DORSET & WILTSHIRE FIRE AND RESCUE

DORSET & WILTSHIRE FIRE AND RESCUE SERVICE

IM 3 - Managing Personal Information Procedure

To be used in conjunction with the Information Management Policy

Information Management

Information is an important organisational asset and needs to be appropriately and efficiently managed and protected. As well as ensuring legal compliance, the Authority wishes to ensure high standards of governance to support open and transparent decision-making. We will continuously work to ensure that information is complete, accurate, relevant, accessible and timely. In line with our strategic vision, we wish to continue to be a trusted partner. We will responsibly share and receive information by following good practices and where appropriate secure recognition through achieving externally accredited standards.

Effective information management systems will be established, embedded and managed throughout the organisation. These systems will directly support our strategic intent and the need to ensure legal compliance against a range of statutory requirements. We will take advantage of cost effective technology to ensure that appropriate and secure solutions are in place to support the management of information held by the organisation.

The information system policy and its underpinning procedures will be the responsibility of a nominated senior information risk owner (SIRO) within the senior leadership team. The policy and procedures will be reviewed by senior management and annually reviewed and scrutinised by Members as part of the Statement of Assurance. This Statement and our assurance framework will be made publically available to further promote confidence in the Authority and its Service.

1.	Purpose & Definition	Detailed Info
2.	Procedure Principles	Detailed Info
2.2	Processing personal information	Detailed Info
2.3	Principle 1 – Processed fairly and lawfully	Detailed Info
2.4	Principle 2 – Processed for limited purposes	Detailed Info
2.5	Principle 3 – Adequate, relevant and not excessive	Detailed Info
2.6	Principle 4 – Accurate and up to date	Detailed Info
2.7	Principle 5 – Keep no longer than necessary	Detailed Info
2.8	Principle 6 – Individuals' rights	Detailed Info

2.9	Principle 7 – Kept secure	Detailed Info
2.10	Principle 8 – Not transferred to other countries without adequate protection	Detailed Info
3.	Responsibilities	Detailed Info
3.2	All Staff	Detailed Info
3.3	Line Managers	Detailed Info
3.4	Senior Information Risk Owner (SIRO)	Detailed Info
3.5	Information Asset Owners	Detailed Info
3.6	Information Governance Group	Detailed Info
3.7	Information Management Team	Detailed Info
4.	Monitoring and Assurance	Detailed Info
5.	Document Reference	Detailed Info
6.	Document Management & Version Control	Detailed Info

Ref No:	IM 3	**FRS:**	DWFRS
Date of Issue:	01/04/2016	**Review Due:**	01/04/2019
Version No:	V1.0	**Review Completed:**	DD/MM/YYYY

1. Purpose & Definition

1.1. We must process accurate and relevant information about individuals to provide an efficient and effective public service. This is often in partnership with other organisations.

1.2. All staff have a responsibility for the security of information and respect for confidentiality and must ensure that all personal data is processed in line with the Data Protection Act 1998 (DPA). This procedure:

- provides advices and guidance on the processing of personal information in accordance with the DPA
- outlines your responsibilities as a member of staff processing personal information on behalf of DWFRS
- outlines your rights relating to your own personal information processed by DWFRS.

1.3. Terms used:

- Data Controller – this is Dorset & Wiltshire Fire and Rescue Service (DWFRS).
- Data Subject – an individual who we hold information about.
- Data Processor – all people processing personal information on behalf of the Data Controller.
- Processing – obtaining, holding, amending, reading, sorting, disclosing, deleting, or destroying.
- Information Asset Owner (IAO) – A Senior Manager responsible for one or more identified information assets within the Service.
- Senior Information Risk Owner (SIRO) – A Brigade Manager with responsibility for the Service's information risk policy.
- Information Commissioner's Office (ICO) - UK's independent public authority set up to uphold information rights. The ICO enforces and oversees compliance with the Act. 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. This action can include criminal prosecution, non-criminal enforcement, audit and serving a monetary penalty notice.
- Information Governance Group - This group is chaired by the SIRO and is made up of Information Asset Owners, Information Management and IT. It is responsible for promoting information management across the Service, ensuring that information risks are identified and appropriately managed.

