County Durham and Darlington
Fire and Rescue Service

Administration & General AD/2/83

Data Protection Procedure

Document Overview

The following areas are covered by this document:

- Procedural guidance to address the main issues when dealing with personal information under the Data Protection Act 1998.

Document Control

Version	Date	Author	Reasons for Change
001	20/05/2013	K Pallister	New Procedure

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	Unrestricted

Review Date	August 2016

1. INTRODUCTION

1.1 This procedure will assist staff to apply the Data Protection Policy. It covers the key areas when dealing with personal information on a day to day basis under the Data Protection Act (DPA).

2. PROCESSING PERSONAL DATA

2.1 **Collecting and using personal data.**
The main requirement for processing (using) personal data is that the process meets the conditions for the processing (use) of personal data or sensitive personal data. These conditions are set out in appendix B in the Data Protection Policy.

As a general rule consent should be sought from the individual (data subject) to process their data. They should also be informed as to the purpose for which the information is required and how that information will be used including who it may be shared with. This information is usually contained in a Privacy Notice (also referred to as a Fair Processing Notice), which should be present on most data collection forms. Please see **Appendix A** for examples of privacy notices.

To assist staff in their understanding of processing personal data and practices to avoid; a guidance list has been produced at **Appendix B.**

2.2 **Holding personal data (records management).**
The DPA puts a responsibility on organisations to maintain a focus on keeping personal information accurate, up to date and for no longer than is necessary.

(a) **Updating**: When collecting personal data reasonable steps should be taken to ensure the accuracy of that information and regular review processes should be in place to check, update or discard personal data.

(b) **Storage:** Precautions should be taken to prevent any unauthorised access to personal data. Any information relating to named individuals should be handled and stored securely:

(i) Personal data should not be removed from Service premises or stored elsewhere unless such use is recognised and authorised. Off-site security must conform to Service standards and be in line with the seventh data protection principle.

(c) **Retention:** Principle 5 of the Data Protection Act states that records must be kept only for as long as necessary. The retention period adopted needs to take account of this. Data must be maintained for as long as is required for historical, legal, fiscal and auditing purposes. The duration depends on the data and its application. Developing and maintaining a good data 'housekeeping' procedure is important.

(d) **Archiving:** Some records may be archived for historical or research purposes. The provision of the 'research, history and statistics' exemption in section 33 of the Act allows personal data to be stored indefinitely as archives for research purposes provided that 'relevant conditions' are met:

(i) Data is not processed to support measures or decisions relating to particular individuals.

(ii) Data is not processed in such a way that substantial damage or substantial distress, is or is likely to be, caused to any data subject. s.31 (1).

(e) **Disposal:** If personal information is to be disposed, it must be destroyed securely and confidentially. The Service has a contract with a secure shredding organisation. Managers should make sure they have procedures in place to have suitable access to the facility.

Electronic records, files, media and devices should also be disposed of appropriately. Methods of disposal for these mediums are defined in the relevant ICT policy and procedure.

2.3 Keeping Personal Data Secure.

(a) The Service has a legal responsibility under the DPA to keep all information it holds, including personal data, secure and safe from any unauthorised use, damage, loss and theft. How information is to be stored and communicated should be considered before any collection of data takes place.

(b) Keeping personal data secure may involve encrypted and password protected devices and files or keeping paper files locked away. When Elected Members, employees and others acting on behalf of the Service access or use personal data, they must only have access or use personal data that is necessary to carry out their duties and responsibilities.

(c) Off-site use of personal data presents a potentially greater risk of loss, theft or damage to personal data and the Service and personal liability that may accrue from the off-site use of personal data is similarly increased. For these reasons, staff (and where applicable, Elected Members):

(i) Should take personal data off-site only when absolutely necessary, and for the shortest possible time, especially where sensitive data is to be processed. All personal data whether it is paper or encrypted electronic files must be kept physically secure at all times (e.g. for paper records, whilst at home keep in a locked draw or cupboard. Paper records and electronic devices must not be left in vehicles for long periods or overnight);

(ii) Should take particular care when laptop computers or personal devices are used to process personal data at home or in other locations.

2.4 Rights of Individuals

(a) Data subjects have certain specific rights under the DPA, all of which are listed in **Appendix C.** One of the main rights is for an individual to be able to see their personal data held by an organisation.

