



# ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

2023

## Abstract

This annual report provides an update from the Senior Information Risk Owner (SIRO) in respect of activity and performance related to information governance. It provides assurances that information risks are being effectively managed; what is going well; and where improvements are required.

Martina Doolan  
Data and Governance Manager

OFFICIAL

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

## Contents

Executive Summary .....	2
Introduction .....	3
Key Roles and Responsibilities .....	3
Governance and Monitoring Arrangements.....	5
Management and Assurance .....	5
Training _.....	6
Planned and Completed Activity in 3PT .....	6
What has been done .....	7
What is planned .....	8
Freedom of Information 2000 .....	9
Level of activity .....	9
FOI requests processed within 20-day statutory time limit .....	10
Exemptions .....	11
FOI Exemptions by Year .....	<b>Error! Bookmark not defined.</b>
Charges .....	12
Internal Reviews.....	12
Outcomes of Internal Reviews.....	12
Referrals to the Information Commissioner’s Office (ICO) .....	13
Referrals to the First Tier Tribunal (FTT) .....	13
Data Protection Act 2018 (DPA).....	14
Data Breach Management and Reporting .....	14
Environmental Information Regulations 2004 (EIR) .....	17
Transparency and Open Data .....	17
Conclusion .....	18

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

### Executive Summary

This annual report provides an update from the Senior Information Risk Owner (SIRO) in respect of activity and performance related to information governance for the previous year. It provides assurances that information risks are being effectively managed; what is going well; and where improvements are required. The report outlines new and emerging information governance considerations and the projects and tasks the organisation has in place to minimise risk and improve performance.

West Midlands Fire Service continues to be committed to effective information governance, with robust arrangements in place to ensure the organisation complies with legislation and adopts best practice. Governance arrangements are closely monitored to ensure systems, policies and procedures are fit for purpose; and that all employees and elected members understand the importance of information governance and security so that good practice is everyone's business and is embedded as part of the West Midlands Fire Service culture.

The most recent audit undertaken gave an outcome of 'substantial assurance' for freedom of information arrangements. Cyber risks present a real and increasing challenge to all organisations with a summary included to list action already undertaken and further activity planned to maintain and strengthen defences and enhance corporate resilience. Performance in relation to information requests processed under for example Freedom of Information and Data Protection legislation is summarised in the report.

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

### Introduction

- The annual report from the Senior Information Risk Owner (SIRO) reflects on the organisation's information governance work undertaken during the preceding year and provides assurances that personal data is held securely; information is disseminated effectively and provides an overview of key performance indicators relating to the organisation's processing of information requests within the necessary legal frameworks.
- The Annual Report also provides a forward look at new and emerging information governance considerations for the organisation, the work the organisation has in place to minimise risk or improve performance.

### Key Roles and Responsibilities

The Chief Fire Officer (CFO) is the most senior role in the service and is responsible for advising the Fire Authority and for ensuring, along with the Authority's Monitoring Officer and Treasurer, that the Authority can effectively discharge all responsibilities imposed upon it by statute and guidance.

West Midlands Fire and Rescue Authority are responsible for West Midlands Fire Service and are required to operate in accordance with a wide range of legislation. They are accountable to the communities of the West Midlands for the service provided by the fire service.

The role of Senior Information Risk Owner (SIRO) is held by the Assistant Chief Fire Officer (ACFO) for Community Risk Reduction with responsibility for information security within West Midlands Fire Service. There is a new post holder in this role during the reporting period and to provide resilience and support, other senior managers have undertaken SIRO training.

The SIRO role is supported by the Information Asset Owners (IAO) who are the Strategic Enabling Team (SET) with responsibilities for information assets within their respective areas. Some initial training has taken place for IAOs in Q4 2023 with more planned for the next reporting period.



The Data Protection Officer is responsible for monitoring internal compliance, inform and advise on the organisation's data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority i.e. The Information Commissioner's Office (ICO).

