DORSET & WILTSHIRE FIRE AND RESCUE

DORSET & WILTSHIRE FIRE AND RESCUE SERVICE

Managing Personal Information Procedure

To be used in conjunction with the Corporate Governance Policy Statement

Information Governance

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 advice 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 UK 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 – another organisation processing personal information on behalf of the Data Controller.
- Processing – obtaining, holding, amending, reading, sorting, disclosing, deleting, or destroying.
- Senior Information Risk Owner (SIRO) – A member of SLT with responsibility for information risk management.
- 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.
- Data Protection Impact Assessment (DPIA) – a DPIA is a process designed to help analyse, identify and minimise the data protection risks of a project, new system or way of working. A DPIA does not necessarily remove all risk, but should help minimise and determine whether or not the level of risk is acceptable in the circumstances.

- Technical Security Assessment (TSA) – a TSA is an assessment of the technical controls required in order to adequately protect information.
- Information Governance Impact Assessment (IGIA) – a DPIA and a TSA are incorporated into an IGIA, which is a wider assessment of the information risk a new project or system may pose to the Service.

2. Procedure Principles

2.1. Data Protection legislation (Data Protection Act/ UK 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 an overarching responsibility of accountability. This means being able to demonstrate compliance with the above principles. To do this, we must have appropriate records and measures in place, and ensure that we embed a privacy by design approach.

2.2.3. Before processing personal data, you may need to carry out an Information Governance Impact Assessment. 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

- Implementation of audio or visual surveillance
- Monitoring of staff.

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.

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 notices on our website informs the public why and how we use their information. We also must inform people about what we will be doing with their information at the point of collection, for example, at the start of a Home Safety Check form. This applies if you are collecting information over the telephone, in person, on a form (paper or electronic), 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. 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 or 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 held within our Information Asset Register (IAR). The IAR must 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 DPIA.

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. Please see IG checklist on Connect 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. Please 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 lawful 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 must 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. See supporting information 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 DWFRS privacy notices

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 via their website.

2.11. **Disclosing and sharing of personal information**

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

2.11.2. For more information on sharing personal information, please refer to the Information Sharing procedure or seek advice from the IG team.

2.12. **Buying in services and outsourcing of personal data/data processors**

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

2.12.2. Where a contractor or supplier is processing personal data on our behalf they are known as a data processor. This can include suppliers who are providing us with a software system. We are still legally responsible for the information and must provide the processor with clear instructions about how to process our data. This is known as a data processing agreement.

2.12.3. Prior to appointing a data processor, you must do the following:

- Complete an Information Governance Impact Assessment which may include a Technical Security Assessment.
- Put in place a contract which covers all the terms and clauses necessary to comply with data protection law. This includes providing clear instructions on the data they can process and what they can do with it.
- Carry out due diligence checks to guarantee that the processor will implement appropriate technical and organisational measures to meet data protection requirements. This could be done as part of the procurement process but needs to be carried out regardless of the procurement process that you follow and the value of the contract.
- Review the data processor's compliance with data protection throughout the duration of the contract.
- Seek advice from the Information Governance Team.

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. **Monitoring staff**

2.14.1. Data protection law does not prevent you from monitoring workers, but you **must** do so in a way which is compliant with data protection requirements.

2.14.2. Prior to carrying out any monitoring you must:

- Seek advice from the Data Protection Officer and approval from a member of SLT.
- Carry out an IG impact assessment.

2.14.3. If it is considered necessary to monitor staff we must follow the above data protection principles and the ICO guidance on monitoring workers 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 - Irregular Staff Monitoring 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.

2.14.4. 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.

2.15. **Complaints**

2.15.1. Our Data Protection Officer will investigate and respond to any complaints about how we process personal data.

2.15.2. 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 an Information Governance Impact Assessment Ifor 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 on the Information Asset Register and be 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**

- ensure you handle all personal information relating to members of staff who report to you in accordance with this procedure and data protection legislation. Further information is available in Personal Information Handling Guidance for line managers
- make sure all members of your staff (including temporary and agency staff) sign the non disclosure agreement
- make sure your team completes their elearning 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 an Information Governance Impact Assessment.

3.3. **Senior Information Risk Owner (SIRO)** make sure appropriate Information Governance arrangements are in place.

3.4. **Information Governance Team**

- Ensure that any actual or potential data breaches are logged and mitigated in accordance with Information Security Incident Management procedure.
- 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.
- Work with Information Asset Owners to ensure privacy notices are available on the website and on forms, as required.
- Assist in the completion of DPIAs/IGIAs, recommend controls and highlight risks to IAOs and the SIRO as appropriate.
- Ensure appropriate data sharing agreements are in place and provide advice on their content.
- Work with the procurement team to ensure data processing agreements are in place and provide advice on the completion of these.
- Provide advice and guidance to managers and members of staff to ensure compliance with data protection legislation
- Maintain knowledge and skills for the provision of accurate advice and guidance for processing personal data.

3.5. **Head of Information Governance and Security and 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 IG impact assessments and monitor performance.
- Cooperate with the 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 and Digital Data and Technology (DDaT) Board monitor information risk and compliance on a regular basis.

4.2. Learning and Development

4.2.1. All members of staff must complete the e-learning Protecting Information course during their induction and a refresher every two years.

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

Information Governance Impact Assessment

Covert Surveillance Risk Assessment - Irregular Staff Monitoring

CO-FO-0006 - Subject Access Application Form

CO-FO-0004 - Non Disclosure Agreement

CO-FO-0013 - Request for disclosure of personal data

5.2. Document References

CO-PR-0034 - Access to Information – FOI Act

CO-PR-0050 - Regulation of Investigatory Powers (RIPA)

CO-PR-0054 - Acceptable use of ICT

CO-PR-0051 - Information Security Incident Management (Security Breach)

CO-PR-0044 - Physical Information Security

CO-PR-0032 - Information handling and classification

CO-PR-0040 - Information Security Management

Information Sharing

5.3. Supporting Information

CO-SI-0073 - Subject Access

CO-SI-0072 - Personal information handling guidance for line managers

Information Asset Register (IAR)

Your Data, Your Rights

Information Governance Checklist

DWFRS privacy notices

Policy for processing special category data

ICO website

ICO guidance on monitoring workers

5.4. **Impact Assessment Link**

IA138025 - IM 3 - Managing Personal Information

6. Document Management

Policy Statement Reference: Corporate Governance			
Owner	**Review Date**	**Author**	**Status**
Lisa Breakspear	13/05/2028	Lisa Breakspear	Published

6.1. **Version Control:**

Page & Par Ref	Date	Changes Made	Authorised By
Entire document	25/07/2025	Number changed due to migration to new system	Connor Pepper

Top of doc