(b) Some exceptions to this right apply in certain circumstances. If someone asks for a copy of a confidential reference which has been written about them relating to training, employment or providing a service, it does not have to be provided it because of an exemption in the Act. However, whoever wrote the reference may choose to provide the information. It would seem reasonable to provide a copy if a reference is wholly or largely factual in nature, or if the individual is aware of an appraisal of their work or ability.

(c) When someone requests his or her own information, it is referred to as a Subject Access Request (SAR). A formal SAR should be made in writing (an email or fax is as valid as one sent in hard copy). All formal SARs should be forwarded to the Governance Team immediately who will administer and manage the process. The information must be provided as soon as is possible and in any event within 40 calendar days. The Service is entitled to require the individual to pay a fee of up to £10.00 for any subject access request.

(d) An individual may request their personal information in the course of business as usual (a routine enquiry) in which case this would not be treat as a formal SAR. An example of this would be someone making an enquiry about their salary payment. However, in this case, before releasing any information, the identity of the individual must be ascertained.

2.5 **Surveillance at Work.**

(a) The legal right of the Service as an employer to monitor workers' activities such as e-mails, telephone calls and use of the Internet is governed by the Regulation of Investigatory Powers Act 2000 (please refer to Service Policy AD/1/25 Regulation of Investigatory Powers Act 2000), the Lawful Business Practice Regulations 2000 and the Data Protection Act 1998.

(b) More detailed information about the monitoring of internet and e-mail activity can be found in the Internet and Email Acceptable Usage Policy (AD/2/12).

2.6 **Data Sharing**

(a) **Third Party Requests for Personal Data.**
A third party in this context, means organisations or individuals other than the Data Subject. The DPA Act does not give third parties a right of access to personal data although it does not absolutely prohibit such access.

(b) Staff should always exercise caution when dealing with requests from third parties for the disclosure of personal data. Disclosure requests should normally be required to be in writing, and should be responded to in writing. Where reasonable, the party making the request should be required to provide a statement explaining the purpose for which the data is requested, the length of time for which the data will be held, and an undertaking that the data will be held and processed according to the data protection principles.

(c) Where the request relates to the prevention/detection of crime, the apprehension/prosecution of offenders, assessment/collection of any tax or duty, or the discharge of regulatory functions, appropriate paperwork should be produced by the enquirer to support their request (e.g. official documentation stating that the information is required in support of an on-going investigation).

(d) If the request is for none of the purposes above, consent should be sought from the data subject where reasonably possible before releasing the information unless there is an exemption which applies within schedule 2 and 3 of the DPA (see appendix in Data Protection Policy).

2.7 **Data Processors**

(a) When entering into any arrangement/contract with another party who will process personal data on behalf of the Service (Data Processor) there must be a written contract which states that:

(i) The processor only acts on instructions from the data controller;

(ii) It has security in place that is equivalent to that imposed on the data controller by the seventh data protection principle.

(b) Examples of data processors include payroll organisations, accountants, software companies and market research companies. Therefore a data processor involved in data sharing doesn't have any direct data protection responsibilities of its own; they are all imposed on it through its contract with the data controller (the Service).

2.8 **Data Sharing with Partner Organisations**

(a) Information sharing is key to the Service's ability to deliver a better, more efficient service which is coordinated around the needs of the individual. It is essential to enable early intervention and preventative work and in some cases for safeguarding and promoting welfare and for wider public protection. Therefore information sharing is sometimes a vital element in improving outcomes for all. At the same time, the Service is aware that individuals want to be confident that their personal information is kept safe and secure.

(b) The following checklist provides the general guidance rules about data sharing under the DPA:

(i) **Remember that the Data Protection Act is not a barrier to sharing information.** It provides a framework to ensure that personal information about living persons is shared appropriately.

(ii) **Be open and honest.** Let the person from the outset know about why, what, how and with whom information will, or could be shared, and seek agreement, unless it is unsafe or inappropriate to do so.

(iii) **Seek advice.** If you are in any doubt seek advice about the data sharing. Contact the Governance Team if you have any questions, without disclosing the identity of the person where possible.

(iv) **Share with consent where appropriate.** Where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest.

(v) **Consider safety and well-being.** Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

(vi) **Necessary, proportionate, relevant, accurate, timely and secure.** Remember that the data protection principles still apply. You must ensure that the data you are sharing is necessary for the purpose you are sharing it, is shared only with those who need it, is accurate and up-to-date and is shared and stored securely.

(vii) **Keep a record of your decision to share information.** Remember to record the reasons for sharing what you have shared, with whom and for what purpose.