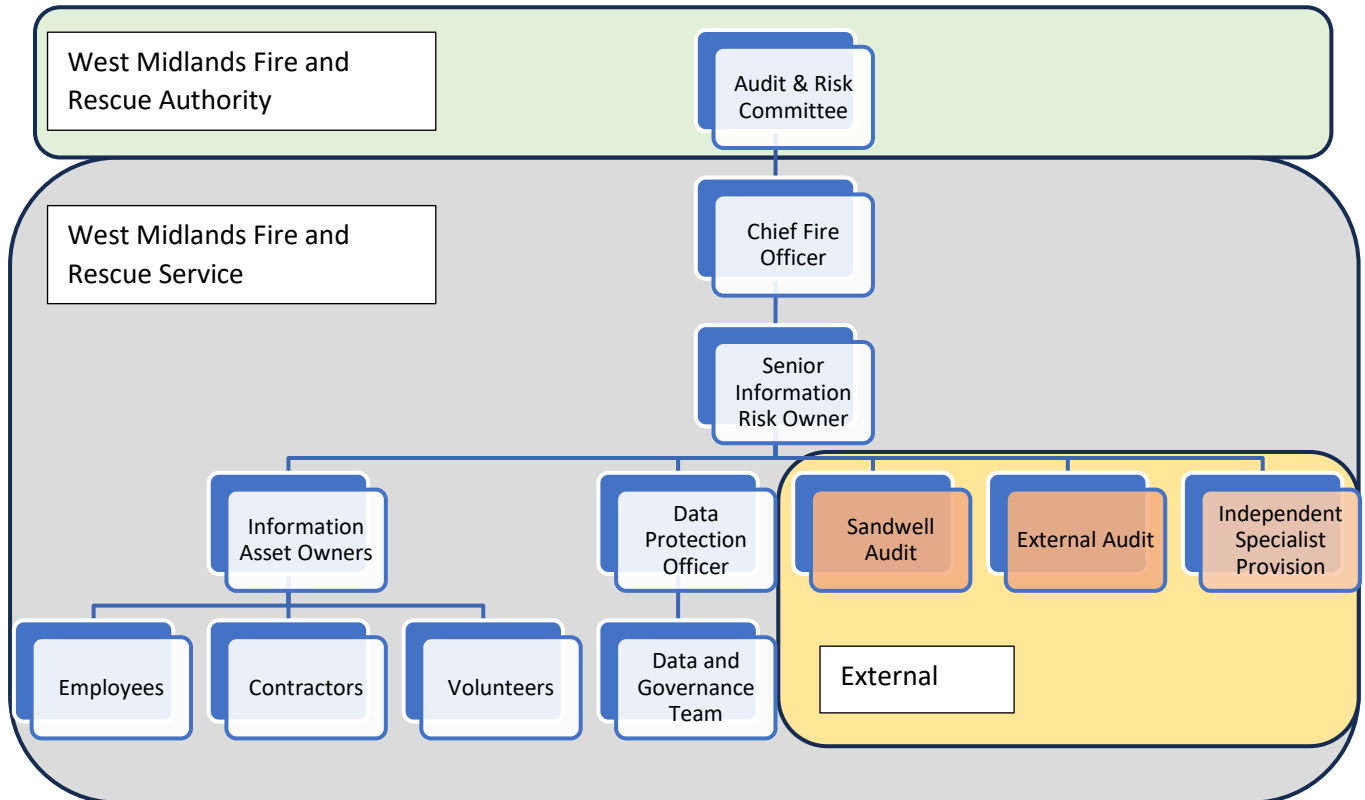
The Data and Governance team support the Data Protection Officer to effectively undertake their duties and provide specialist skills and experience to ensure appropriate resilience for information governance activities. The Data and Governance team has undergone restructure along with the rest of the Digital and Data area and more resources have been refocused into the Governance area.

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

Employees are responsible for adhering to the relevant policies of the organisation in respect of protecting information and adhering to appropriate classifications, handling instructions and confidentiality requirements.

Any third parties such as contractors or volunteers are also required to handle organisational assets in line with the relevant policies and this is supervised by the relevant hiring manager.

### Information Governance corporate structure



## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

### Governance and Monitoring Arrangements

West Midlands Fire Service is audited by Sandwell Metropolitan Borough Council (MBC) who conduct an annual themed review of matters related to information management. External audits are also undertaken by Grant Thornton to provide an additional layer of assurance. The most recent audit from Sandwell MBC gave the highest level of 'substantial assurance' without any advisory matters in relation to freedom of information activities for this reporting period. The planned information governance activities will build upon this outcome and seek to exceed this assessment.

The Audit and Risk Committee of West Midlands Fire Authority provide scrutiny of the arrangements in place within West Midlands Fire Service including information governance and compliance with relevant legislation.

The ICO is the UK's independent supervisory body set up to uphold information rights with responsibility for data protection, freedom of information and other legislation related to accessing information.

### Management and Assurance

West Midlands Fire Service has a Corporate Risk Register and Risks 7.1 and 7.2 relate to the confidentiality, integrity and availability of systems and data including identification of risk and the controls applied to mitigate the risk. Corporate risk 7.3 Cyber Security recognises the external



threats to organisational systems and data and gives focus to this important area. These risks are reviewed and reported to the Strategic Enabling Team monthly to ensure that emerging and new risks are captured in a timely manner.

The Portfolio, Programmes and Project system (3PT) captures risks related to transition and operational activities and ensures that these are monitored at Portfolio and Programme Board level.

