County Durham and Darlington
Fire and Rescue Service

Administration & General AD/1/35

Data Protection Policy

Document Overview

The following areas are covered by this document:

- The Service's approach to handling personal information in accordance with the Data Protection Act 1998.
- An overview of the main obligations for staff and Elected Members in dealing with personal information to comply with the Act and the data protection principles.

Document Control

Version	Date	Author	Reasons for Change
001	02/05/2013	K Pallister	New Policy

Sign-Off List

Position
Head of Corporate Resources
Deputy Chief Executive

Approved By(to be completed by author)

		Date
Section		02/05/2013
SMT		16/05/2013
SLT		24/05/2013
CFA		16/07/2013
Comment		

Equalities Impact Assessment

Screening	Full
X	

FOI exemption required?	**Yes**		**Reason**
	No	X	

Security Level	Restricted	
	Unrestricted	X

Review Date	August 2016

1. INTRODUCTION

1.1 The Data Protection Act 1998 (DPA) is the law that protects personal privacy and upholds individuals' rights. It applies to anyone who handles, or has access to information about individuals. It also gives rights to the people the information is about.

1.2 The DPA is one of several pieces of legislation which deals with individual rights and information policy. A list of related legislation that may also need to be considered when handling personal information can be found in **Appendix A**.

1.3 It applies at all levels in County Durham and Darlington Fire and Rescue Service/Authority and this policy provides an overview of the main obligations for staff and Elected Members in dealing with personal information.

2. POLICY STATEMENT

2.1 County Durham and Darlington Fire and Rescue Service (CDDFRS) regards the lawful and correct treatment of personal information as critical to successful operations and in maintaining the confidence of service users, employees and those we serve.

2.2 CDDFRS is committed through its policy, procedures and guidelines to comply with the requirements of the Data Protection Act 1998 to ensure the protection and security of the personal information that it processes and in particular, will:

- Comply with both the law and good practice;
- Respect individuals' rights;
- Be open and honest with individuals whose data is held;
- Provide training and support for staff who handle personal data.

2.3 When handling personal information and sensitive personal information the Service will act in accordance with the eight enforceable principles of the Data Protection Act.

3. POLICY SCOPE

3.1 This policy and the procedure arising from it applies to all employees and to associated individuals who work for the Service including agency staff, contractors and others employed under a contract of service. The policy also applies to Elected Members in their role as a Member of the Combined Fire Authority.

3.2 The policy covers all personal information that the Service (and Authority) holds (in either electronic or paper format or file system) from the time it is created or arrives within the Service (or Authority) to the time it is destroyed.

4. THE PRINCIPLES OF DATA PROTECTION

4.1 The DPA requires that all staff and others who process or use any personal information must ensure that they adhere to the eight data protection principles. If the Service or an individual follows these principles, they will be acting in accordance with the Act.

4.2 The principles are based on three key concepts:

- **Purpose** – personal data must only be held for a clear purpose or purposes.
- **Fairness** – personal data must only be processed for legitimate purposes.
- **Transparency** – data subjects must be given certain basic information about the personal data held about them.

4.3 The eight principles, which form the basis of the Act, state that personal data must be:

a) **Principle 1 – Fairly and lawfully processed.**
Nobody should be deceived or misled about the purpose for which their data is to be processed. It must not be processed unless at least one of the conditions in Schedule 2 of the Act is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met. See **Appendix B** for the conditions.

b) **Principle 2 – Obtained only for one or more specified and lawful purposes, and not further processed in any manner incompatible with that purpose.**
Personal data must only be processed for limited purposes with the permission from the data subject for each purpose.

c) **Principle 3 – Adequate, relevant and not excessive.**
The data must be sufficient to meet their purpose but not provide more information than the purpose requires, or provide information outside the scope of the purpose

d) **Principle 4 – Accurate and where necessary up to date.**
The data must be accurate when recorded, and accuracy must be maintained throughout the life cycle of the data.

e) **Principle 5 – Not kept for longer than necessary.**
Personal data must not be kept for any longer than is necessary for the purpose for which it was obtained.

f) **Principle 6 – Processed in line with the rights of the data subject.**
Individuals, also known as data subjects, have the right to access their personal data and can request that any processing that causes or is likely to cause them distress be ended. They can insist that their data is not used for marketing and other purposes, and can request that inaccurate data is amended.

g) **Principle 7 – Stored and processed securely.**
Appropriate technical and organisational measures must be taken to prevent unauthorised or unlawful processing of personal data and to protect against loss, damage or destruction.

h) **Principle 8 – Not transferred to a country outside of the European Economic Area (EEA) without adequate protection.**
Personal data must not be transferred outside of the EEA unless that country has in place a level of data protection comparable to that in the EEA.

