ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

2022

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.

Karen Gowreesunker
Karen.Gowreesunker@wmfs.net

ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

Contents

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 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.

Introduction

- The annual report from the Senior Information Risk Owner (SIRO) Annual 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, as the most senior role in the service, 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. There has been an interim Chief Fire Officer appointed within the organisation due to the retirement of the previous incumbent.

West Midlands Fire and Rescue Authority are responsible for the governance of 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 for Enabling Services with responsibility for information security within West Midlands Fire Service.

There is a new post holder in this role and to provide resilience and support, other Brigade Managers have also undertaken SIRO training.

The SIRO role is supported by the information Asset Owners (IAO) who are the Strategic Enabling Team (SET) with responsibility for information assets within their respective areas.

The Data Protection Officer is responsible for monitoring internal compliance, informing and advising on the organisation's data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and acting 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 are undergoing restructure along with the rest of the Digital and Data area and more resources are being 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.

ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

Governance and Monitoring Arrangements

West Midlands Fire Service is audited by Sandwell 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' in relation to data protection 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 including identification of risk and the controls applied to mitigate the risk. A new risk 7.3 Cyber Security was added to the Corporate Risk Register

in this reporting period to give greater 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 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.

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

Data protection training, specific to role, has been provided to Staffordshire and West Midlands Fire Control by the Data Protection Officer from Staffordshire Fire and Rescue Service.

Training

Course Name	Completed	Not Completed
Management of Information	75%	25%
GDPR	87%	13%

Going forward, the GDPR module will be withdrawn, and data protection will be embedded across the Management of Information training. It will be modular in structure focusing in-depth on specific aspects of information governance. This aligns to the organisation's strategy and data driven approach requiring a greater level of maturity and enhanced capability in the organisation.

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 being 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.

Automated information retrieval is 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.

Implementation of a Data Protection Feedback process has captured organisational learning from data protection breaches to aid future prevention and identify emerging risks.

A programme of work is underway to reduce or remove permanent paper archives and continue to digitise information going forward which is supported as 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.

ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

The implementation of an automated FOI management process is in development and development time has been substantially reduced by reusing existing code and aligning this process to the very successful Complaints, Compliments and Comments (CCC) system that has been introduced within the organisation.

Progress within this workstream 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 risk are considered to be 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:
- Attainment of Cyber Essentials which is a government backed scheme that enables organisations to assess themselves against a set of pre-defined standards.
- Implementation of outcomes from an external information assurance to remediate weaknesses in the management of passwords, patching of systems and treatment of legacy hardware and software systems.
- Proactive scanning of infrastructure to monitor activities and more easily identify areas of concern.
- Implementation of multi-factor authentication and conditional access giving improved management of identification of users and devices rolled out widely across the organisation.

What is planned
Progress has also been made with the following actions, with further work planned during the next year:
- Outputs from external audit of IT by Grant Thornton to be scheduled into program of work.
- 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.
- Implementation of multi-factor authentication and conditional access giving improved management of identification of users and devices to be rolled out to all users.
- Automated classification of information and application of controls by default to reduce data loss.

- Planned internal cyber security exercises using toolkits provided by the Cabinet Office.
- 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.

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 our public facing website. The National Cyber Security Centre (NCSC) has advised that Cyber risk has been increasing for several years and where possible WMFS has followed the published guidance and achieved accreditation with Cyber Essentials. Pockets of global instability heighten the risk of cyber-attacks, and this has been experienced by the organisation through 'spoofing' emails from Russian email domain addresses.