The outcomes of audits by Sandwell MBC are integrated into the organisational

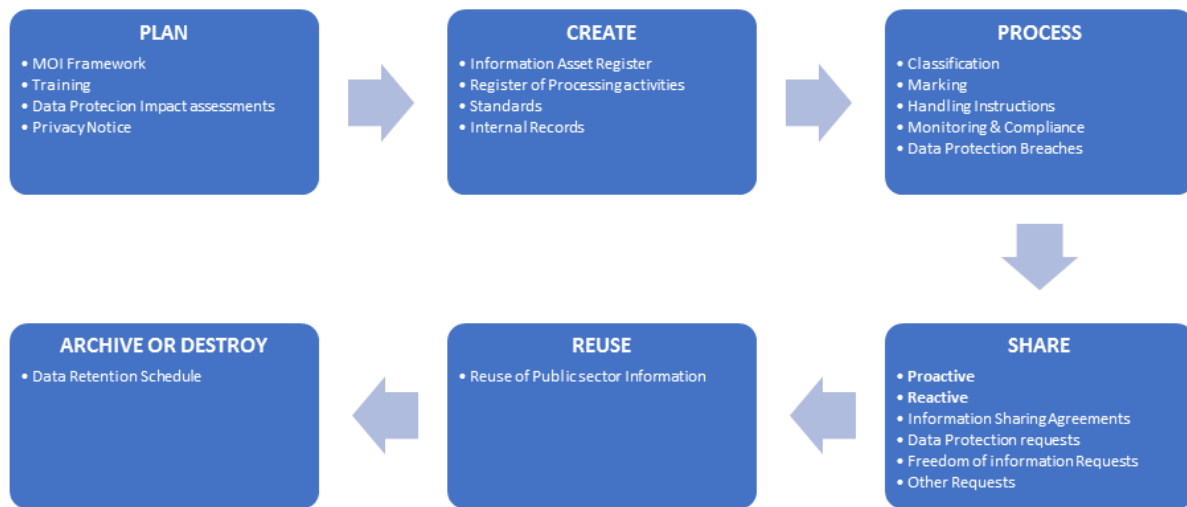
policies, processes, and procedures.

Periodically the organisation will commission external organisational assurance reviews and work with specialist companies to provide independent scrutiny of specialist areas such as Digital and Data to provide assurance that the organisational infrastructure is secure, and the threat of cyber security incidents is minimised.

The organisation has a Management of Information framework that is a comprehensive policy covering how information should be managed and includes classification, handling instructions, best practice, and guidance for all employees and is based upon the government Data Quality Life Cycle.

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

### Data Quality Life Cycle



Generic training is provided by the Data and Governance Team and covers managing information principles and compliance with data protection legislation. This is supported by regular global updates to remind employees about protocols related to the security of information and any new relevant policies. SET as the Information Asset Owners also receive bespoke training sourced externally to enable them to perform their role.

### Training

Course Name	Completed	Not Completed
Management of Information	80%	20%

Data protection awareness and education is embedded within the Management of Information training. This training has been refreshed to be available in the new Oracle system within the Learn module. Supplementary information and guidance are published periodically on the organisation's internal communications platforms in relation to best practice and when trends are identified through organisational intelligence.

### Planned and Completed Activity in 3PT

Information governance has been embedded as a key part of the digital transformation within the organisation, this area of work has moved to the Enabling Services Programme of Work and Digital and Data Business as Usual (BAU) project.

#### Completed in the Reporting Period:

The Management of information framework is a fast-moving policy and under continual review to ensure that the digital first strategy of the organisation is achieved and supported by the framework. The policy was updated to align to the government data quality life cycle and to set out a digital first approach to record retention thus reducing paper archives.

The automated enforced marking of documents, emails and other material was implemented and is continuing to be monitored for compliance against data loss prevention policies whereby incorrect application of the classification and labelling of material can be intelligently and automatically identified without manual intervention.

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

Automated information retrieval is embedded within the Data and Governance area and used regularly to improve compliance with statutory time limits for subject access requests under the Data Protection Act 2018 and reduce reliance on manual processes. This technology is also being used to maintain the information sharing register to ensure that a complete picture of where proactive information sharing is taking place with partner agencies.

The number and size of permanent paper and media archives has continued to be managed downwards and the digitising of information is the preferred approach in policies.

### Planned for the next Reporting Period:

The Management of Information framework has been updated to include further information about the subject access requests process, imagery, and digitisation of paper copies. Further work about contemporaneous notes and recording of information to align with best practice is planned.

Enforcement of information protection processes such as encryption will be implemented by default to minimise data loss and ensure that information is adequately protected in line with its classification.

Automation of activities within the information governance area will continue to streamline processes and deliver greater efficiencies.

Progress within this workstreams is reported monthly to the Enabling Services Programme Board including issues, risks, assumptions and dependencies with other organisational projects and programmes of work. Deviations from expected outputs are highlighted and discussed and impacts upon the expected value from the project are considered.

## Digital and Data Security & Cyber Risks



Information governance and cyber are significant risk areas for all organisations locally, nationally and globally, with risks of accidental data loss, physical system failures and direct malicious cyber-attacks an ongoing area requiring focus. There is an ongoing need for the organisation to address all aspects of this risk through robust technical solutions and risk management processes as well as addressing the cultural and behavioural elements of this risk. The National

Cyber Security Centre (NCSC) produces a weekly cyber security threat bulletin that evidences the risks to organisations both within the public and private sector.

### What has been done?

In summary, the following key actions were delivered which has improved the organisation's management of information risks:

- Implementation of outcomes from an external information assurance to remediate weaknesses in the management of passwords, patching of systems, administrators of systems.
- Decommissioning of legacy hardware servers and systems that are no longer required.