(c) Although the principles above cover the sharing of information with anyone or any organisation, staff should ensure that if they are sharing information on a regular basis with an organisation, that they have an agreed information sharing protocol in place.

(d) When sharing or disclosing personal information to a third party, staff must ensure that they have proper authorisation to do so as part of their normal working practice.

2.9 **Information about the Deceased**

(a) The DPA relates to the handling of the personal information of living individuals only; it does not cover that of individuals once they are deceased. However, we still owe a duty of confidence to the deceased and their families. Each request for information about the deceased must be carefully considered in light of the circumstances of each individual case.

3. BREACH/LOSS OF PERSONAL DATA

3.1 On occasion, personal data may be lost, stolen, or compromised. When this happens, it is important to establish what data has been lost, mitigate the loss and where relevant, contact the people whose data was lost.

3.2 A data breach is any incident involving the loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as serious. The data breach includes both electronic media and paper records it can also mean inappropriate access to information.

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

(a) Loss or theft of data or equipment on which data is stored
(b) Inappropriate access controls allowing unauthorised use
(c) Equipment failure
(d) Human error
(e) Hacking attack
(f) Blagging offences where information is obtained by deceiving the organisation who holds it

3.4 If a breach occurs, staff must notify their line manager immediately who should then contact the Governance Team who will investigate and assess the level of the breach and take steps as necessary. Managers should complete the reporting form at Appendix D. All breaches will be reported to the Senior Information Risk Officer who will inform the Fire Authority and/or the Information Commissioners Officer if deemed appropriate.

4. TRAINING AND AWARENESS

4.1 All staff and Fire Authority Elected Members will be made aware of this procedure and policy from which it arises. For some posts within the Service, additional training and guidance will be required. Those posts will be identified through their work and any additional training requirements will need to be discussed with line managers. Managers will inform the Governance Team of these identified posts requiring additional training.

4.2 **Induction** – When staff and Elected Members join the Service and Fire Authority, it is important that they are introduced to their basic responsibilities under the DPA. For staff, in addition to being made aware of the contents of the Data Protection Policy and Procedure, completion of the data protection training programme will form part of the induction process.

4.3 **Continuous training and awareness –** To ensure staff are kept up to date with any changes in requirements and reminded of their obligations in respect of data protection they will be required to complete the data protection training programme every two years. If additional training is required beyond this, this will be identified through line management communication. Line managers should then liaise with the Governance Team with regard to identifying appropriate training programmes and/or materials before formally raising a request with the Training section.

August 2013 **Deputy Chief Fire Officer**

APPENDIX A

Examples of fair processing notices:

County Durham and Darlington Fire and Rescue Service is responsible for providing fire and emergency services under the Fire and Rescue Services Act 2004. To assist us to do this we are collecting your details to enable us to provide you with a home fire safety service.

For the purposes of the Data Protection Act 1998, County Durham and Darlington Fire and Rescue Authority is the Data Controller (the holder, user and processor) of the information. We will keep all information safe and secure.

If you would like to know more about what information we hold about you, or the way we use your information you can contact ….

County Durham and Darlington Fire and Rescue Service is committed to complying with the Data Protection Act 1998, ensuring the accuracy and security of your personal information.

We will:
Only use the information we hold about you for the purpose you provided it;
Only collect the minimum information necessary to fulfil that purpose; and
Tell you what we will do with your information and who it will be shared with. Although sometimes the law requires that we share your information with other agencies to help reduce crime or investigate fraud.

We work closely with councils, other emergency services and community organisations and often need to share information with them, to deliver our services. We will not supply these organisations with your information unless we are satisfied that equal or stronger measures are in place to protect the information from unauthorised access. We will not supply your information to any organisation for marketing purposes.

Data Protection Act 1998

The data collected on this form will only be used for the purpose of …….. within County Durham and Darlington Fire and Rescue Service and will not be disclosed to any external sources without your consent. Both electronic and paper records will be deleted/shredded when ……..