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
2020	123
2021	146
2022	152

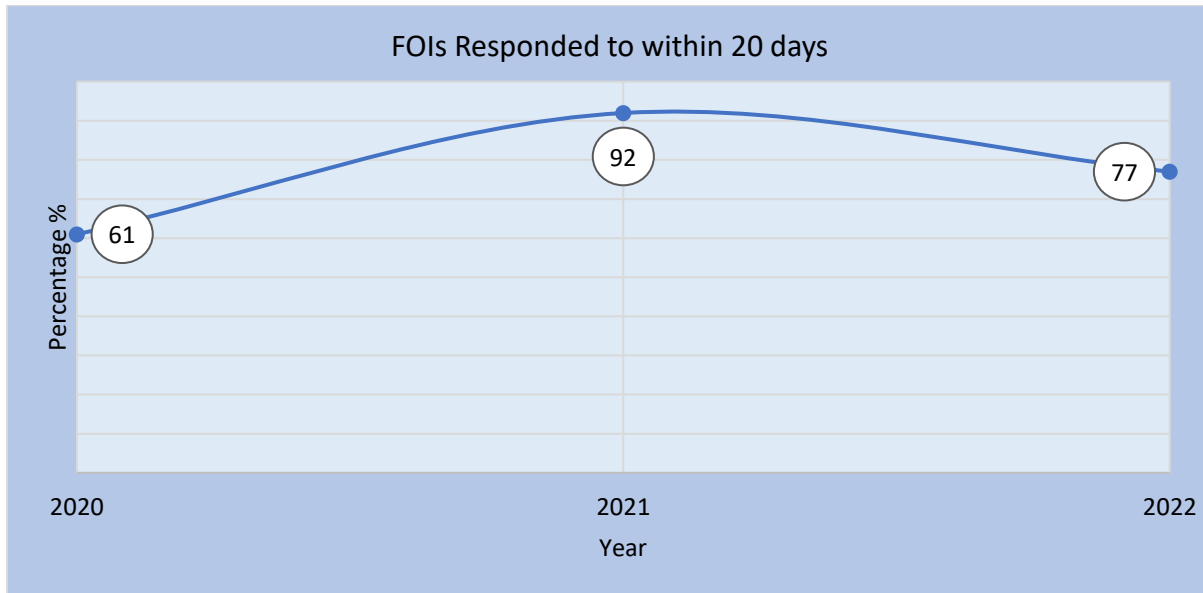**Number of FOI Requests by Year**
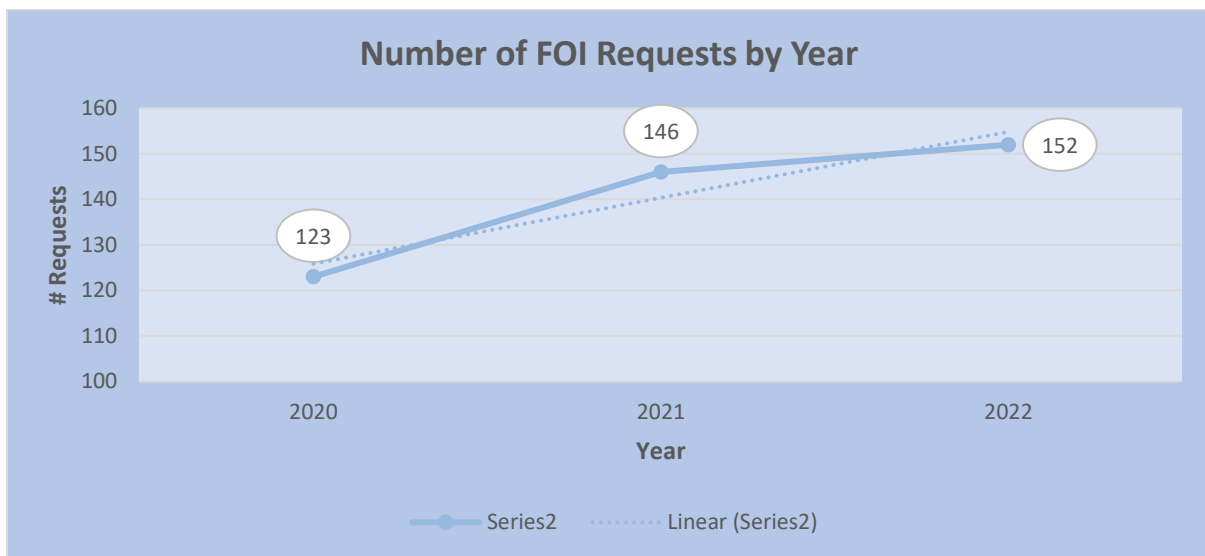
The number of requests processed and the trendline is upwards but not as pronounced as the increase from 2020 to 2021 which may be attributable to the global pandemic. Anecdotal evidence from the Data and Governance team indicates that the complexity of requests has increased.

Statistics are showing that the number of occasions where the information is readily accessible to the requester has increased. This negates 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 %
2020	61
2021	92
2022	77

In 2022 there was a decline in the number of FOI requests being processed within the statutory time limit. It did not return to the previously lower levels of 2020 but is a cause for concern. The approvals process was automated in Q4 2022 and it is anticipated that the response times will improve for the next reporting period.