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

- Implementation of multi-factor authentication and conditional access giving improved management of identification of users and devices rolled out across the organisation.
- Better auditing of systems to identify incorrect sharing of information.
- Sharing of the content within this report with the Organisational Intelligence Team to improve policies and learning.
- Inclusion of the content within this report within the Station Peer Assessment (SPA) process.

### What is planned?

Progress has also been made with the following actions, with further work planned during the year 2024/5:

- Compliance with Government Minimum Technical Cyber Security Standards and accreditation with Cyber Essentials Plus which is an external verification and assurance of the organisational approach to information security.
- Automated classification of information and application of controls by default to reduce data loss.
- Introduction of new policies and procedures related to 'Bring Your Own Device' (BYOD)
- Significant investment in cyber security e.g. Virtual Chief Information Security Officer (CISO)
- Managed Detection and Response, Vulnerability Management, Identity Protection and Response
- Review and update of MOI/ GDPR Required training

As the importance of digital information and networks grows, cyber security is of high importance and remains a corporate priority. The type of risks posed include theft of sensitive corporate and personal data, theft or damage to data, threat of hacking for criminal or fraud purposes and potential disruption to infrastructure such as ICT systems, intranet, and public facing website.

The National Cyber Security Centre (NCSC) has advised that Cyber risk has been increasing over time and have published the NCSC Cyber Assessment Framework. Where possible WMFS has followed the published guidance and will be increasing compliance by working within the prescribed frameworks and standards.

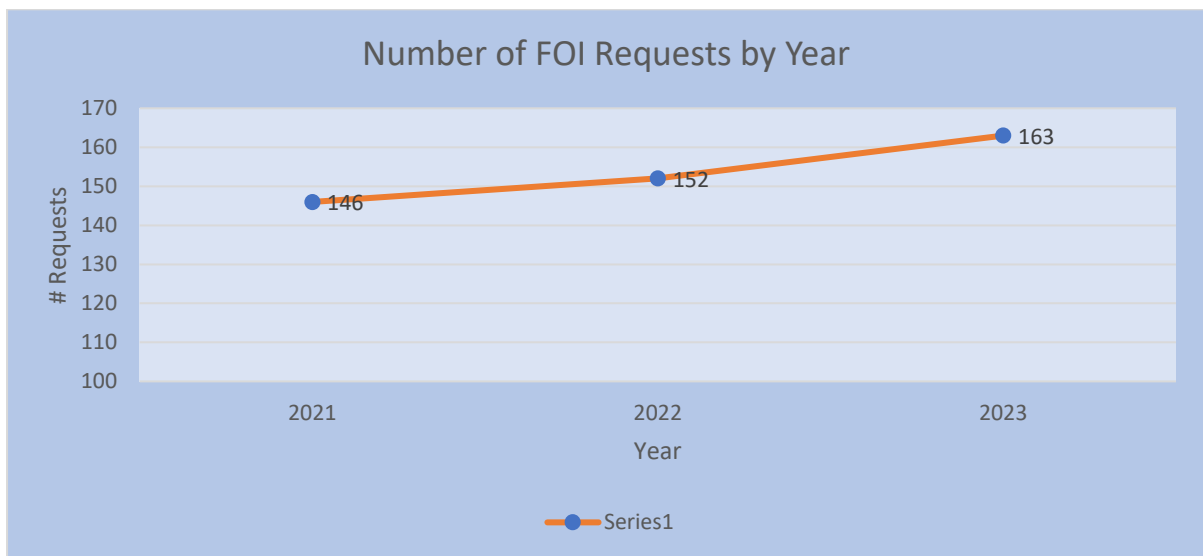
## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

## Freedom of Information 2000

The Freedom of Information Act 2000 gives people the right to request information from public authorities and is intended to promote a culture of openness, transparency and accountability amongst public sector bodies and enable the public to better understand how public authorities carry out their duties, how they make decisions and how they spend their money.