5. DEFINITIONS

5.1 **Personal Data** - data which relates to a living individual who can be identified: a) from that data, or; b) from that 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 the individual.

5.2 **Sensitive Personal Data -** personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious beliefs or other beliefs of a similar nature;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Proceedings for any offence committed or alleged to have been committed and convictions.

5.3 **Data Subject** - any living individual who is the subject of personal data.

5.4 **Data Controller** - person who (either alone or jointly or in common with other persons and could be an organisation) determines the purposes for which, and the manner in which, any personal data are, or are to be processed. An employee of a data controller processes data under the remit of the data controller (who is their employer).

5.5 **Data Processor -** any person (or organisation) other than the employee of the data controller, who processes the data on behalf of the data controller.

5.6 **Processing** - obtaining, recording or holding information or data, or carrying out any operation or set of operations on that information or data (i.e. organising, adapting, altering, retrieving, consulting or disclosing).

6. TRAINING AND AWARENESS

6.1 All staff and Fire Authority Elected Members will be made aware of this policy and the procedure arising from it. The training and awareness process which must be followed is detailed in the Data Protection Procedure.

7. ENFORCEMENT

7.1 **Information Commissioners Office** – The Information Commissioner's Office (ICO) is the UK's independent public authority set up to uphold information rights. They do this by promoting good practice, ruling on complaints, providing information to individuals and organisations and taking appropriate action when the law is broken. The ICO enforces and oversees the following legislation:

- Data Protection Act 1998;
- Freedom of Information Act 2000;
- Privacy and Electronic Communications Regulations 2003;
- Environmental Information Regulations 2004;
- INSPIRE Regulations 2009.

7.2 **Notification -** The ICO maintains a public register of data controllers and details of the types of data held. County Durham and Darlington Fire and Rescue Authority is registered as such. The DPA requires every organisation (data controller) that processes personal data to notify the ICO, and to renew their notification on an annual basis (unless they are exempt). Failure to notify is a criminal offence. Any changes to a register entry must be notified to the ICO within 28 days of that change. An example of the Service's register entry can be found in **Appendix C.**

7.3 **Breaches and Penalties -** The ICO has powers to take action to serve enforcement notices, conduct audits and serve monetary penalty notices for a failure to comply with the data protection principles as it sees appropriate in each circumstance.

7.4 **Criminal proceedings** – The Act removes the corporate protection of individual employees or agents from prosecution should they breach the conditions imposed by the Act. The unauthorised accessing or processing of personal data is a criminal offence under section 55 of the DPA. Therefore an individual who for example accesses some files without authorisation and discloses it to someone else will have breached the Act and would be liable for a criminal prosecution.

8. ROLES AND RESPONSIBILITIES

8.1 **County Durham and Darlington Fire and Rescue Authority -** Overall responsibility for the efficient administration of data protection legislation lies with the Authority. County Durham and Darlington Fire and Rescue Authority is named as the data controller in the ICO register.

8.2 **Elected Members –** Elected Members must make themselves aware of the Data Protection Policy and Procedure and apply it accordingly when dealing with personal data they handle during the course of their work with the Combined Fire Authority.

8.3 **Principal Officers -** The Principal Officers (Chief Executive Officer and Deputies) will promote and support arrangements to deliver effective data protection compliance. They will monitor the on-going effectiveness of the management processes.

8.4 **Senior Information Risk Officer** - The senior officer responsible for data protection is the Deputy Chief Executive who is the Service's Senior Information Risk Owner (SIRO) and as such provides assurance to the Authority that personal data is being managed and secured effectively. The SIRO will report any serious breaches of personal information security to the Information Commissioners Office.