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 would want to at least return to the 90% threshold by Q4 2023.

ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

Exemptions

Exemption applied	2020	2021	2022
Section 12 - Exceeds Cost Limit	1	0	3
Section 14 - Vexatious or Repeated	0	0	0
Section 30 - Investigations	0	0	0
Section 41 - Confidentiality	0	0	0
Section 32(1) - Court record	0	0	0
Section 43 - Commercially Sensitive	0	0	0
Section 31(b) - Exempt from Disclosure	0	1	0
Section 36 - Prejudice public affairs	0	1	0
Section 22 - Future Publication	1	3	3
Section 8 - Invalid request	1	5	2
Section 44 - Prohibition on Disclosure	2	6	0
Section 38 - Health & Safety	0	6	2
Section 40 - Personal Data	2	8	5
Section 1 - Do not hold information	8	9	14
Section 24 - National Security	1	9	6
Section 21 - Reasonably Accessible by other means	16	34	39
Total	32	79	74

Exemptions Applied by Year'
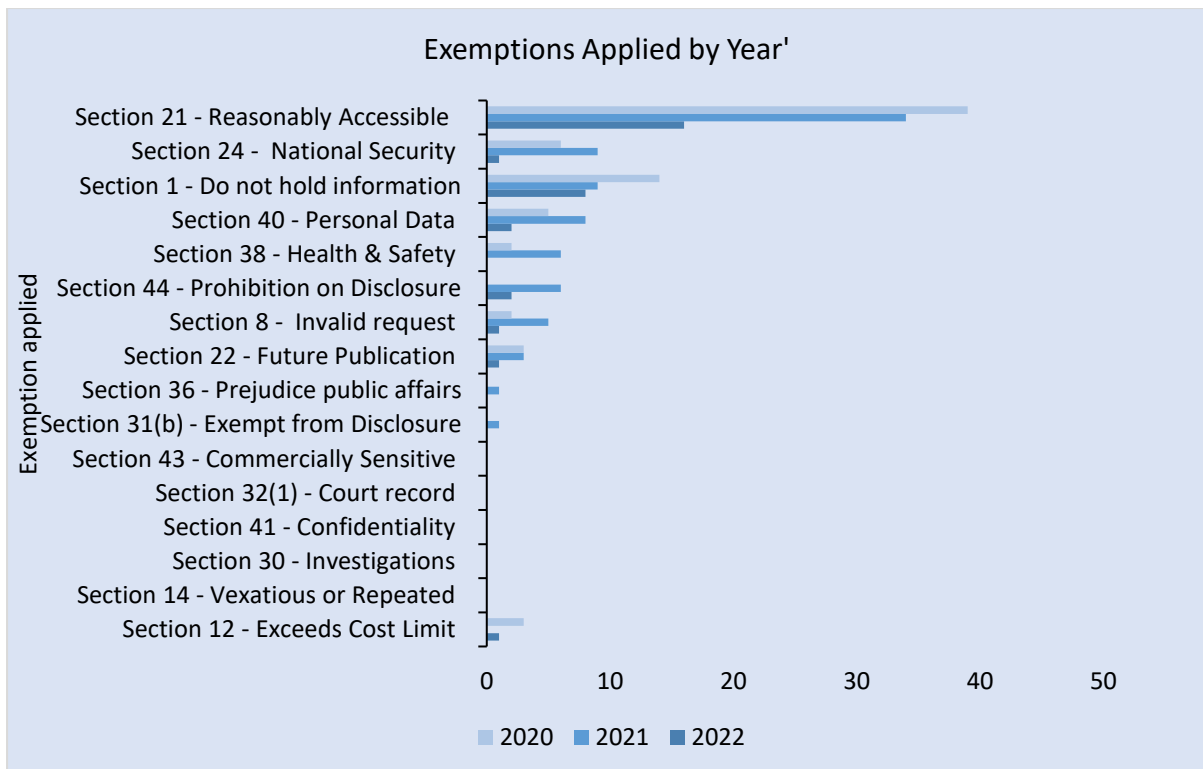
ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

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
2020	1	£6250	None
2021	0	0	Not applicable
2022	3	£1150	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
2020	1
2021	1
2022	1