## Level of activity

Year	Number of FOI requests
2021	146
2022	152
2023	163



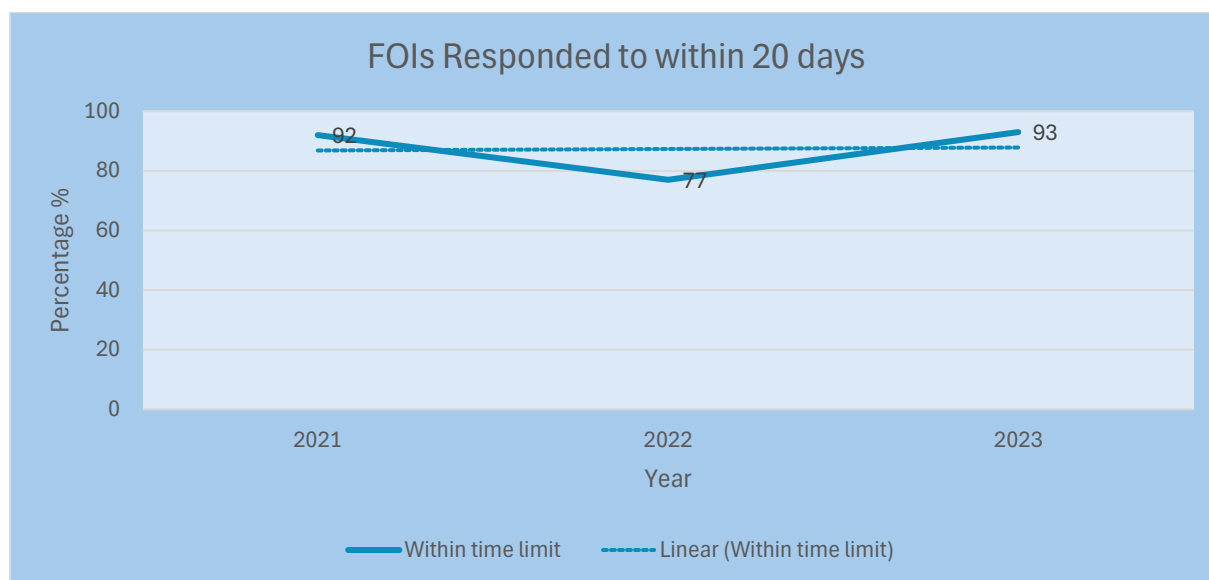
The number of requests processed and the trendline is upwards. Evidence from the Data and Governance team indicates that the complexity of requests has increased too.

Statistics are showing that the percentage of occasions where the information is readily accessible to the requester has increased therefore negating the requirement to gather the information which is more resource intensive than signposting to where the data is published or available. This approach adopted by the organisation to proactively publish information has underpinned this increased efficiency and aided transparency and openness.

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

FOI requests processed within 20-day statutory time limit.

Year	Within time limit %
2021	92
2022	77
2023	93



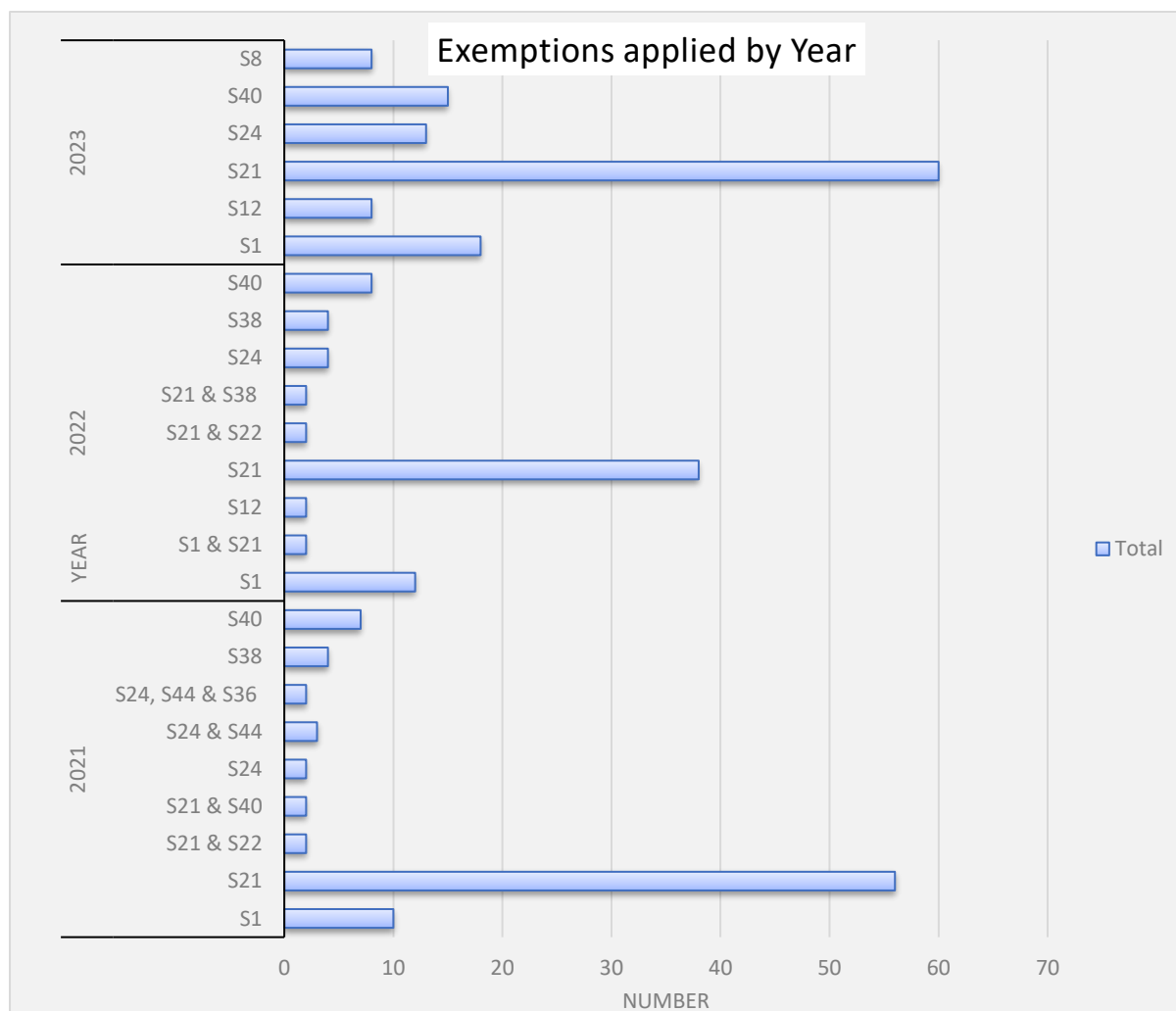
In 2022 there was a decline in the number of FOI requests being processed within the statutory time limit which was a cause for concern. An approvals process was automated in Q4 2022 and the response times have improved over the last reporting period (+16%).

