

## **HIGHLANDS & ISLANDS FIRE & RESCUE SERVICE**

### **DATA PROTECTION ACT 1998**

#### **POLICY STATEMENT**

Highlands & Islands Fire & Rescue Service fully endorse and adhere to the Principles of the Data Protection Act 1998.

Highlands & Islands Fire & Rescue Service regards the lawful and correct treatment of personal information as very important to successful operations, and to maintain confidence between service users, employers and those we serve. Highlands & Islands Fire & Rescue Service will treat personal information lawfully and correctly.

Each employee will be given such information, instructions and training as is necessary. This will ensure they are aware of their contractual responsibilities in relation to personal data and inform them that they can, in some cases, be held personally responsible if any personal data is improperly disclosed, destroyed or obtained.

A programme of awareness training will be provided to existing and new employees.

The role of the Data Protection Officer has been allocated to the Head of Finance and Administration whose tasks are to co-ordinate the Authority's response to the Act and to ensure that the provisions of the Act are met.

Reviewing the Service's Data Protection Act Strategy and Management System will be carried out by the Service Management Team and Heads of Departments on a regular basis.

Signed

Firemaster  
Highlands & Islands Fire & Rescue Service

Principles Data Protection Act.

## PRINCIPLES OF THE DATA PROTECTION ACT 1998

### 1. Principle 1 – Fair Processing

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:-

- a) at least one of the conditions in schedule 2 is met, and
- b) in the case of sensitive personal data, at least one of the conditions in schedule 3 is also met.

#### 1.1 Schedule 2 Conditions

Schedules 2 and 3 set out specific conditions that have to be met before processing of personal data can take place, these relate to the first of the 8 principles. The conditions are different for sensitive data and non-sensitive data.

Broadly, **non-sensitive data** is not to be processed unless at least one of the following conditions has been met:-

- The data subject has given their consent to the processing,
- The processing is necessary for the performance of a contract to which the data subject is party (the employment contract), or for taking steps to enter into such a contract,
- The data controller has to process the information in order to comply with non-contractual legal obligations (such as health & safety obligations);
- The processing is necessary to protect the vital interests of the data subject;
- The processing is necessary for the administration of justice/exercise of crown functions/ the exercise of any other functions of a public nature exercised in the public interest; or
- The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party/parties to whom the data is disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

#### 1.2 Schedule 3 Conditions

In the case of **sensitive data**, processing is permitted only if at least one of the following conditions is met:-

- The data is of sensitive personal nature consisting of information as to racial or ethnic origin,
- The individual has given their explicit consent to the processing;

- The processing is necessary for the purposes of exercising or performing any right conferred or obligation imposed by law on the data controller in connection with employment;
- The processing is necessary to protect the vital interests of the individual in a case where either the consent cannot be given (incapacity, for example) or else the data controller cannot reasonably be expected to obtain consent (for example, the individual cannot be contacted despite various attempts over a considerable length of time);
- The processing is carried out in the course of its legitimate activities by anybody or association not established for profit and which exists for political, philosophical or trade union purposes, and which relates only to individuals who are members of that body;
- The individual has already made the information public, by taking deliberate steps;
- The processing is necessary for the purpose of/in connection with legal proceedings, obtaining legal advice or establishing/exercising or defending legal rights;
- The processing is necessary for the administration of justice/exercise of crown functions;
- The processing is necessary for medical purposes and is undertaken by a health professional.
- The personal data are processed in circumstances specified in an order made by the Secretary of State.

The Data Protection Act 1998 defines sensitive personal data as relating to:

- Racial origin
- Political opinions
- Religious or other beliefs
- Physical or mental health
- Sexual life
- Criminal convictions/proceedings
- Trade Union membership

If an organisation holds any data that matches any of the above criteria, then they will have to legitimise why they are holding this data. The Data Protection Act 1998 states that you cannot hold any of this data unless you meet at least one criteria from Schedules 2 & 3 of the Act.

If you do not meet at least one criterion, you will be in breach of the Act. An organisation will also be in breach of the Act if it cannot legitimise the reason for holding the data even if it does match one of the criteria.

**2. Principle 2 – Compatible Purposes**

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. Principle 3 – Extent of Data**

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

**4. Principle 4 – Data Accuracy**

Personal data shall be accurate and, where necessary, kept up to date.

**5. Principle 5 – Retention Period**

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

**6. Principle 6 – Data Subject Rights**

Personal data shall be processed in accordance with the rights of data subjects under this Act. They include:

- the right to be informed that processing is being undertaken;
- the right to inspect personal data;
- the right to prevent processing in certain circumstances; and
- the right to rectify, block or erase data.

**7. Principle 7 – Security and Management of Data**

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss of destruction of, or damage to, personal data.

**8. Principle 8 – Foreign Data Transfer**

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.