Head of Legal Services
Data Protection Officer & Monitoring Officer Helen Miles

Data Protection Policy 2016

Corporate Information Unit
Legal Services
ciu@iow.gov.uk

Contents

1 Purpose of Data Protection Policy

1.1 It is the Isle of Wight Council's (“the council”) obligation to ensure compliance with the Data Protection Act 1998 (“the act”). The Information Commissioner, who oversees compliance and promotes good practice, requires all organisations, and individuals, who process personal data, to comply with the eight data protection principles of 'good information handling'.

These are:

1. Personal data shall be processed fairly & lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes
3. Personal data shall be adequate, relevant and not excessive
4. Personal data shall be accurate and, where necessary kept up to date.
5. Personal data shall not be kept for longer than is necessary
6. Personal data shall be processed in accordance with the rights of data subjects, including the rights to access information (Subject Access Request)
7. Personal data will be kept in an appropriately controlled and secure environment
8. Transfers outside of the European Economic Area require adequate levels of protection

1.2 The Act also requires all organisations, and individuals, who process personal information, to register with the Information Commissioner’s Office. This process is called Notification. The council, and its elected members, are required to review their notification on an annual basis.

1.3 Data Protection law and policy aims to ensure that individual's rights and freedoms are protected. Using personal data to abuse, discriminate or deny access to services is unlawful. The council is committed to ensuring that personal data that it holds is used fairly, lawfully and in a non-discriminatory manner.

1.4 This policy applies to all personal data held by the council. It encompasses manual/paper records and personal data electronically processed including information gathered on CCTV systems, of whatever type and at whatever location, used by, or on behalf of, the council.

1.5 This policy will be reviewed on an annual basis to ensure that it reflects changes to existing legislation, and any new legislation.

2 Overview of the Data Protection Act 1998

2.1 The Data Protection Act 1998 gives individuals the right to see information about them held by companies and organisations. In certain circumstances they may have the information corrected or erased, or they may even be able to prevent the processing of their personal data. If a Data Controller causes an individual damage or distress as a result of non-compliance, they could claim compensation. The

council is classed as a Data Controller and could be prosecuted for any serious offences that may be committed as well as an individual employee.

2.2 The Data Protection Act 1998 is not optional. It is mandatory and there can be substantial monetary penalties imposed for non-compliance with the act, either by the Information Commissioner's Officer or the court.

3 Obligations on staff and elected members

3.1 The obligations outlined in this policy apply to all those who have access to personal data held by the council, whether employees, agency staff, elected members (or other public representatives), trustees, employees of associated organisations or volunteers. It includes those who work at home, from home, or have remote, or flexible patterns of working.

3.2 All individuals who have access to personal information have a personal responsibility to ensure that all processing complies with the data protection act principles. Personal data should not be sent to any other organisation, without first checking the relevant Data Exchange Agreement/Information Sharing Protocol, and obtaining appropriate authorisation. These agreements/protocols govern what information will be shared, with which organisations, under what circumstances. They should include practical arrangements for how we and our partners will manage information in accordance with the act and this and related policies.

3.3 Any individual who knowingly, or recklessly, processes data for purposes other than those for which it is intended, or is deliberately acting outside of their recognised responsibilities, may be subject to the council's disciplinary procedures, including dismissal where appropriate, and possible legal action liable to prosecution. All individuals permitted to access personal data in line with their work duties must comply with this policy and agree to undertake any relevant training that may be appropriate to the job/position being undertaken.

3.4 As well as the council, individuals can also be prosecuted for unlawful action under the act. Upon summary conviction (in a Magistrate's Court), fines of up to £5000 could result if employees process information about other people without their consent or proper authorisation from the council. Upon conviction or indictment (Crown Court), the fine can be unlimited. Employees could be committing an offence by sharing information with others who do not need to be told that information in order to carry out their legitimate council duties.

3.5 The Information Commissioner's Office (ICO) has recently issued fines of up to £325,000 to organisations who have breached the act.

3.6 Any complaint that alleges that the council, or a member of staff, has failed to comply with the Data Protection Act, should be sent to the Corporate Information Unit ("CIU") who will investigate on behalf of our Data Protection Officer and Caldicott Guardian. In addition, any incidents relating to the loss of; inappropriate access to; unlawful sharing of, personal data, must also be reported to the CIU.