The aspiration would be to respond to 100% of requests within the statutory timescale. The Information Commissioner's Officer has set the tolerance threshold at 90% and currently 52% of central government departments are not meeting this threshold. The organisation is currently achieving the 90% threshold by increasing automation of processes and using technology to assist where possible.

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

## Exemptions

Exemption applied	2021	2022	2023
Section 12 - Exceeds Cost Limit	0	3	4
Section 31(b) - Exempt from Disclosure	1	0	0
Section 36 - Prejudice public affairs	1	0	2
Section 22 - Future Publication	3	3	4
Section 8 - Invalid request	5	2	0
Section 44 - Prohibition on Disclosure	6	0	5
Section 38 - Health & Safety	6	2	5
Section 40 - Personal Data	8	5	16
Section 1 - Do not hold information	9	14	18
Section 24 - National Security	9	6	14
Section 21 - Reasonably Accessible by other means	34	39	60
Total	32	79	128



## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

### Charges

WMFS cannot charge for the provision of information, however if it is estimated that a request will incur unreasonable cost then it can issue a Refusal Notice under Section 12 of the Act and issue a Fees Notice. The threshold set by the Act is 18 hours (equivalent to £450 at a notional hourly rate of £25).

To reach a decision about whether to apply a Section 12 exemption, the Data and Governance Team works with the service area to estimate the expected time to:

- determine whether the information is held
- locate information or appropriate documents
- retrieve the information or document containing it
- extract the information.
- process the request

Year	Section 12 Notice	Total value	Paid
2021	0	0	Not applicable
2022	3	£1,150	None
2023	3	£3,462	None

### Internal Reviews

Customers who submit a FOI request can request an internal review if they are not satisfied with the response provided. Internal reviews provide WMFS with an opportunity to review the request handling process prior to any potential referral to the Information Commissioner's Office by the requester.

Year	Internal Review Requests
2021	1
2022	1
2023	0

### Outcomes of Internal Reviews

Year	Decision upheld	Fee notice	Further information
2021	1	1	0
2022	1	0	1*
2023	Not applicable	Not applicable	Not applicable

\*The requester had been directed to the information in the data published by the organisation but could not find it so further clarity was provided.

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

### FOI Referrals to the Information Commissioner's Office (ICO)

If an applicant is not satisfied with the outcome of an Internal Review, they can refer their case to the Information Commissioner, who will assess the case and make an independent decision about the way WMFS has handled the request.

Following a referral and a subsequent case investigation, the ICO can issue a Decision Notice requiring WMFS to disclose information it may previously have refused to disclose.

Year	Number
2021	0
2022	0
2023	0

No applicants have referred the organisation's internal reviews to the ICO for further review in the reporting period.

### Referrals to the First Tier Tribunal (FTT)

If an applicant is dissatisfied with the Information Commissioner's decision, they have the right to refer the matter to the First Tier Tribunal (FTT). WMFS can also appeal fines issued for data breaches and enforcement notices to the FTT. The FTT is independent of the Government and listens to representation from both parties before it reaches a decision. Any party wishing to appeal against an ICO Decision Notice has 28 days to do so.

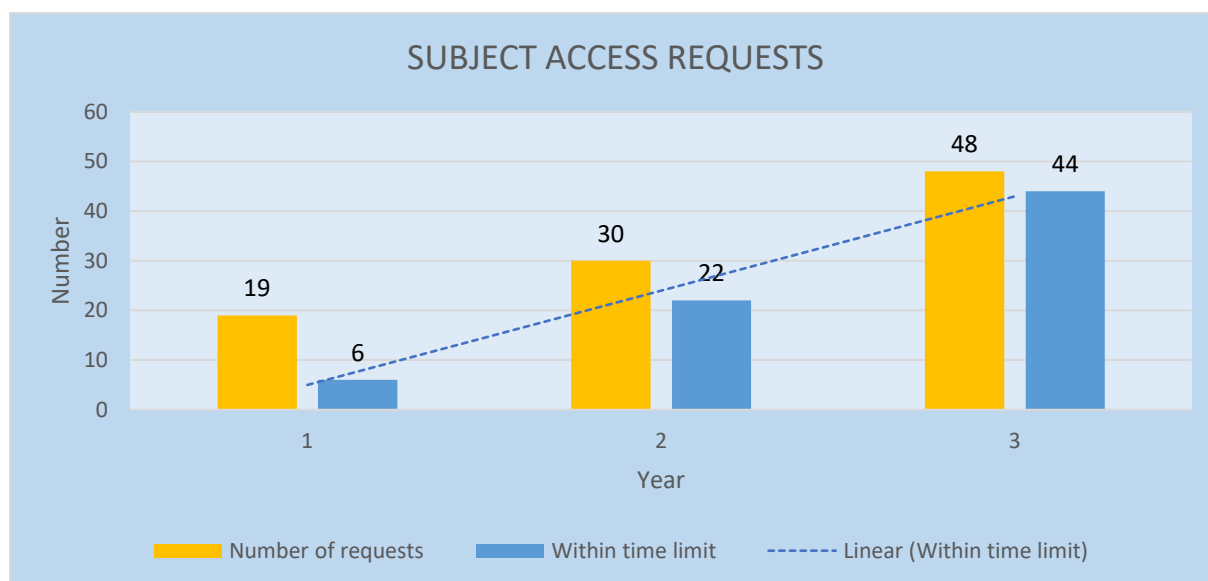
There have been 0 referrals to the FTT in the past 3 years

