South Wales Fire & Rescue Service Privacy Notice – The National Fraud Initiative

Introduction

Under Data Protection legislation, SWFRS is required to provide information to all individuals about any personal information we collect from them and how we use that information.

This document relates specifically to data processed as part of the National Fraud Initiative.

For information on how SWFRS manages your personal data please refer to our Employee Privacy Notice, available via the HR – Employee Relations section of the intranet.

What is the National Fraud Initiative?

SWFRS is required by law to protect the public funds it administers, and may share information provided to it with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud. The National Fraud Initiative (NFI) is one way that this is achieved.

The Auditor General for Wales (the Auditor General) audits the accounts of all Welsh public sector bodies, and have tasked the Wales Audit Office (WAO) with undertaking the analysis required by the NFI.

The NFI is an exercise carried out every two years that aims to detect/prevent fraud and overpayments from the public purse across the UK.

It requires SWFRS (and a number of other public sector bodies) to collate a particular set of data over a 2 year period.

The analysis involves “Data Matching”.

What is Data Matching?

Data matching is the comparison of two or more sets of data.

For the NFI, the WAO will receive data sets from all of the mandatory organisations (such as SWFRS), as well as other public sector bodies that wish to participate.

These records are then compared, electronically, to see how far they match.

Where a match is found, it may indicate that there is an inconsistency which requires further investigation. This does not necessarily mean that there has been fraudulent activity or any overpayment, but it does highlight areas that may require further investigation.

What personal information is collected/provided for the NFI?

The information used for this exercise is already held by SWFRS for employment purposes. The Auditor General specifies the information needed. It will include the same information about every employee. The following information is provided (if we already hold it). We do not ask employees for any additional information purely for the NFI exercise:
- Staff Number, name and salary details,
- Date of Birth,
- Employee Contact details (such as telephone numbers and email address if held)
- Passport number,
- Employee start and finish dates
- National Insurance Number
- Date last paid,
- Bank details including sort code,
- Details of role undertaken – e.g. hours of work, location of work and post number.

Legal Basis to Process Your Data

In order to collect or use personal information, for any purpose, we must have a valid legal or lawful basis.

In this particular case the following bases apply:

- **The processing is necessary for compliance with a legal obligation of the controller**
  
  The information is requested by the Auditor General for Wales, under his powers under the Public Audit (Wales) Act 2004, as amended by the Serious Crime Act 2007. Under that legislation, the Auditor General has the power to conduct data matching (section 64a) and to identify organisations that must provide information to them. SWFRS is one those mandatory organisations, meaning we are required by law to provide the information.

In addition, as already stated, SWFRS has a responsibility to ensure that the public funds that it is responsible for are appropriately managed, therefore the following also applies:

- **The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller**

- **The processing is necessary for the purposes of the legitimate interests pursued by the controller**

Preparing the Information for NFI

As previously explained, the information provided for the NFI is already held by SWFRS. It is held by our HR department and is collated directly from the Core HR system.

For this exercise, the Payroll Manager is responsible for collating the data and is given the access needed to collate the information from the various databases within Core HR, only for the duration of the NFI.

How long will the information be held?

The report prepared by SWFRS will be held only until we have confirmation that it has been received by WAO and has been accepted. Once that confirmation is received the report itself is deleted from SWFRS systems, unless WAO ask us to keep it longer for any reason.
The data itself will still be on CORE HR – as it is held for other employment purposes; however, it is not held as one report, and the individual HR teams have access only to the elements needed for their particular role.

The WAO and the Auditor General securely destroy all the original datasets within 6 months of their submission. Any data that they collect or produce through the data matching exercise will destroyed within 3 months after the data matching exercise is completed. (They may retain elements if they are required for the purposes for any criminal investigations).

**How we protect your information**

All of our IT systems are protected by technical security measures to prevent unauthorised access, and those that retain your personal data are given access level controls, to ensure that only those people with the appropriate authorisation can access it.

The information itself is held on our HR system (Core HR). That system has in place access security – it is accessible only to those that require access to the data for their specific role, and they have access only to the parts of that system required for that role.

The data required for the NFI is collated from the different areas of the Core HR system, and the collated data set/report is stored on the Payroll Drive – accessible only to member of the payroll team. Only the Payroll Manager, has authorisation to work with and amend the collated data, although the report may be viewed by senior managers for quality assurance.

Disclosure of the final data set is done through a secure (encrypted) portal.

The WAO and the Auditor General are legally required to have in place specific security measures to comply with all relevant legislation, including Data Protection legislation.

**More Information**

For more information about the powers of the Auditor General for Wales, and the National Fraud Initiative, please visit the website of the Wales Audit Office - [Wales Audit Office](#)

**Your rights**

To enable individuals to have more control over the way their personal data is collected and used, data protection legislation gives you specific rights.

You have a legal right to request a copy of the information that we hold about you. Your request will be dealt with in line with Data Protection legislation. Please submit your request, in writing, to the Information Management Team.

SWFRS want to make sure that your personal information is accurate and you have the right to request we correct or remove information which you think is inaccurate. (Please note that you can update your own personal details using the CORE HR Portal)
You also have the right to ask for any personal data to be deleted, however, this applies only where it is inaccurate, incorrect and/or where there is no legal basis for us to retain it.

If you have any queries about the way SWFRS looks after your data, please refer to our employee privacy notice – SWFRS Employee Privacy Notice

Should you still have concerns, please contact our Information Governance and Compliance Officer (who is also our designated Data Protection Officer) on 01443 232213, or via email through dataprotection@southwales-fire.gov.uk

You also have the right to raise any concerns you have with the Information Commissioner, who oversees Data Protection Legislation. Further information can be found on their website - https://ico.org.uk/concerns/ or you can contact them here:

The Information Commissioner’s Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone - 0303 123 1113