APPENDIX B

General Guidance for processing personal data

Do:

- Think of personal data held about individuals as though it were held about you;
- Get permission from the data subject to hold their personal data unless consent is obviously implied;
- Be particularly careful about sensitive data: concerning race, political opinion, religious belief, trade union membership, physical or mental health, sexual life, criminal offences;
- Hold personal data about people only when necessary;
- Ensure personal data is kept accurate and up to date;
- Tell people you hold personal data about them and tell them why you need to do so (fair processing);
- Be very careful about passing personal data to third parties;
- Respect confidentiality and the rights of the data subject (the person whose information you hold);
- Make sure security measures are strictly controlled and well maintained to ensure that only authorised people can access, alter, disclose or destroy personal data held within databases;
- Review personal data kept in files from time to time and at least annually;
- When writing documents, bear in mind that the data subject (any person who is mentioned in the document) has a right to see information relating to them;
- Realise emails may be retrieved and revealed to those about whom they are written;
- Take care when sending documents to shared printers. Be mindful that other people may see the information;
- Be vigilant when working with personal information outside of Service premises. Ensure laptops and other mobile devices are encrypted and paper records are kept physically secure at all times;
- Direct any official requests to see personal data to the Governance Team at Service Headquarters.

Avoid:

- Worrying about the complexities of the Act - the Data Protection Act principles are simple;
- Revealing personal data to third parties without the data subject's permission or justification;
- Disclosing any personal data over the telephone unless the person has been identified appropriately;
- Holding sensitive data about a person without their explicit consent or seeking advice from the Governance Team;
- Leaving personal data insecure in any way, whether it is physical files or information held electronically; (keep a clean desk);
- Taking personal data home that is unencrypted;
- Use personal data held for one purpose for a different purpose without permission from the data subject.

APPENDIX C

Individual Rights under the DPA

There are seven rights under the Data Protection Act:

1. The right to subject access
This allows people to find out what information is held about them on computer and within some manual records.

2. The right to prevent processing
Anyone can ask a data controller not to process information relating to him or her that causes substantial unwarranted damage or distress to them or anyone else.

3. The right to prevent processing for direct marketing
Anyone can ask a data controller not to process information relating to him or her for direct marketing purposes.

4. Rights in relation to automated decision-taking
Individuals have a right to object to decisions made only by automatic means e.g. there is no human involvement.

5. The right to compensation
An individual can claim compensation from a data controller for damage and distress caused by any breach of the act. Compensation for distress alone can only be claimed in limited circumstances.

6. The right to rectification, blocking, erasure and destruction
Individuals can apply to the court to order a data controller to rectify, block or destroy personal details if they are inaccurate or contain expressions of opinion based on inaccurate information.

7. The right to ask the Commissioner to assess whether the Act has been contravened
If someone believes their personal information has not been processed in accordance with the DPA, they can ask the Commissioner to make an assessment. If the Act is found to have been breached and the matter cannot be settled informally, then an enforcement notice may be served on the data controller in question.

Personal Information Security Incident Form

County Durham and Darlington Fire and Rescue Service

(TO BE COMPLETED IN ACCORDANCE WITH THE DATA PROTECTION POLICY AND PROCEDURE AD/1/35 AND FORWARDED IMMEDIATELY TO THE GOVERNANCE TEAM, PERFORMANCE AND INFORMATION SERVICES)

SECTION ONE: EMPLOYEE INFORMATION

NAME:	
SECTION/STATION:	
JOB TITLE:	
MANAGER:	

SECTION TWO: PERSONAL DATA FORMAT

WAS THE DATA IN PAPER OR ELECTRONIC FORMAT? IF ELECTRONIC, WHAT MEDIUM IT WAS (I.E. USB DEVICE, E MAIL, CD, DATABASE FILE)	
WHAT SECURITY MEASURES WERE IN PLACE (I.E. ENCRYPTION, PASSWORD PROTECTION ETC.)	
DOES IT CONTAIN ANY SENSITIVE PERSONAL DATA?	

SECTION THREE: DETAILS OF DATA LOSS/BREACH

ESTIMATED DATE AND TIME OF BREACH/LOSS:	
DATE REPORTED TO MANAGER:	
BRIEFLY DESCRIBE THE INCIDENT: **(PLEASE PROVIDE DETAILS OF THE TYPE OF FILE INVOLVED I.E. EXCEL, JPEG, WORD ETC.)**	
APPROXIMATELY HOW MANY DATA SUBJECTS HAVE BEEN AFFECTED?	
HAVE YOU INFORMED THE DATA SUBJECTS THAT THIS INCIDENT OCCURRED?	
HAVE YOU TAKEN ANY ACTION TO MINIMISE/MITIGATE THE EFFECT ON THE DATA SUBJECTS INVOLVED? IF SO PLEASE PROVIDE BRIEF DETAILS.	