2. Procedure Principles

2.1. **The Data Protection Act**

2.1.1. The Data Protection Act (DPA) works in two ways. Firstly, it gives you the right to know what information is held about you and secondly it provides a framework to ensure that we handle personal information properly.

2.1.2. Personal information identifies a living individual, such as a name or it could just be reference to a female firefighter at a station where there is only one female firefighter. Personal information could be a photograph, CCTV imaging, paper or electronic records where an individual can be identified.

2.1.3. It is also information that with other information we hold or are likely to hold, could identify a living individual, such as a postcode. Personal information also includes the expression of opinion, such as interview notes on an employee's file.

2.1.4. The Act does not cover information relating to a business but some information may be commercially sensitive so this needs to be handled in confidence.

2.2. **Processing personal information**

2.2.1. The Act states that anyone who processes personal information must comply with eight principles. All staff have a responsibility to make sure that personal information is:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than necessary
6. Processed in line with your rights
7. Secure
8. Not transferred to other countries without adequate protection.

2.2.2. To make sure we comply with the eight principles, you need to carry out a Privacy Impact Assessment (PIA) for any new systems/procedures or changes to existing ones. Initially you need to answer a set of screening questions to determine whether a full PIA is needed. Please contact the Information Management Team for further guidance and assistance in completing the PIA.

2.3. **Principle 1 – Processed fairly and lawfully**

2.3.1. **Lawful** – this means that before we obtain and use personal information we must have the statutory powers to do so.

2.3.2. We must meet at least one of the following conditions before processing personal information:

- Do we have consent from the individual?
- Is processing necessary for the performance of a contract?
- Is it processed in the legitimate interests of DWFRS?
- Is there a legal obligation to obtain or use the information?
- Is processing necessary for the administration of justice?
- Is it necessary to carry out statutory functions of the Authority?
- Is it necessary to carry out public functions?
- Is it to protect their vital interests?

2.3.3. So, if you're processing personal information to carry out our functions as a Fire Service, it is lawful for you to do this.

2.3.4. **Sensitive personal data** – The Act classes the following data as sensitive:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs

- Trade union membership
- Physical or mental health conditions
- Sexual life
- Offences (including alleged).

2.3.5. To process sensitive data we need to meet at least one of these additional conditions:

- We have explicit consent from the individual.
- Processing is necessary to meet our obligations under employment law.
- It's for monitoring equal opportunities.
- It's to protect the vital interests of the data subject or another individual.
- The data subject has made the information public themselves.
- It's required in connection with legal proceedings.

2.3.6. **Fair** – whenever you obtain or receive personal information, you must make sure the individual knows or has access to the following information:

- Who they are giving the information to.
- Why it is needed and what we may use if for.
- If we will use it for other purposes.
- Who we may disclose it to.
- How to obtain information held about themselves.

2.3.7. The privacy notice on our website informs the public why and how we use their information. We also have to inform people about what we will be doing with their information at the point of collection, for example, on the Home Safety Check form. This applies if you are collecting information over the telephone, in person, on a form, via email or fax.

2.3.8. To the quality and security of information over the telephone you should:

- repeat what the individual has said to avoid recording inaccurate information
- try not to use abbreviations
- avoid adding personal comments
- shred any rough notes.

2.3.9. There are some occasions when exemptions apply which means we can process certain personal information without complying with some of the principles. See supporting information for more detail on DPA exemptions. Some examples of this are as follows:

- Personal information has to be made public by law, for example, the Electoral Register.
- Legal professional privilege applies.

