DORSET & WILTSHIRE FIRE AND RESCUE

DORSET & WILTSHIRE FIRE AND RESCUE SERVICE

IM 3 - Managing Personal Information Procedure

To be used in conjunction with the Corporate Governance Policy Statement

Information Governance (IM)

Ref No:	IM 3	**FRS:**	DWFRS
Date of Issue:	06/04/2020	**Review Due:**	01/12/2022
Version No:	V9.0	**Review Completed:**	27/11/2019

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 to ensure that all personal data is processed in line with data protection legislation. This procedure:

- provides advices and guidance on the processing of personal information in accordance with data protection legislation
- 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 protection legislation – the current data protection legislation (either General Data Protection Regulation or Data Protection Act)
- 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 Governance and IT. It is responsible for promoting Information Governance across the Service, making sure information risks are identified and appropriately managed.

2. Procedure Principles

2.1. Data Protection legislation (Data Protection Act/ General Data Protection Regulation)

2.1.1. Data protection 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 a member of staff's file.

2.1.4. Data protection legislation 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. Anyone who processes personal information must comply with the following 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. Kept securely.

2.2.2. DWFRS also has a responsibility to demonstrate compliance with the above principles.

2.2.3. Before processing personal data, you may need to carry out a Data Protection Impact Assessment (DPIA). It is important that this is done before you do any of the following that involve personal data:

- Procurement – such as, procuring a new system or subcontract to an external data processor
- Data sharing
- Change or implement new processes/procedures.

2.2.4. Initially you need to answer a set of screening questions to determine whether a full DPIA is needed. Please send completed DPIAs to the Information Governance Team and contact them for further guidance and assistance, as necessary.

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 a lawful reason for doing so.

2.3.2. We must meet 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 there a legal obligation to obtain or use the information?
- Is it to protect their vital interests?
- Is processing necessary for performance of a task carried out in the public interest or in our official authority as a Fire & Rescue Service?
- Is it necessary for the purposes of our legitimate interests?

2.3.3. Please see the ICO website for more information on lawful conditions and how they apply https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.

2.3.4. **Special category information** – The following information is known as special category or sensitive information:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health conditions
- Sexual life
- Biometrics.

2.3.5. To process special category 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 to protect the vital interests of the data subject or another individual
- It is carried out by a foundation, association or not for profit body with a political, philosophical, religious or trade union aim

- The data subject has made the information public themselves
- It's for the establishment or defence of legal claims
- It's necessary for reasons of substantial public interest
- It's necessary for the purposes of preventative or occupational medicine
- It's necessary for public interest in the area of public health.

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 long we will keep it for
- Their rights, including 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 ensure 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. We need to keep records of all the personal data we process. These records are kept by the Information Governance Team and need to be made available to the Information Commissioner's Office (ICO) on request. We need to record the purpose, lawful condition, who we share information with and how long we will keep it for.

2.3.11. Please notify the Information Governance 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 Data Protection 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. 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 make sure the information you process is accurate. 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 Information Asset Register 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 Governance team to make sure the Information Asset Register is updated.

2.8. **Principle 6 – Keep secure**

2.8.1. 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. **Individuals' rights**

2.9.1. Data protection legislation provides individuals with the following rights:

- know what we will do with their personal information.
- see a copy of what information is held about them (subject access right)
- ask us to have information rectified if it is inaccurate or incomplete

- request the deletion of their personal data (right to be forgotten)
- restrict the processing of their personal data
- data portability – request a machine readable copy of the personal data they have provided to us
- object to the processing of their personal data
- challenge automated decisions.

2.9.2. It is important to note that not all these rights apply in all circumstances. It will depend on the legal basis that we rely on to process the personal data.

2.9.3. We have one month to respond to a request in relation to the above rights. For complex cases, we can extend this for a further two months.

2.9.4. If you receive a request under any of the above rights, please forward it promptly to the Information Governance Team who will work with you to consider the request and provide a response.

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

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

- help to meet the one-month deadline and tell the Information Governance 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.

2.9.7. See supporting information 1 and 7 for additional information.

2.10. **Your rights as a member of staff**

2.10.1. We process your personal information throughout your employment and for a period of time afterwards. For more information, see our employee privacy notice.

2.10.2. 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 Governance Team.

2.10.3. 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)

2.11. **Disclosing information**

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

2.11.2. 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 Governance Team.

2.11.3. In cases where we regularly share personal data with another organisation, a data sharing agreement is required. The Information Governance 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.

2.11.4. When we release incident reports or provide interviews/statements for the Police, we will comply with the principles of Data Protection.

2.11.5. See Disclosure of Personal Information for more information.

2.12. **Buying in services**

2.12.1. 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.

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

2.12.3. 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 Governance Team if you have any questions.

2.13. **Enforcement action and criminal offences**

2.13.1. If we contravene data protection legislation, 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 £17 million, or prosecution of the Service or **an individual member of staff.**

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

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

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

2.14. **Information sharing**

2.14.1. Data protection doesn't stop you sharing personal information, but it does provide a framework to ensure any sharing is done lawfully.

2.14.2. Before you share personal information, you may need to carry out a Data Protection Impact assessment to ensure that the sharing is justified and proportionate. You will need to consider the following:

- Only share minimum amount necessary to satisfy the purpose
- Identify legal basis/processing condition
- Think about how you will share.

