Compliance is achieved by:

3.33 Technical security measures include:

- password protection of computer systems;

- controlled access to Council buildings;
- access rights of users appropriate to the needs of their job; and
- management to ensure that performance with regard to personal data is regularly assessed and evaluated.

3.34 Organisational measures include:

- all staff to have a level of understanding of the DPA commensurate with their duties;
- adequate checks to ensure the suitability of all staff who have access to personal data; and
- management to ensure that everyone managing and handling data is subject to appropriate line management.

3.35 The Council shall have in place appropriate security arrangements both covering physical and electronic security. See section 15 for further details.

The Eighth Principle – sending personal data outside the European Economic Area

3.36 This eighth principle states that personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Compliance is achieved by:

3.37 If the Council transfers information to any country outside the European Economic Area this must be done in a way which is compliant with the DPA.

3.38 Any organisation processing data on behalf of the Council should be contractually bound to follow the principles as described in the DPA.

4. Roles and Responsibilities

4.1 For the purpose of the DPA the data controller is Forest Heath District Council.

4.2 The senior officer with specific responsibility for data protection and therefore overall responsibility for ensuring that the Council is compliant with the DPA (the Council's designated Senior Information Risk Owner) is the Strategic Director (Resources).

Information Governance Group

4.3 The Information Governance Group advises service areas in respect of developing procedures and applying this policy, and ensures that Council employees and members have access to support in terms of training to adhere to the DPA and this policy. In addition, the Information Governance Group is responsible for reviewing this policy.

Heads of Service

4.4 Heads of Service have responsibility for ensuring that their service area complies with the principles of the DPA when processing personal data. This includes ensuring that all staff are aware of their responsibilities under the DPA and trained to discharge those responsibilities.

Staff

4.5 All staff have a responsibility to ensure that they comply fully with the DPA. It is a criminal offence to knowingly or recklessly obtain or disclose personal data. They should not process any personal data unless they are sure that they are authorised to do so. Staff failing to comply with this policy could be subject to action under the Council's disciplinary procedure.

Members

4.6 When handling personal data on Council business, Members must comply with this policy and be aware of their responsibilities as individuals under the DPA. They should be mindful that it can be a criminal offence to process personal data in a manner which they know that they are not authorised to do. A breach of this policy by a Member is a potential breach of the Code of Conduct.

5. Notification

5.1 The ICO maintains a public register of data controllers. The DPA requires every data controller who is processing personal data to notify and review their notification, on an annual basis.

5.2 It is an offence under the DPA if the notification is not kept up-to-date, and also an offence to use personal data in a manner which has not been notified.

5.3 It is the responsibility of all Heads of Service to advise the Senior Information Risk Owner of any changes to the uses of personal data within their service areas as soon as they occur so that the Council's notification can be updated.

5.4 The Council's notification will be reviewed annually and kept up-to-date by the Senior Information Risk Owner.

5.5 A copy of the Council's current notification can be viewed at the Information Commissioner's Web site: www.ico.gov.uk

6. Sensitive Personal Data

6.1 Sensitive personal data is defined in the DPA as data concerning an individual's:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sexual life
- criminal convictions or alleged offences

6.2 Extra care must be taken when processing sensitive personal data as additional requirements under the DPA must be met to ensure that the processing is legitimate and safe. At least one of the legitimising conditions described under the *First Principle,* and also one of the legitimising conditions shown below, must be met:

- the data subject has given their explicit consent;
- the processing is necessary for performing a legal obligation in relation to employment;
- to protect the vital interests of the data subject or another person;
- the processing is carried out as part of the legitimate activities of a not for profit body or organisation;
- the information has been made public by the data subject;
- the processing is necessary in relation to legal rights; or
- the processing is necessary for the administration of justice.

6.3 The advice of the Senior Information Risk Owner or his deputy should be sought before the processing or collection of sensitive personal data for any new purpose commences.

7. Staff Records and the Monitoring of Staff

7.1 The Council should comply with the ICO's *'Employment Practices Code'* in relation to the processing of staff personal data. This Code is intended to help employers comply with the DPA and to encourage them to adopt good practice. The Code aims to strike a balance between the legitimate expectations of staff that personal data about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own organisations carrying out their legitimate business.

7.2 In particular, staff monitoring should only be carried out in accordance with this Code. A copy of this Code is available on the ICO website or from Internal Audit.

8. CCTV Monitoring

8.1 CCTV monitoring must only be carried out in accordance with the ICO's *'CCTV Code of Practice'*. A copy of this Code is available on the ICO website or from Internal Audit.

9. Retention and Disposal of Personal Data

9.1 It is the responsibility of the service areas holding personal data to ensure that the data that they hold is kept accurate and up-to-date, and is not held for any longer than is necessary for the purpose for which it was collected.

9.2 When the data is no longer required the service area must dispose of the data safely. Guidance on retention periods for classes of data is available from Internal Audit.

10. Subject Access Requests

10.1 It is one of the fundamental rights of the individual under DPA that they are able to see copies of any information stored about them. It is in the interests of the Council to have an open and honest approach with all individuals on which we hold data.

10.2 The DPA sets out guidance and a time limit within which a SAR must be answered.

10.3 Any individual requesting access to their personal data should be asked to complete a request in writing which must be referred to the Senior Information Risk Owner. This gives clarity around the date the

request was made and therefore the deadline date and also encourages the individual to think clearly about the data they require. Detailed guidance on responding to a SAR is included within the data protection procedures developed from this policy.

10.4 The Council will approach all requests for data in an open and honest way and seek to ensure that the individual gets all the data they require as long as this is permissible within the law.