- There is a legal requirement to obtain or use the personal information.
- the personal information is needed.
- For the prevention and detection of crime.
- For the apprehension or prosecution of offenders.
- For the assessment or collection of any tax or duty.
- To carry out regulatory duties such as Trading Standards, Environmental Health
- Negotiations being carried out by DWFRS.

2.3.10. **Notification** – we must notify the Information Commissioner's Office (ICO) about what we do with the personal information we hold. Our entry is available on the public register at http://www.ico.gov.uk/.

2.3.11. Please notify the Information Management Team of any new electronic or paper filing systems before any personal information is processed so we can keep our entry to the ICO as accurate as possible. You may also need to complete a Privacy Impact Assessment.

2.4. **Principle 2 – Processed for limited purposes**

2.4.1. You must only hold information for the purpose(s) that you need it, and for which the data subject has, explicitly or implicitly, agreed. If the information is to be used for a different purpose, you must notify and get authority from the data subjects concerned prior to the new processing taking place.

2.5. **Principle 3 - Adequate, relevant and not excessive**

2.5.1. Do not hold information "just in case" it could be useful one day. When collecting information, do not ask for more information than you need.

2.6. **Principle 4 – Accurate and up to date**

2.6.1. You must the information you process is accurate because this is used to:

- manage performance
- report on our performance
- deliver and improve our services.

2.6.2. See Adequacy and Accuracy for more information.

2.7. **Principle 5 – Keep no longer than necessary**

2.7.1. Do not keep information for longer than necessary. Our Retention Schedule details how long we should keep specific information and you must comply with these guidelines. See Retention and Disposal of Personal Information for more information.

2.7.2. Electronic systems for holding personal information should have built in prompts to review/destroy the information according to our Retention Schedule. If new

processes are introduced or changes to existing processes are being proposed, always notify the Information Management team to make sure the Retention Schedule is updated

2.8. **Principle 6 – Individuals' rights**

2.8.1. The second area covered by the Act provides individuals with important rights. You have a right to:

- see a copy of what information is held about you (there is no charge for staff but we charge members of the public £10)
- prevent processing likely to cause damage or distress
- prevent processing for direct marketing purposes
- fairness in relation to automated decision making
- apply to the court for ratification, blocking, erasure and destruction of personal information
- compensation
- request an assessment by the ICO.

2.8.2. **Subject access requests** – Individuals have a right to request a copy of the personal information we hold about them. We need to respond within 40 calendar days.

2.8.2.1. If you receive a subject access request, please forward it promptly to the Information Management Team.

2.8.2.2. Do not deter an individual from making an application to see their personal information or tell them that they cannot see the personal information we hold about them.

2.8.2.3. If you are asked to help with a subject access request you must:

- help to meet the 40 day deadline and tell the Information Management team if you will have difficulty with this. Information can be in files, forms, notes, emails and everything we hold has to be disclosed
- not destroy, delete, amend or otherwise tamper with material to make it 'acceptable' to the applicant - this is a criminal offence
- not withdraw material because it may be embarrassing. Information can only be withheld under one of the exemptions to the Act or to preserve third party confidentiality.

2.8.2.4. See Subject Access and Individual Rights for additional information.

2.8.3. **Your rights**

2.8.3.1. We process your personal information throughout your employment and for a period of time afterwards. For more information, see Personnel Employment information.

2.8.3.2. You are entitled to receive a copy of the personal information we hold about you, including your Personal Reference File (PRF). To request access to the personal information we hold about you, complete the Subject Access Request form and send it to the Information Management Team.

2.8.3.3. Should you feel you are being denied access to personal information you are entitled to, you can contact the ICO for help (http://www.ico.org.uk)

2.9. **Principle 7 – Kept secure**

2.9.1. You must make sure any personal information and the equipment that stores the information is kept secure. For example, only give access to staff who have a genuine business need to see the information and you should store personal information in locked cabinets. Please see Security of Personal Information and refer to the Information Security procedures for more information.