2.14.3. If you decide to share personal information, you will need to draw up an information sharing agreement. Please contact the Information Governance Team for assistance.

2.14.4. All completed information sharing agreements are kept in a central location by the Information Governance Team.

2.14.5. For more information on sharing personal information, please refer to the ICO's Data Sharing Code of Practice.

2.15. **Monitoring staff**

2.15.1. If it is considered necessary to monitor staff we must follow the Data Protection 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 covert Surveillance Risk Assessment is conducted. This must be approved by a member of SLT).
- 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.

2.15.2. 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.

2.16. **Complaints**

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

2.16.2. If individuals are still not satisfied after using our complaints procedure, they have a right to complain to the Information Commissioner.

3. Responsibilities

3.1. **All Members of Staff**:

- make sure you process personal information in accordance with this procedure and data protection legislation. 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
- carry out a Data Protection Impact Assessment for any new or changes to personal data processing
- advise the Information Governance team of any new personal data collection so that it can be recorded and made available to the ICO on request.

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 Governance 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 completes their e learning training on induction and refreshers every two years
- make sure your team follows the procedures and are appropriately trained
- where new processes and systems involving personal data are being introduced, carry out a Data Protection Impact Assessment (DPIA).

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

- make sure appropriate Information Governance arrangements are in place
- ensure 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

- work with the Information Governance team to ensure privacy notices are available and up to date
- advise the Information Governance team of any new personal data collection so that it can be recorded and made available to the ICO on request
- keep their Information Asset Register up to date
- make sure retention periods are set and adhered to.

3.5. **Information Governance Group**

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

3.6. **Information Governance Team**

- Keep records of personal data processing activities and make them available to the ICO on request.
- Record and monitor all subject access requests. Direct them to the relevant team and make sure a response is received within one month (or additional two months for complex cases).
- 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 Information Asset Register and Register of Processing Activities.
- Work with Information Asset Owners to ensure privacy notices are available on the website and on forms, as required.
- 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 for the provision of accurate advice and guidance for processing personal data.

1.2. **Information Governance Manager (Data Protection Officer)**

- Advise managers and members of staff on obligations under data protection legislation.
- Monitor compliance with data protection and the associated procedures.
- Provide advice on Privacy Impact Assessments and monitor performance.
- Cooperate with ICO on data protection issues and act as contact point with them.

4. Monitoring & Assurance

4.1. **Procedure Management**

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

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

4.1.3. Internal auditors will audit our Information Governance processes in line with the Information Governance Framework audit plan. There is a key performance indicator (KPI) on Data Protection at the quarterly Governance, 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 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.

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

5. Document Reference

5.1. Forms to complete

IM001 – Data Protection Impact Assessment Template

IM002 – Covert Surveillance Risk Assessment – Irregular staff monitoring

IM003 – Subject Access Application Form

IM004 – Non Disclosure Agreement

IM015 – Request for disclosure of personal data

5.2. Document References

IM 1 – Access to Information – FOI Act

IM 2 – Regulation of Investigatory Powers (RIPA)

IM 5 – Acceptable use of ICT

IM 9 – Information Security Incident Management (Security Breach)

IM 15 – Physical Information Security

IM 16 – Information Security Management

IM 17 – Closed Circuit Television (CCTV) (Premises)

5.3. Supporting Information

1 Subject Access

2 DPA Exemptions

3 Disclosure of Personal Information

4 Adequacy and accuracy

5 Retention and Disposal of Personal Information

6 Security of Personal Information

7 Individuals' Rights

Employee privacy notice

Information Asset Register

ICO's Data Sharing Code of Practice

6. Document Management

Policy Statement Reference: Corporate Governance			
Owner	**Review Date**	**Author**	**Status**
Lisa Smith	01/04/2019	Lisa Smith	Published

6.1. **Version Control:**

Version	Page & Par Ref	Date	Changes Made	Authorised By
V9.0	First and last pages	06/04/2020	Updated links within Relevant Document section to point from BrigadeHQ3 to pandp.dwfire.org.uk. No other changes made.	Tonya Saben
V 8.0	Entire document	27/11/2019	Reviewed entire document. Updated Information Management Team to Information Governance Team.	Lisa Smith
V7.0	Page 12 / Section 5.2	05/12/2018	Added a link to the newly received NFSP Request for disclosure of personal data. No other changes made.	Lisa Smith / Tonya Saben
V6.0	Page 1 & 13 1.2	12/06/2018	Updated Policy reference in accordance to new framework. Updated title of Information Manger to Information Governance Manger.	Tonya Saben
V5.0	Entire document	17/5/2018	Updated to reflect changes to data protection legislation	Lisa Smith
V4.0	Page 1	27/06/2017	Updated Policy Statement section with standardized description. No other changes made.	Tonya Saben
V3.0	Page 1 Page 11 / 5.1, 5.2 & 5.4	06/06/2016	Added link to IM Policy. Added section 5.1 and completed links to newly created forms and	Tonya Saben

			supporting Info.	
V2.0	11 & 12 / 5.1, 5.2 & 5.3	13/05/2016	Completed hyperlinks to forms, some of the document references and supporting information	T. Saben
V1.0	Entire document	27/01/2016	Published	V Shearing

Top of doc