8.5 **Heads of Service/Area Managers** – Heads of Service have responsibility for seeing that their area of service complies with the principles of the DPA. They will ensure that their staff (including contractors, consultants, volunteers and agency staff employed) are aware of their responsibilities under the Act and trained to discharge those responsibilities.

8.6 **Information Asset Owners -** are responsible for ensuring that the measures in place to protect the personal information that forms part of the assets they are responsible for.

8.7 **The Governance Team -** will advise sections and departments on developing procedures and applying the Data Protection Policy. They will ensure that staff have access to support in terms of training and development in adhering to the Data Protection Policy and Procedure. They will be responsible for:

- Reviewing and updating the Policy and Procedure when relevant;
- Notification with the ICO;
- Handling subject access requests;
- Investigating possible breaches under DPA;
- Carrying out quality assurance of Service documentation periodically.

8.8 **Managers -** All managers will actively promote the Data Protection Policy and Procedure and take steps to implement improvements to work processes within their own area of functional responsibility. They are responsible for ensuring that staff under their direction are aware of the policy and procedure and understand their obligations and responsibilities.

8.9 **Staff -** All staff must read and understand the policies and procedures relating to the personal data they handle during the course of their work. See section 10 for examples of related policies and procedures. They must take steps to ensure that personal data is kept secure at all times and processed in accordance with the 8 principles of the Act. Non-compliance of this policy and procedure may be investigated under the Services Discipline Policy (AD/1/7).

8.10 **Contractors/Partners/Consultants** who are users of personal information supplied by the Service will be required to confirm that they will abide by the requirements of the DPA in respect of that information. This will be in the form of a written agreement.

9. MONITORING AND REVIEW

9.1 The Governance Team will report any issues around personal data security processes and any new/impending changes in the approach taken by the Information Commissioner's Office to the Service Management Team and the Service Leadership Team.

9.2 This document will be reviewed either within three years; after a change in relevant legislation or recognised best practice and for the purposes of continuous improvement.

9.3 A Management Indicator will report on instances of data protection breaches which are progressed to the Information Commissioner.

10. RELATED DOCUMENTS

10.1 This policy should be read in conjunction with the Data Protection Procedure. Other related documents include:

- Internet And Email Acceptable Usage Policy (AD/2/12);
- Information Security Policy (AD/1/11);
- ICT Mobile Computing Policy (AD/1/18);
- ICT Physical Security Policy (AD/1/19);
- ICT Security Incident Procedure;
- Protective Marking and Security Policy (AD/1/20);
- Regulation of Investigatory Powers Act 2000 Policy (AD/1/25);
- Closed Circuit Television Policy (AD/1/28);
- Closed Circuit Television Procedure (AD/2/77);
- Code of Conduct (AD/2/42);
- Protection Marking and Security Procedure (AD/2/71);
- Appraisal and Review Procedure (AD/2/72).

August 2013 **Deputy Chief Fire Officer**

APPENDIX A

Related Legislation

- Common Law Duty of Confidence
- The Human Rights Act 1998
- Computer Misuse Act 1990
- The Freedom of Information Act 2000 (FOI Act)
- The Regulation of Investigatory Powers Act 2000 (RIPA)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/2905)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)
- The Environmental Information Regulations 2004 (SI 2004/3391)
- The United Kingdom Data Protection (Processing of Sensitive Personal Data) Order 2006 (SI 2006/2068)
- The Criminal Justice and Immigration Act 2008
- The Data Protection (Notification and Notification Fees) (Amendment)
- Regulations 2009 (SI 2009/1677)
- The Data Protection (Processing of Sensitive Personal Data) Order 2009 (SI 2009/1811)
- The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 (SI 2010/31)
- The Data Protection (Monetary Penalties) Order 2010 (SI 2010/910).

APPENDIX B

Conditions for Processing (Schedule 2 and 3 of the DPA)

Conditions necessary for processing personal information (Schedule 2 and Schedule 3 of the Data Protection Act)

Processing is not allowed unless one or more of the following conditions is satisfied (Schedule 2 of the Act):

1. with the consent of the data subject
2. to establish or perform a contract with the data subject
3. to comply with a legal obligation
4. to protect the vital interests of the data subject
5. for the exercise of certain functions of a public interest nature
6. for the legitimate interests of the data controller unless outweighed by the interests of the data subject.