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

## Data Protection Act 2018 (DPA)

Under the Data Protection Act 2018 any living person, regardless of their age, can request information about themselves that is held by WMFS. This application process is referred to as a Subject Access Request (SAR).

Year	Number of requests	Within time limit
2021	18	7
2022	30	22
2023	48	44



Automation improvements were embedded within the information governance area to support the retrieval of information for SARs as previously the process was predominantly manual searches and redaction. It was reliant upon employees responding promptly to requests from the Information Governance Team, but this was impacted by availability and capacity. This new functionality has led to a significant improvement in retrieving relevant information increasing from 39% in 2021 to 92% in 2023. This is against a backdrop of a significant increase (+60%) in the number of SARs but also the complexity.

## Data Breach Management and Reporting

Any concerns relating to potential data breaches are promptly investigated and risk assessed based on scale, assessment of numbers of people affected, sensitivity, nature of breach and likely impact. Dependant on the assessment, the incident may need escalation to the SIRO and IAO and may be self-referred by WMFS to the Information Commissioners Office (ICO). The reporting, attempt to recover, investigation and learning phases of data breach incidents play a key role in the management of risk and improvement of internal controls. The introduction of the data protection feedback process also captures organisation learning and identifies improvements to prevent similar occurrences.

## Summary of Data Protection Breaches

The table below shows the number and broad categories of the type of data protection breaches within the organisation. The data protection breaches increased from 2018 which aligned with the

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

introduction of the General Data Protection Regulations and Data Protection Act 2018. Within the organisational implementation plan, increased training and guidance was made available to all employees so the increase in reporting may be an indicator of greater awareness.

	Number
<b>2021</b>	<b>23</b>
DM Security Incident - Human error - Personal information - breached	9
DM Security Incident : Criminal Activity : Spoofing Email: Personal Information – Breached	1
DM Security Incident : Unauthorised Access : Personal Information – Breached	4
DM Security Incident : Systems Error : Personal Information – Breached	6
DM Security Incident : Systems Error : Personal Information – Not Breached	2
DM: Security Incident: Ransomware 3 <sup>rd</sup> Party Supplier: Personal Information – Breached	1
<b>2022</b>	<b>24</b>
DM Security Incident Data Breach - Human Error Access to personal information	17
DM Security Incident Data Breach – Systems error – Personnel Information	4
DM Security Incident Data Breach – Lost equipment – Radio	1
DM Security Incident Data Breach – Human Error – Photograph	1
DM Security Incident Data Breach – Ransomware attack – external	1
<b>2023</b>	<b>33</b>
Human Error	19
Determined no breach occurred	5
System Error	4
Process	2
Inappropriate disclosure	2
Misuse of information	1

Consistently across the reporting period ‘Human Error’ was the single highest factor in data protection breaches. A refresh of the organisational Management of Information training is currently in progress to reduce the number of these incidents and consideration of more targeted training for specific areas.

There were 5 data protection breaches that were reported to the ICO in 2023. 4 of these were classified as ‘High risk’ to the individual’s rights and freedoms and were reported on this basis. One report was due to a data protection breach complaint, which we referred to the ICO for their determination.



- 1. P60/Payslip Sent to the wrong address** - The process requires payslips and P60s to be printed. Two Payslips and P60s were sent to the incorrect recipients. Both individuals had the same first name and a similar surname.

The ICO determined that no further action was required and that the case is now closed. They advised that it is important to have appropriate technical and organisational measures in place to ensure the security of personal data.

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

2. **LinkedIn Screenshots and email disclosure-** Information Governance referred a data protection breach complaint to the ICO for their determination. Although we did not believe that a data protection breach had taken place, the circumstances were complex, and the Data Subject did not agree with our decision.

Upon assessment, the ICO agreed with WMFS position that a breach did not appear to have taken place.

3. **Confidential Clinical notes-** 'Clinical in confidence' medical notes were shared in error with the Data Subjects Line Manager. The Line Manager would have been entitled to see an outcomes report from the Occupational Health Team, the notes should not have been shared.