10.5 There are cases where it is not possible or appropriate to release personal data, for example, when doing so would involve releasing personal data about another individual, or if the data relates to ongoing criminal investigations. Any concerns about releasing data should be discussed with the Senior Information Risk Owner or his deputy prior to release of the information.

11. Fair Processing Notices (Privacy Notices) and Subject Consent

11.1 Fair processing notices / privacy notices are issued to individuals at the time they provide their personal data to organisations. They are designed to inform the individual of the nature of the processing for which their personal data is collected.

11.2 If consent has to be relied upon to process data then it must be fully informed and freely given. In the case of sensitive personal data it must be explicit consent.

11.3 Where it is possible to obtain explicit written consent to process personal data the Council should aim to do so. This should be taken into account when designing forms or requesting details in any other format.

11.4 Further guidance when collecting information can be found in the data protection procedures developed from this policy.

12. Sharing Personal Data

12.1 Where requests are received from external organisations or third parties for personal data about individuals advice should be sought from the Senior Information Risk Owner or his deputy unless there is an up-to-date information-sharing/data exchange agreement in place with that organisation or third party. **Under no circumstances** should any personal data about any individual be passed outside the Council without the authority of the Senior Information Risk Owner or his deputy.

12.2 Agencies which request data on a regular basis such as the police or banks will have easy access to appropriate paperwork and guidance for use in these circumstances.

12.3 It should be noted that whilst staff understandably will wish to assist external agencies wherever possible especially if the request relates to criminal activity (for example the police or banks), the Council is under no obligation to release personal data unless the request is made by a court order.

12.4 Personal data should generally only be made public if there is a legal or statutory requirement to do so. On occasions it may be appropriate to publish personal data with the individual's consent. However, in such cases staff must ensure that the consent is fully informed and freely given. Staff must also be aware that it is possible to withdraw consent at any time and, if that happens, publication of the data must cease immediately.

12.5 Staff should be aware that publishing personal data on the Council's web pages or internet effectively means that the data is published world-wide and outside the European Economic Area. It, therefore, cannot be protected by the DPA or the European Directive on Personal Privacy. Great care should be taken before publishing any personal data (or any data from which individuals could be identified) in this manner and the approval of both the Council's Business Development and Innovation Manager and the Council's Senior Information Risk Owner or his deputy should be obtained before publication.

13. What to do in the Event of a Data Breach

13.1 The ICO defines a data breach as a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provisions of a public electronic communications service'.

13.2 A data breach can happen for a number of reasons:

- loss or theft of data or equipment on which data is stored;
- inappropriate access controls allowing unauthorised use;
- equipment failure;
- human error;
- hacking attack; and

- 'blagging' offences where information is obtained by deceiving the organisation who holds it.

13.3 If a member of staff becomes aware of a data breach their first action should be to inform their line manager, who will then ensure that the breach is reported to the Senior Information Risk Owner or his deputy.

13.4 The Senior Information Risk Owner or his deputy will then decide on the most appropriate steps to take depending on the nature and quantity of data released. An investigation will be carried out into all data breaches.

13.5 It is a requirement of the DPA that the ICO is notified of all serious data breaches. .

13.6 All data breaches should be recorded in a data breach log as described in the Council's Information Security Policy.

14. Training and Awareness

14.1 In order to fully comply with the DPA it is important that all staff who have access to any personal data have an awareness of the DPA.

14.2 Training is a crucial element of staff awareness. Council staff must be aware of their obligations relating to personal data as part their duties.

14.3 Training may be achieved in a number of ways:

- all staff and Members to be made aware of the Council's Data Protection Policy;
- e- learning tools; and
- data protection procedures developed, publicised, and made available for staff to refer to on the intranet.

14.4 For some posts additional training and guidance is required. Those posts will identified through their work and any additional training and guidance will need to be discussed with the line manager in the first instance.

15. Keeping Information Secure

15.1 The *Seventh Principle* of the DPA requires organisations to take appropriate technical and organisational measures to keep data secure. The security of data held by the Council is a relatively complex area and more information on the technical details of information security can be found in the Council's Information Security Policy.

15.2 However, security of data goes beyond the use of computer equipment. Data will inevitably be stored or processed in hard copy forms at some time and access to this must be restricted to only those authorised to view it. As a general guide hard paper copies should not be left in the open in offices but should be kept locked away when not in use, in the same way as computer terminals should not be left unlocked and unattended.

15.3 It is important to remember that individuals should only be able to access data which they need to do their job. Personal data should not be left unattended and freely available to anyone in the office.

16. Administration

16.1 The Senior Information Risk Owner has overall responsibility for the maintenance and operation of this policy, and will be pleased to answer any questions about it.

16.2 Responsibility for monitoring adherence to this policy belongs to the Information Governance Working Group.

16.3 This policy will be reviewed at least every two years to confirm it reflects best practice and to ensure it complies with any legislative changes or amendments. Any significant and necessary changes will be reported to the Performance and Audit Committee

See also: -

Council Guidance

Information Security Policy

Websites:

Information Commissioner: www.ico.gov.uk

Glossary of Terms

Data means information which –

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or

(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Personal data means data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of

Sensitive personal data means personal data consisting of information as to:

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have

Data subject means an individual who is the subject of personal data

Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller

Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Recipient, in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

Third party, in relation to personal data, means any person other than –

(a) the data subject,

(b) the data controller, or

(c) any data processor or other person authorised to process data for the data controller or processor

Disclosure is any release of information by the data controller to any recipient.