There are additional conditions for processing sensitive data (Schedule 3 of the Act).

Sensitive personal data may be processed if one of the conditions in the first list is met **and** one of the following:

1. with the explicit consent of the data subject
2. to perform any right or obligation under employment law
3. to protect the vital interests of the data subject or another person
4. for the legitimate activities of certain not-for-profit bodies
5. when the data have been made public by the data subject
6. in connection with legal proceedings
7. for the exercise of certain functions of a public interest nature
8. for medical purposes
9. for equal opportunities monitoring

APPENDIX C

Data Protection Register - Entry Details

Registration Number: Z4757495

Date Registered: 05 May 2000 **Registration Expires:** 04 May 2013

Data Controller: COUNTY DURHAM FIRE AUTHORITY

Address:

FRAMWELLGATE MOOR

DURHAM

DH1 5JR

This data controller states that it is a public authority under the Freedom of Information Act 2000 or a Scottish public authority under the Freedom of Information (Scotland) Act 2002

This register entry describes, in very general terms, the personal data being processed by:

COUNTY DURHAM FIRE AUTHORITY

This register entry contains personal data held for 7 purpose(s)

Purpose 1

Method 2

Data Controllers further description of Purpose:

FIRE AND EMERGENCY PREVENTION AND CONTROL:

THE PREVENTION AND DETECTION OF FIRE, PROTECTION OF LIFE AND PROPERTY AND PROVISION OF FIRE FIGHTING AND EMERGENCY SERVICES.

TO INCLUDE -

INSPECTION OF PREMISES

MANAGING RESPONSE TO FIRES, TRAFFIC ACCIDENTS, OTHER INCIDENTS AND EMERGENCIES

LICENSING, REGISTRATION AND CERTIFICATE ISSUE (IN COMPLIANCE WITH THE REQUIREMENTS OF THE FIRE PRECAUTIONS ACT 1971 AND THE EXPLOSIVES AND PETROLEUM ACTS)

PROMOTION OF THE FIRE SERVICE THROUGH EDUCATION AND TRAINING FOR THIRD PARTIES (INCLUDING COURSES, DEMONSTRATIONS, ISSUE OF CERTIFICATES AND PRODUCTION OF GUIDANCE)

VEHICLE MANAGEMENT AND MAINTENANCE

EQUIPMENT MANAGEMENT AND MAINTENANCE

Data subjects are:

Staff including volunteers, agents, temporary and casual workers

Suppliers

Complainants, correspondents and enquirers

Relatives, guardians and associates of the data subject

Advisers, consultants and other professional experts

Offenders and suspected offenders

Witnesses

Landlords

RECIPIENTS OF FIRE AND RESCUE SERVICES

APPLICANTS FOR CERTIFICATES, LICENCES AND REGISTRATION

OWNERS OF PROPERTY

Data classes are:

Personal Details

Education and Training Details

LIFESTYLE AND SOCIAL CIRCUMSTANCES

INCIDENT, ACCIDENT DETAILS

LICENCES, CERTIFICATES HELD

SERVICES PROVIDED TO THE DATA SUBJECT

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

PUBLIC UTILITIES

INSURANCE COMPANIES

LAWYERS

EDUCATIONAL ESTABLISHMENTS

D ELECTED MEMBERS

D TOURIST BOARDS

Data subjects themselves

Relatives, guardians or other persons associated with the data subject

Business associates and other professional advisers

Employees and agents of the data controller

Suppliers, providers of goods or services

Persons making an enquiry or complaint

Police forces

Local Government

Central Government

The media

Auditors

Courts / Tribunals

Landlords

Transfers:

None outside the European Economic Area

Purpose 2

Method 2

Data Controllers further description of Purpose:

FIRE SERVICE ADMINISTRATION:
ADMINISTRATION AND MANAGEMENT OF FIRE SERVICE PROPERTY/ASSETS
PLANNING AND ADMINISTRATION OF PROPERTY REPAIR AND MAINTENANCE,
ACCESS, SECURITY AND SAFETY ARRANGEMENTS
OFFICE ADMINISTRATION (INCLUDING OFFICE DIRECTORIES, E-MAIL, WORD PROCESSING,
DEALING WITH ENQUIRIES AND COMPLAINTS)

Data subjects are:

Staff including volunteers, agents, temporary and casual workers
Suppliers
Complainants, correspondents and enquirers
Relatives, guardians and associates of the data subject
Advisers, consultants and other professional experts

Data classes are:

Personal Details
Employment Details
Financial Details
Goods or Services Provided

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

Data subjects themselves
Relatives, guardians or other persons associated with the data subject
Employees and agents of the data controller
Suppliers, providers of goods or services
Financial organisations and advisers

Transfers:

None outside the European Economic Area

Purpose 3

Research

Purpose Description:

Research in any field, including market, health, lifestyle, scientific or technical research.

Data Controllers further description of Purpose:

CONTRIBUTION OF DATA TO FIRESTAT (HOME OFFICE STATISTICAL ANALYSIS DATABASE), AND THE COMPILATION AND MAINTENANCE OF A LOCAL FIRE SERVICE DATABASE.
TO INCLUDE:
IDENTIFICATION OF SUBJECTS FOR SURVEY OR ANALYSIS
COLLECTION OR EXTRACTION OF DATA
ANALYSIS, INTERPRETATION AND EVALUATION OF DATA
OUTPUT/PRESENTATION OF RESULTS OR FINDINGS

Data subjects are:

Staff including volunteers, agents, temporary and casual workers
Complainants, correspondents and enquirers
Relatives, guardians and associates of the data subject
Advisers, consultants and other professional experts
Offenders and suspected offenders
Witnesses
Landlords
RECIPIENTS OF FIRE RESCUE SERVICES

Data classes are:

Personal Details
Racial or Ethnic Origin
Religious or Other Beliefs Of A Similar Nature
Physical or Mental Health or Condition
LIFESTYLE AND SOCIAL CIRCUMSTANCES
INCIDENT AND ACCIDENT DETAILS

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

PUBLIC UTILITIES

INSURANCE COMPANIES

LAWYERS

D ELECTED MEMBERS

Data subjects themselves

Relatives, guardians or other persons associated with the data subject

Healthcare, social and welfare advisers or practitioners

Employees and agents of the data controller

Suppliers, providers of goods or services

Persons making an enquiry or complaint

Police forces

Local Government

Central Government

The media

Auditors

Courts / Tribunals

Landlords

Transfers:

None outside the European Economic Area

Purpose 4

Staff, agent and contractor administration

Data Controllers further description of Purpose:

THE ADMINISTRATION OF PROSPECTIVE, CURRENT AND PAST EMPLOYEES INCLUDING CONTRACT PERSONNEL, TEMPORARY STAFF OR VOLUNTARY WORKERS

PLANNING AND MANAGEMENT OF STAFF WORKLOAD AND/OR BUSINESS ACTIVITIES

ADMINISTRATION OF AGENTS OR OTHER INTERMEDIARIES

DISCIPLINARY MATTERS, INDUSTRIAL TRIBUNALS ETC

STAFF TRAINING

HEALTH AND SAFETY

OCCUPATIONAL HEALTH SERVICES

PENSIONS ADMINISTRATION

Data subjects are:

Staff including volunteers, agents, temporary and casual workers

Customers and clients

Suppliers

Complainants, correspondents and enquirers

Relatives, guardians and associates of the data subject

Advisers, consultants and other professional experts

Previous and prospective employers of the staff and referees

AGENTS AND CONTRACTORS

Data classes are:

Personal Details

Education and Training Details

Employment Details

Financial Details

Racial or Ethnic Origin

Trade Union Membership

Physical or Mental Health or Condition

Offences (Including Alleged Offences)