3.7 The Isle of Wight Council's Data Protection Officer is the Monitoring Officer, County Hall, Newport, Isle of Wight, PO30 1UD.

4 Confidentiality and Security

4.1 The council recognises the importance of the personal information it processes. Personal information will be maintained with an appropriate level of security to ensure compliance with the act.

4.2 Extra protection will be afforded to sensitive personal information.

4.3 Personal data should be managed carefully and processed in accordance with the Data Protection Principles as defined in the Data Protection Act 1998. The council also recognises that article 8 of the Human Rights Act 1998 affords protection to individual's personal information. This means that the council will only seek to process personal information that may infringe this right, where it is lawful, proportionate and necessary to do so.

4.4 Some personal data may also attract a duty of confidence initially, particularly when given in a health or social work environment. It is important also to recognise that sensitive personal information (see below) may require additional security measures to ensure both its integrity and security.

4.5 Employees, agency staff, elected members (or other public representatives), trustees, employees of associated organisations or volunteers have a duty to ensure that personal information is not knowingly or recklessly misused, lost, or destroyed.

- Manual files (paper records) - access must be restricted solely to relevant staff and stored in secure locations (eg lockable cabinets), to prevent unauthorised access.

- Computer systems will be configured and computer files created with adequate security levels to preserve confidentiality, and ensure only those that need access have access. Those who use the council's computer equipment will have access only to the data that is both necessary for the work they are doing and held for the purpose of carrying out that work. Access will only be provided once relevant training has been undertaken and appropriate authorisation given.

- Those with access to personal information must comply with all council policies relating to the management of information including: use of electronic equipment and email, information security, protective markings. All policies are available on the council's intranet and internet sites, as appropriate.

- Personal data will be disclosed only to the data subject (the individual the information relates to); authorised agents in accordance with our Access to Information Policy; and other organisations and persons who are pre-defined as notified recipients within the council's Notification Register Entry held with the Information Commissioners Office (www.ico.org.uk). At certain times it may be

required that personal data be disclosed under one of the exemptions within the Data Protection Act 1998. These exemptions allow for personal data to be shared for the purposes of the prevention or detection of crime; or the assessment or collection of tax, for example, without gaining consent from the data subject.

- If there is a requirement for this, appropriate authorisation will be obtained, and an audit trail will be kept to provide accurate records of any disclosures of personal data.

- The council will ensure that appropriate technical and organisational measures are taken when transferring personal information, in accordance with our security policy. The level of security will be proportionate to the damage that may arise in the event of a security breach or loss of data. Sensitive personal data should only be transferred by way of secure electronic transfer. Manual transfer of sensitive personal information should be undertaken via a secure means as detailed in our Protective Marking Policy.

- Preventing abuse and discrimination. The council processes **sensitive personal data** (as defined in the act) on employees, councillors and service users. The council will have regard to its various diversity policies to ensure that if instances of abuse or discrimination occur, appropriate action is taken

- Where it is necessary to transmit personal information by facsimile, this will only occur where the sender is satisfied that the information will not be viewed by any unauthorised person at the receiving machine. The adoption of safe harbour machines with our partner organisation will be encouraged to assist routine transmission. However, consideration should be given to alternative methods of transfer.

- **Sensitive Personal data** consists of information relating to the following:

    - the racial or ethnic origin of the data subject,
    - their political opinions,
    - their religious beliefs or other beliefs of a similar nature,
    - Trade union membership,
    - their physical or mental health or condition,
    - their sexual life,
    - the commission, or alleged commission, of any offence,
    - any proceedings for any offence committed or alleged to have been committed.

5 Ownership of Data

5.1 Each council service is responsible for the personal data that it holds. This responsibility also extends to personal data that is processed by a third party on behalf of the council. The service will hold a record of all processing activities containing personal data, whether paper based or electronic. Where required, the

service will provide the necessary information to the Data Protection Officer in order to facilitate the notification of the data with the Information Commissioner.

5.2 Elected members are responsible for the personal information they hold.

6 Obtaining, Recording, Using and Disclosing

6.1 Processing

6.1.1 Each of these activities comes within the definition of **processing.** Processing in relation to personal data, means carrying out any of the processing activities "on the data".

6.1.2 Any activity/operation performed on personal data - whether held electronically or manually, such as obtaining, recording, holding, disseminating or making available the data, or carrying out any operation on the data.