The ICO recorded this as infringement under data protection law and advised that it is important to ensure that there is an appropriate level of security when processing personal data. The Data Subject is seeking litigation regarding this matter.

4. **Investigation bundle-** A package containing an appeal hearing bundle, was addressed incorrectly by the organisation and was received by a neighbour of the intended recipient. A secure delivery service had been used but checks and balances were not appropriately carried out by the operative. The 3<sup>rd</sup> party delivery service carried out an internal investigation under their relevant legislation.

The ICO did not pursue any regulatory action after receiving the report above but did provide advice and guidance to reduce the likelihood of future occurrences and processes were updated in the area to reflect this.

5. **Reckless disclosure** - A former WMFS employee disclosed sensitive information to an external trainer. The former employee had obtained the information while employed by WMFS.

This breach has been reported to the ICO and they have not provided a determination to date.

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

## Environmental Information Regulations 2004 (EIR)



Since the EIR Regulations came into force in 2004, WMFS has processed a very limited number of requests for information under this legislation.

EIR is similar to the Freedom of Information Act insofar as it gives the public access to environmental information to encourage greater awareness of issues that affect the environment. It includes policies, plans and procedures relating to the environment, reports on the state of the environment, and environmental impact studies. It also includes data taken from monitoring activities and risk assessments that affect or are likely to affect the environment.

There have been no requests received within the organisation under this legislation. However this may change due to a recent decision by the ICO ([Reference: IC-90850-D4P0](#)) that fire safety reports are environmental information and the appropriate legislation is the Environmental Information Regulations 2004.

## 12. Transparency and Open Data

The organisation routinely publishes data about its activities to promote awareness, understanding and scrutiny as a public body. It also creates efficiencies and reduces the time taken to handle FOI requests if the requester can be directed to the information.

Incident data is published on the organisational website and gives an anonymised overview of the incidents received, the type of incidents and the operational response in terms of appliances sent to deal with the incident. This information is processed against standardised geographies that are published from the Office of National Statistics (ONS).

Information about the breakdown of the workforce is also published giving detail about gender, ethnicity, belief systems, sexual orientation, age, and gender pay differentials.

Every FOI request is anonymised and published on the organisational website so that the public can see what has already been requested and re-use that information.

The Community Risk Management Plan is published on the organisational website setting out the priorities and objectives in 'Our Plan'. It was a rolling, three-year document which covered areas such as reducing serious traffic accidents, helping people have safer, healthier lives and ensuring emergencies are tackled effectively and safely. The format of this document will be changing during the next reporting period.

The Annual Assurance Report provides a yearly overview of governance activities and the framework in which the organisation operates. The document is available on the organisational website and links to other key pieces of information such as the Statement of Accounts (Summary and Full Reports), Annual Audit Letter, Efficiency Plan, Contracts, Expenditure over £500, land and building assets of the Authority and the Pay policy.

## ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

Information about fire safety enforcement action such as prohibitions and enforcement notices under the Regulatory Reform (Fire Safety) Order 2005 are published for every fire and rescue service through a data portal managed by the National Fire Chiefs' Council (NFCC).

The organisation also routinely provides returns to the Home Office about the incidents that it attends, the number of safe and well visits and fire safety audits it has undertaken, and information about the workforce profile. This information is anonymised and published on the government (.gov.uk ) website.

Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) publishes its assessment about how effectively and efficiently West Midlands Fire Service prevents, protects the public against and responds to fires and other emergencies. It also assesses how well the organisation looks after the people who work for the service.

### 13.Conclusion

Information is a key organisational asset and West Midlands Fire Service strives to derive maximum benefit from the information that it collects, shares and receives. To deliver this, it is critical that information is managed effectively and protected in terms of confidentiality, integrity, and availability so that the organisation can continue to make data driven decisions. A program of work is in place as part of the organisation's Portfolio to ensure that the benefits of data driven decision making are firmly embedded and the risks to this approach are mitigated.

The foundations of a robust information management framework have been delivered and is being reviewed to align with new ways of working and the introduction of technologies that will automate protecting data and accessing systems. The National Fire Chiefs' Council (NFCC) has published a national fire standard related to Data Management. A gap analysis is underway, and a program of work will follow to ensure that the organisation meets and exceeds this standard.

Minimum cyber security standards have been published by government and progress is being made against this to achieve compliance and benchmark against industry standards. Within the next reporting period, there will be a concerted effort to ensure that we build upon the 'substantial assurance' outcome from the last information governance themed audit by Sandwell MBC and maintain a position of excellence with information governance and assurance activities. Where possible technology is being used to simplify how we protect the confidentiality, integrity, and availability of information.

The focus for the following year is to implement functionality across the organisation to improve cyber security, protect information assets and prevent data loss by default. Retention and archiving of information will become more automated and proactive. There will also be a drive to consolidate and simplify data across fewer platforms so that manual entry reduces, efficiencies are realised, and it becomes easier to make information available to those who need it and protect it from those who should not have access.