LIFESTYLE AND SOCIAL CIRCUMSTANCES

CUSTOMER, CLIENT AND SUPPLIER DETAILS

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

EDUCATION, TRAINING ESTABLISHMENTS, EXAMINING BODIES

Data subjects themselves

Relatives, guardians or other persons associated with the data subject

Current, past or prospective employers of the data subject

Healthcare, social and welfare advisers or practitioners

Business associates and other professional advisers

Employees and agents of the data controller

Suppliers, providers of goods or services

Financial organisations and advisers

Credit reference agencies

Police forces

Local Government

Central Government

Voluntary and charitable organisations

Auditors

Courts / Tribunals

Careers service

Trade unions and staff associations

Customers and clients of the data controller for goods and services

Transfers:

None outside the European Economic Area

Purpose 5

Accounts & Records

Purpose Description:

Keeping accounts related to any business or other activity carried on by the data controller, or deciding whether to accept any person as a customer or supplier, or keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by him or to him in respect of those transactions, or for the purpose of making financial or management forecasts to assist him in the conduct of any such business or activity

Data subjects are:

Staff including volunteers, agents, temporary and casual workers
Customers and clients
Suppliers
Advisers, consultants and other professional experts

Data classes are:

Personal Details
Employment Details
Financial Details
Racial or Ethnic Origin
Offences (Including Alleged Offences)
CUSTOMER, CLIENT AND SUPPLIER RECORDS

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

Data subjects themselves
Current, past or prospective employers of the data subject
Education, training establishments and examining bodies
Business associates and other professional advisers
Employees and agents of the data controller
Suppliers, providers of goods or services
Persons making an enquiry or complaint

Financial organisations and advisers

Credit reference agencies

Debt collection and tracing agencies

Trade, employer associations and professional bodies

Local Government

The media

Auditors

Courts / Tribunals

Transfers:

None outside the European Economic Area

Purpose 6

Method 2

Data Controllers further description of Purpose:

THE ADMINISTRATION OF SUPPLIER RECORDS RELATING TO GOODS, ORDERS, SERVICES AND

ACCOUNTS PROVIDED BY THE FIRE SERVICE.

Data subjects are:

Staff including volunteers, agents, temporary and casual workers

Customers and clients

Suppliers

Advisers, consultants and other professional experts

Data classes are:

Personal Details

Employment Details

Financial Details

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

D LOCAL AUTHORITIES

D ELECTED MEMBERS

D PUBLIC UTILITIES

Data subjects themselves

Current, past or prospective employers of the data subject

Business associates and other professional advisers

Employees and agents of the data controller

Suppliers, providers of goods or services

Persons making an enquiry or complaint

Financial organisations and advisers

Credit reference agencies

Debt collection and tracing agencies

Trade, employer associations and professional bodies

Central Government

Auditors

Courts / Tribunals

Customers and clients of the data controller for goods and services

Claimants, beneficiaries, assignees, payees

Transfers:

None outside the European Economic Area

Purpose 7

Crime Prevention and Prosecution of Offenders

Purpose Description:

Crime prevention and detection and the apprehension and prosecution of offenders.

Data Controllers further description of Purpose:

INCLUDES THE USE OF CLOSED-CIRCUIT TELEVISION FOR THE MONITORING AND COLLECTION OF SOUND AND/OR VISUAL IMAGES FOR THE PURPOSE OF MAINTAINING THE SECURITY OF PREMISES, FOR PREVENTING CRIME AND FOR INVESTIGATING CRIME.

Data subjects are:

Customers and clients
Offenders and suspected offenders
MEMBERS OF THE PUBLIC
THOSE INSIDE, ENTERING OR IN THE IMMEDIATE OF THE AREA UNDER SURVEILLANCE
VISITORS & EMPLOYEES TO ANY COUNTY DURHAM & DARLINGTON FIRE AND RESCUE AUTHORITY
PREMISES AT WHICH CCTV CAMERAS ARE IN OPERATION.

Data classes are:

Personal Details
Goods or Services Provided
Offences (Including Alleged Offences)
Criminal Proceedings, Outcomes And Sentences.
SOUND AND/OR VISUAL IMAGES

Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):

SECURITY ORGANISATIONS

Data subjects themselves

Business associates and other professional advisers

Employees and agents of the data controller

Suppliers, providers of goods or services

Persons making an enquiry or complaint

Police forces

Courts / Tribunals

Transfers:

None outside the European Economic Area
