

Report to	Executive Panel
Date	18 September 2023
Lead Officer	ACFO Stuart Millington
Contact Officer	Brian Mottershead, Data Protection Officer
Subject	Freedom of Information Assurance Report



PURPOSE OF REPORT

- 1 To provide assurance to the Executive Panel (the Panel) that the Service's process for handling information requests submitted under the Freedom of information Act 2000 is robust and minimises the risk of a data breach involving personal information.

RECOMMENDATION

- 2 It is recommended that Members:
 - i) note the content of this report.

BACKGROUND

- 3 There have been a number of reports recently of significant and serious personal data breaches by public authorities, including two in which personal data, including special category 'sensitive' data, were inappropriately released as part of responses to Freedom of Information (Fol) Act requests.

INFORMATION

- 4 The breaches in question are:
 - (i) Norfolk and Suffolk Constabularies including raw data relating to victims, witnesses and suspects, as well as descriptions of offences, in response to a number of Fol requests for crime statistics;
 - (ii) Police Service of Northern Ireland (PSNI) releasing data which included the surname, initials, rank/grade, role and location of all serving officers and staff, in response to a request submitted through the WhatDoTheyKnow web site ([whatdotheyknow.com](https://www.whatdotheyknow.com)) and which was available to view on the site for up to three hours before it was removed.

- 5 Fol requests received by North Wales Fire and Rescue Service (the Service) are actioned using the following process:
- (i) The request is checked for validity by the Data Protection Officer (DPO) and, if valid, recorded in the Fol Register, acknowledged, and sent to the relevant department(s) for provision of the data. The receiving department(s) might, at this point, ask the DPO to seek clarification from the requester of the information that is required, in which case the 20-working-day 'clock' is paused until the clarification is received. If clarification is not forthcoming within three months, the request will be cancelled.
 - (ii) The DPO receives the response from the relevant department(s), checks that the data provided answer the submitted questions and none of the data contain personal identifiable information, and confirms whether there are any exemptions that should be applied to those data. The most frequently used exemptions applied to Service Fol responses are:
 - i. Section 21 – information already reasonably accessible
 - ii. Section 24 – national security
 - iii. Section 38 – endangering health and safety
 - iv. Section 40(2) – personal information
 - v. Section 43(2) – prejudice to commercial interests
- NB Section 12 of the Act is occasionally applied to Fol requests received by the Service. This Section makes provision for public authorities to refuse requests for information where the cost of dealing with them would exceed the appropriate limit, which for local government is set at £450. This represents the estimated cost of one person spending 2.5 working days (18 hours) in determining whether the department holds the information, locating, retrieving and extracting the information.
- (iii) A response is prepared by the DPO and forwarded to the relevant Principal Officer for approval. Once approved the response is sent to the requester.

- 5 Throughout the process there may be discussions between the DPO and the providing department(s) about what data to include, an example being the inclusion of data relating to disciplinary processes, where numbers will be reported in bands (i.e. 0 to 5, 6 to 10, 11 to 15) rather than specific numbers, in order to avoid the possibility of individuals being identified. The same banding process would also be applied to salary information of staff.

- 6 The DPO is aware that some large public authorities delegate Fol responses to individual departments, thereby needing to ensure that staff in those departments have a sufficient level of knowledge to recognise the possibility of a data breach before it happens. This is not the case in the Service, as all Fol requests go through the DPO.
- 7 The DPO is pleased to be able to advise Members that there have been no NWFRS data breaches reported to date as a result of the inappropriate release of personal data in response to an Fol request.

IMPLICATIONS

Well-being Objectives	None
Budget	None
Legal	Possible regulatory action by the Information Commissioner's Office should a personal data breach occur which is likely to result in a high risk of adversely affecting individuals' rights and freedoms
Staffing	None
Equalities/Human Rights/ Welsh Language	None
Risks	None