Outcomes of Internal Reviews

Year	Decision upheld	Fee notice	Further information
2020	1	1	0
2021	1	0	1*
2021	1	0	1*

*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
2020	0
2021	0
2022	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
2020	7	2
2021	18	7
2022	30	22
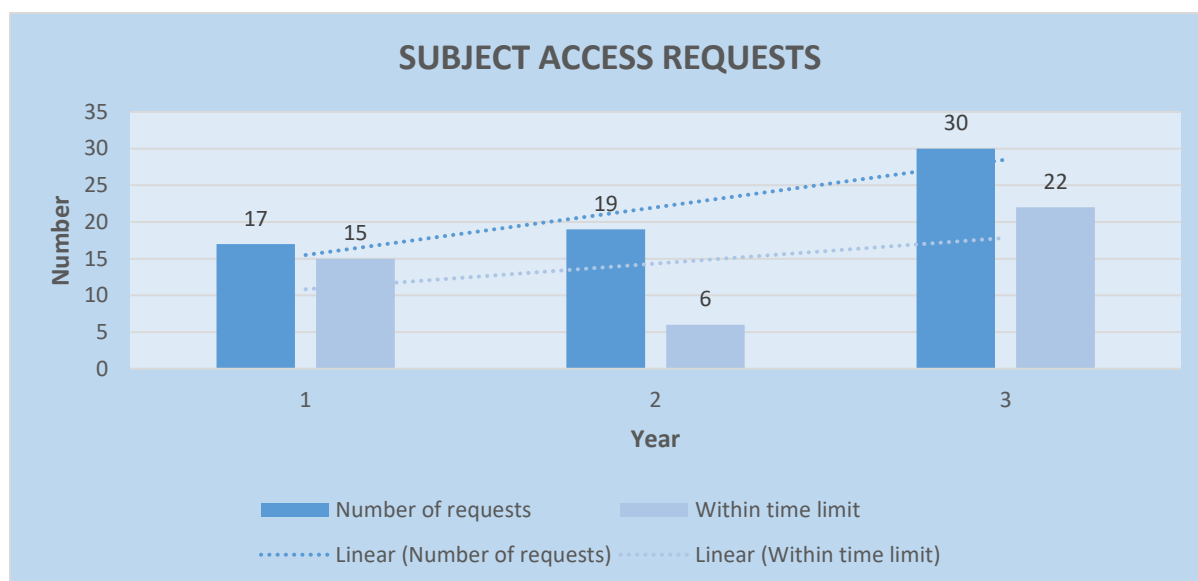
Automation improvements were successfully piloted to support the retrieval of information for SARs as previously the process was predominantly manual searches and redaction. It was reliant upon employees responding promptly to requests from the Governance Team, but this can be impacted by availability and capacity. These new innovations have shown a significant improvement in retrieving relevant information increasing from 39% in 2021 to 73% in 2022. This is against a backdrop of a significant increase 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 introduction of the General Data Protection Regulations and Data Protection Act 2018. Within the

ANNUAL REPORT OF THE SENIOR INFORMATION RISK OWNER

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
2020	**10**
DM Security Incident : Human Error : Personal Information - Breached	8
DM Security Incident : Human Error : Personal Information -Possible Breach	1
DM Security Incident : Unauthorised Access : Personal Information – Breached	1
2021	**22**
DM Security Incident - Human error - Personal information - breached	8
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 3rd Party Supplier: Personal Information – Breached	1
2022	**24**
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
Total	**56**

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 2 data protection breaches that classified as High risk to the individual's rights and freedoms and were reported to the ICO:

1. Inappropriate handling of payslips – Pensioner payslips were posted without an appropriate level of obfuscation of the personal data contained inside and;

2. Inappropriate use of a personal image – A personal image was used inappropriately by a 3rd party causing distress to a female employee.

The ICO did not pursue any regulatory action because of the reports above but did provide advice and guidance to reduce the likelihood of future occurrences.

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 is a rolling, three-year document which covers things like reducing serious traffic accidents, helping people have safer, healthier lives and ensuring emergencies are tackled effectively and safely.

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.

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. There are projects in place to digitise paper records and as part of this process, retention and archiving will become more automated and proactive. There will also be a drive to consolidate and simplify data across fewer platforms so that it becomes easier to make information available to those who need it and protect it from those who do not need it.