2.9.2. **Disclosing information**

2.9.2.1. We can only disclose personal information to outside organisations and other departments within the Service in limited circumstances.

2.9.2.2. Never disclose personal information unless you have the responsibility or authority to do so. If in doubt about whether to comply with a request for information, please discuss this with your line manager or seek advice from the Information Management Team.

2.9.2.3. In cases where we regularly share personal data with another organisation, a data sharing agreement is required. The Information Management Team maintains a register of these. You must advise the team of any new arrangements and ad hoc disclosures, including those that fall under the Freedom of Information Act.

2.9.2.4. When we release incident reports or provide interviews/statements for the Police, we will comply with the principles of the Data Protection Act (DPA).

2.9.2.5. See Disclosure of Personal Information for more information.

2.10. **Principle 8 – Not transferred to other countries without adequate protection**

2.11. Personal data should not be transferred outside the European Economic Area unless the country has an adequate level of protection. Take particular care if cloud services are being considered. This should form part of a Privacy Impact Assessment (PIA).

2.11.1. **Buying in services**

2.11.1.1. You must make sure all contractors that have access to personal information know how to take care of it and can guarantee compliance with the Data Protection principles. You must include the following on the contractual agreement:

- Who owns the information? If it's collected for us it remains our information, not the contractor's.

- A confidentiality agreement.
- Compliance with the DPA – clarify access and security controls and how breaches will be dealt with. Who deals with subject access requests?
- What happens if the work is sub contracted?
- An indemnity clause.

2.12. Where a contractor is processing personal data on our behalf (data processor), please seek advice from the Information Management Team to ensure an appropriate contract is in place.

2.12.1.1. If you are considering using a third party to manage data on our behalf (by connecting in to our network or hosting a web based system), we will need to conduct a security assessment before approval. Please contact the Information Management Team if you have any questions.

2.12.2. **Enforcement action and criminal offences**

2.12.2.1. If we contravene the DPA, the ICO has the power to take action. This could be an information or enforcement notice requiring us to improve, a monetary penalty for up to £500,000, or prosecution of the Service or **an individual member of staff.**

2.12.2.2. It is an offence for a person to knowingly or recklessly, without the consent of the Service, to:

- obtain or disclose personal information
- procure the disclosure to another person.

2.12.2.3. It is a further offence to sell or offer personal information for sale that has been unlawfully obtained or procured.

2.12.3. **Monitoring staff**

2.12.3.1. If it is considered necessary to monitor staff we must follow the DPA employment practices code to justify the benefits against the adverse effect, and to ensure we always:

- Have a clear purpose for monitoring – making sure this is justified against the benefit.
- Consider alternative approaches for maintaining the same information.
- Recognise that monitoring is usually intrusive and workers have a right to expect their personal lives to remain private.
- Recognise there is an expectation of some privacy in the workplace.
- Make sure staff are aware of any monitoring and why (except in exceptional circumstances where covert monitoring is justified – in this situation a risk assessment is conducted. This must be approved by a Brigade Manager.
- Make sure staff are clear on the rules and standards where monitoring is used to enforce these.

- Only use information obtained through monitoring for the purpose the monitoring was conducted, unless it leads to the discovery of an activity that we couldn't reasonably be expected to ignore.
- Keep information gathered through monitoring secure.

2.12.3.2. Areas where regular monitoring takes place include the use of ICT equipment, internet, and email, CCTV installed on our premises and vehicles and telephone recordings. The requirement for monitoring in these areas is covered in the relevant procedures.

2.12.4. **Complaints**

2.12.4.1. We will deal with any complaints about how we process personal data in accordance with our corporate complaints procedure.

2.12.4.2. Unlike the Freedom of Information Act, the DPA does not set out a specific complaints regime for data protection issues. However, individuals do have a right to request that the Information Commissioner make an assessment of particular circumstances with the Data Protection Act.