6.1.3 This includes, organising, adapting, amending and processing the data, retrieval, consultation, disclosure, erasure or destruction of the data. *(It is difficult to envisage any activity, which does not amount to processing)*

6.1.4 All processing of personal data will comply with the data protection principles as defined in the Data Protection Act 1998. In the situation where a third party processes data, the third party will be required to act in a manner which ensures compliance with the Data Protection Act 1998 and have adequate safeguards in place to protect the personal data.

6.2 Obtaining

6.2.1 It is a requirement that any data collection forms used in order to collect personal data will contain a "**Fair processing Notice**". The statement will need to be clearly visible and placed appropriately so the data subject (individual to whom the information relates) is fully aware of the intended uses of their personal data. It should also include as a matter of good practice, the padlock symbol to assist drawing to the attention that personal information is being collected.

6.2.2 The information that would need to be supplied on a fair processing notice is as follows:

- The identity of the data controller or appointed representative
- The purpose or purposes for which the information is intended to be processed
- Any further information in order to make the processing fair.

6.2.3 It is also very important to remember, that when collecting data via the telephone or face to face, the above information should also be made clear to the data subject, before any processing of their personal data takes place.

6.2.4 The council will carefully consider the purposes for which it will use the personal information collected, both at the instant of collection and in the future. Before any further use of the information is considered the council will check the original fair processing notice given. If it is an unrelated purpose, that is not exempted by the Act, such as for the purposes of crime prevention, then the council may not be authorised to use the information.

6.3 Recording and using the data

6.3.1 Data will only be processed for the purpose for which it was collected and should not be used for additional purposes unless permitted by the Act.

6.3.2 The council will endeavour to inform all individuals of why their personal data is being collected. In line with the first data protection principle all information will be collected fairly and lawfully and processed in line with the purpose for which it has been given. The council may need to hold and process information in order to carry out statutory obligations. In these instances, all personal data will be processed fairly and lawfully.

6.4 Disclosing

6.4.1 Personal data must not be disclosed, except to **authorised** users, other organisations and people who are pre-defined as a **notified recipient,** or if required under one of the **exemptions** within the Data Protection Act 1998.

6.4.2 The Corporate Information Unit (CIU), Legal Services, co-ordinates requests for personal information from other agencies such as the police, other local authorities and partner agencies. This is to ensure that there is a justified reason to share, and to apply consistency and for audit purposes. CIU will then contact the relevant department/s to discuss the request.

6.4.3 The council has a number of data exchange agreements (DEAs) in place to assist with consistent disclosure of information between partner agencies, where sharing takes place on a regular basis.

7 Data Subjects Rights

7.1 The Right of Subject Access

7.1.1 A written request from an individual wishing to access their personal information is known as a Subject Access Request. Sections 7 to 9 of the act give an individual the rights to request access to any 'personal data' that they believe may be held about them.

7.1.2 A fee of £10 is applicable and suitable identification is required to confirm the identity of the data subject. This includes photographic identification, together with a bank statement or bill to confirm the address. Where the information is to be posted, recorded delivery will be used once the address had been verified. Where information is to be collected, photo ID must be provided at

the time of collection. This ensures that personal information is handed to and/or delivered to the correct recipient.

7.1.3 With respect to education records, the fee is on a sliding scale, dependant on the quantity of information involved.

7.1.4 The information requested will be provided promptly and the act requires replies to be sent within 40 calendar days of receipt of the fee for the subject access request. If the information cannot be disclosed within the time period specified, the data subject will be kept fully informed of the process and given access to any personal data that may already have been gathered.

7.1.5 Information requests will be dealt with in accordance with the council's Access to Information Policy which can be found at (www.iwight.com/foi)

7.1.6 The Corporate Information Unit has Information Access officers, who co-ordinate and respond to such requests for a number of departments within the council including Social Services, Housing, HR, Special Educational Needs. All other departments within the council will deal with their own services requests.

7.1.7 If you have any queries regarding requests for information please contact CIU (email: information@iow.gov.uk) , by post to: Corporate Information Unit, IW Council, County Hall, High Street, Newport, IW PO30 1UD..

