Annual Report Of The Senior Information Risk Owner

OCTOBER 2020

WEST MIDLANDS FIRE SERVICE

Making the West Midlands Safer, Stronger and Healthier

www.wmfs.net
@WestMidsFire

Contents

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.

WEST MIDLANDS FIRE SERVICE

Making the West Midlands Safer, Stronger and Healthier

www.wmfs.net
@WestMidsFire

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. 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. 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) 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 is the most senior role in the service he 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 and West Midlands Fire Service 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 (Process Programme Executive) with responsibility for information security within West Midlands Fire Service.

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.

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).

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.

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 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 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. This is 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 Programme Board

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.

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. SET as the Information Asset Owners also receive bespoke training sourced externally to enable them to perform their role.

Training Uptake

Course Name	Completed	Not Completed
Management of Information	76%	24%
GDPR	81%	19%

Planned and Completed Activity in 3PT

There is a project within 3PT called Management of Information which contains tasks and sub-tasks to improve and transform the way in which information is managed within the organisation. The high-level stages of the programme of works is below:

Activity	Description	Status	Delivered
Stage 1 Framework	Creation of the Management of Information Framework	Completed	2017
Stage 2 Classification	Definition of organisational classification scheme	Manual system - Completed Automation of marking – In Progress	2017
Stage 3A Information Sharing	Mechanism to ensure that organisational information sharing is managed centrally	Completed	2017
Stage 3B Automated Requests	System to automate requests for information such as under the Freedom of Information Act	In progress	To be completed in 2020/21

Stage 4 Training	Training packages created and made available to employees through the e-learning system	Completed	2017 MOI 2018 GDPR
Stage 5 CIA	Improvements to infrastructure, processes, and systems to strengthen cyber security.	In progress	To be completed in 2020/21
Stage 6 GDPR	Implementation of GDPR and new data protection legislation	Completed	2018

Progress within this project is reported monthly to the Process 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.

What is planned:

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

- 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 giving improved management of identification of users and devices.
- Automated classification of information to reduce data loss by applying controls by default.
- 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.

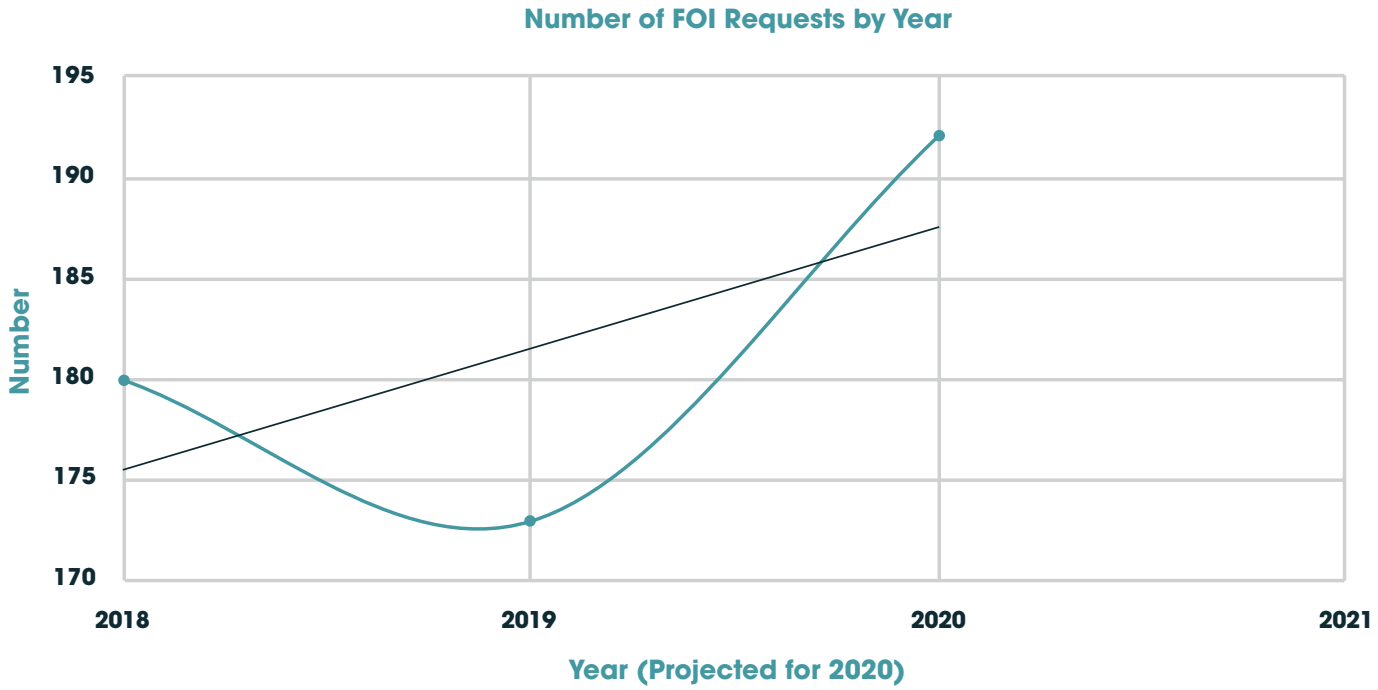
As the importance of digital information and networks grows, cyber security is of high importance and remains a corporate priority. The type of risks posed include theft of sensitive corporate and personal data, theft or damage to data, threat of hacking for criminal or fraud purposes and potential disruption to infrastructure such as ICT systems, intranet, and public facing website. The National Cyber Security Centre (NCSC) has advised that Cyber risk has been increasing and for several years and where possible WMFS has followed the published guidance and achieved accreditation with Cyber Essentials.