3. Responsibilities

3.1. **All staff**:

- make sure you process personal information in accordance with this procedure and the DPA. Failure to do so may result in disciplinary action which could lead to dismissal and, in some cases, criminal proceedings/prosecution
- complete the e learning training at least every two years
- report any breaches (actual or potential) via the Security Incident Reporting Procedure

3.1.1. If any member of staff identifies a practice or procedure that they believe may be a weakness in the security of information they need to bring it to the attention of their line management and the Information Management Team.

3.2. **Line managers:**

- make sure all members of your staff (including temporary and agency staff) sign the confidentiality agreement
- make sure your team follows the procedures and are appropriately trained
- where new processes and systems involving personal data are being introduced, work with the Information Management Team to carry out a Privacy Impact Assessment.

3.3. **Senior Information Risk Owner (SIRO) make sure:**

- appropriate information governance arrangements are in place
- organisational information risk is properly identified and managed and that appropriate assurance mechanisms are in place.

3.4. **Information Asset Owners:**

- promote good practice and Lead and foster a culture that values and protects information
- make sure information contained within your systems (paper and electronic) is accessed and shared appropriately
- manage information risk within your area of responsibility.

3.5. **Information Governance Group**

3.5.1. This group is chaired by the SIRO and is made up of Information Asset Owners, Information Management and IT. It is responsible for promoting information management across the Service, ensuring that information risks are identified and appropriately managed.

3.6. **Information Management Team:**

- annually renew our notification with the ICO and update as required
- record and monitor all subject access requests. Direct them to the relevant team and make sure a response is received within 40 calendar days
- maintain the delivery of data protection training for staff. Make sure all staff complete the e learning training every two years and provide additional training for specific staff as required
- maintain the Retention Schedule
- update the Privacy notice on the website
- assist in the completion of Privacy Impact Assessments (PIAs) as required and keep a central register
- ensure appropriate data sharing agreements are in place
- record all new, and any changes to, systems where personal data is processed
- make sure risk assessment forms are completed for any irregular covert monitoring of staff and assess each request before any such activity can take place
- maintain knowledge and skills to the provision of accurate advice and guidance for processing personal data.

4. Monitoring & Assurance

4.1. **Procedure Management**

4.1.1. Data protection compliance will form part of our annual assurance to the Fire Authority.

4.1.2. The Information Governance Group will monitor information risk and compliance on a regular basis.

4.1.3. Internal auditors will audit our information management processes in line with the Information Governance Framework audit plan. There will be a key performance indicator (KPI) on Data Protection at the quarterly Finance and Audit Committee.

4.2. **Learning and Development**

4.2.1. All members of staff must complete the e learning Protecting Information course on Learning Pool during their induction and a refresher every two years. Office based staff and watch managers and above need to complete the Essentials version, all other operational station staff need to complete the Briefing version. Log in details are available from the Training department.

4.2.2. Line Managers are to notify the Information Management team of any additional training requirements within their teams.

5. Document Reference

5.1. **Forms to complete**

Privacy Impact Assessment (PIA)

Subject Access Request form

Confidentiality Agreement staff/agency

DPA Risk Assessment – Irregular staff monitoring

5.2. **Document References**

Access to Information – FOI Act – IM 1

RIPA – IM 2

Acceptable use of internet – IM 5

Acceptable use of email – IM 6

Security incident reporting

CCTV (Premises)

Security Management

Information Security

Data Sharing

5.3. **Supporting Information**

Subject Access

DPA Exemptions

Disclosure of Personal Information

Adequacy and accuracy

Retention and Disposal of Personal Information

Security of Personal Information

Individuals' Rights

6. Document Management

Policy Reference: Information Management			
Owner	**Review Date**	**Author**	**Status**
Lisa Smith	01/04/2019	Lisa Smith	Pending for Publish

6.1. **Version Control:**

Version	Page & Par Ref	Date	Changes Made	Authorised By
V1.0	Entire document	27/01/2016	Published	V Shearing

Top of doc