7.1.8 If you wish to access any personal information that is held by the council, a form is also available on the internet at: https://www.iwight.com

7.1.9 If a data subject believes that the council has not acted in accordance with the Data Protection Act 1998 they may complain to the Data Protection Officer, Legal Services, Isle of Wight Council, County Hall, Newport, Isle of Wight, PO30 1UD. If the data subject remains dissatisfied they are able to complain to the Information Commissioner. Alternatively they may complain directly to the Information Commissioner at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

7.2 Prevention of processing causing damage or distress (section 10)

7.2.1 If an individual believes that a data controller is processing personal data in a way that causes them substantial unwarranted damage, or substantial unwarranted distress, they can send a notice (data subject notice) to the data controller requesting, within a reasonable time, the data controller to stop the processing.

7.3 Right to prevent processing for purposes of direct marketing (section 11)

7.3.1 An individual is entitled to request (in writing) a data controller to cease, or not to begin, processing their personal data for the purpose of direct marketing. When a data controller receives a written notice they must comply as soon as practically possible.

7.3.2 An individual may apply to a Court for an order if the data controller fails to comply with a written notice.

7.4 Rights in relation to automated decision taking (section 12)

7.4.1 An individual is entitled, by written notice, to require a data controller to ensure that no decision, which significantly affects that individual, is based solely on the processing, by automatic means, of personal data of which that individual is the data subject.

7.5 Right to compensation (section 13)

7.5.1 An individual who suffers damage, or damage and distress, as the result of any contravention of the requirements of the act by a data controller, is entitled to compensation where the data controller is unable to prove that they had taken such care as was reasonable in all circumstances to comply with the relevant requirement.

7.6 Dealing with inaccuracy (section 14)

7.6.1 A data subject may apply to the Court for an order requiring the data controller to rectify, block, erase or destroy such data relating to the data subject that is inaccurate, together with any other personal data relating to the data subject, which contain an expression of opinion which the Court finds is based on the inaccurate data.

8 Training

8.1 It is the council's policy that all employees and elected members who hold or process personal data receive the appropriate training in order to comply with the Data Protection Act 1998.

8.2 Data Protection training is a crucial element of staff awareness. All individuals need to be aware of their obligations relating to any personal data they process as part of their council duties. Failure to adhere to the eight data protection principles can lead to a breach of the act and, potentially, disciplinary action.

8.3 Advice and assistance can be obtained from the Corporate Information Unit within Legal Services.

9 Complaints

9.1 Any complaint received that alleges that the council has failed to comply with the act, will be investigated internally by the council, at the request of the complainant. As there is no automatic right to an internal review, the complainant is entitled to forward their complaint direct to the Information Commissioner's Office ("ICO"). Such complaints fall outside of the councils general Complaints Policy.

9.2 The council will not hesitate to report serious, deliberate, or reckless, breaches of the act by any employee, agency staff, elected members (or other public representatives), trustees, employees of associated organisations or volunteers, past or present; or any other data processor, in relation to personal information that the council holds.

9.3 Any person that wishes to make a complaint about a breach of the act should do so by writing to the Data Protection Officer (DPO), Isle of Wight Council, County Hall, Newport, Isle of Wight PO30 1UD. An independent person will be appointed by the DPO to undertake the investigation.

10 Definitions

Data - Any information automatically processed or going to be automatically processed. This includes information contained within structured and unstructured manual files.

Personal Data - Information relating to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or likely to come into possession of, the data controller.

Sensitive Personal Data – Personal information relating to an individual's race/ethnic origin, their political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, criminal or alleged offences or any proceedings.

Data Controller – The Isle of Wight Council is a Data Controller, being a body who decides the manner in which, and purposes for which, personal data are, or are to be, processed.

Individual elected members are also Data Controller's with respect to the personal information they manage in respect of their duties to their constituents.

Data Subject - An individual who is the subject of the personal data.

Data Processor - A person other than an employee of the council, who processes personal information on behalf of the council under instruction.

Processing - Any activity/operation performed on personal data - whether held electronically or manually, such as obtaining, recording, holding, disseminating or making available the data, or carrying out any operation on the data. This includes, organising, adapting, amending and processing the data, retrieval, consultation, disclosure, blocking, erasure or destruction of the data.

Information Commissioners Office- an independent regulatory body responsible for ensuring compliance with the Data Protection Act

Any queries regarding the above policy please contact the Corporate Information Unit by email to information@iow.gov.uk or in writing to Legal Services, County Hall, High Street, Newport, IW PO30 1UD.