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

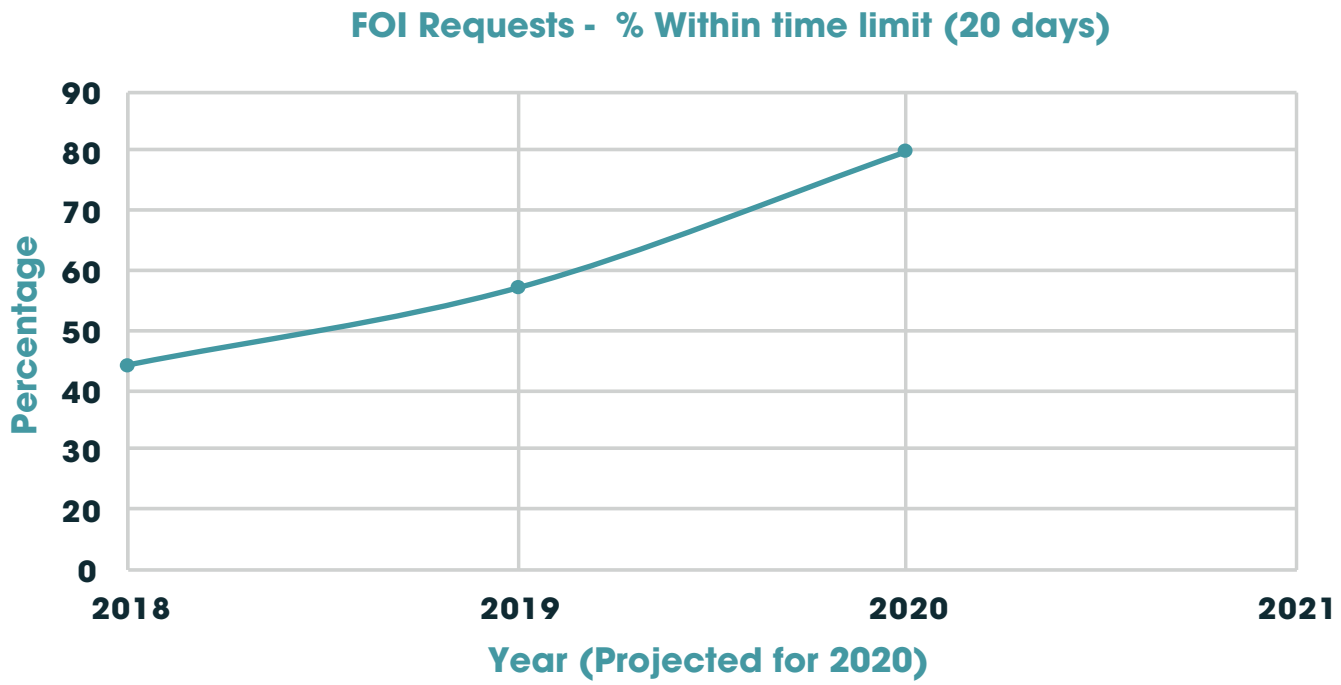
Year	Number of FOI requests
2018	180
2019	173
2020 (To end of August)	76 (Projected 192)



There is an increase in the number of requests processed and the trendline is upwards. Anecdotal evidence from the Governance team indicates that the complexity of requests has also increased.

FOI requests processed within 20 -day statutory time limit

Year	Within time limit
2018	80
2019	98
2020	61

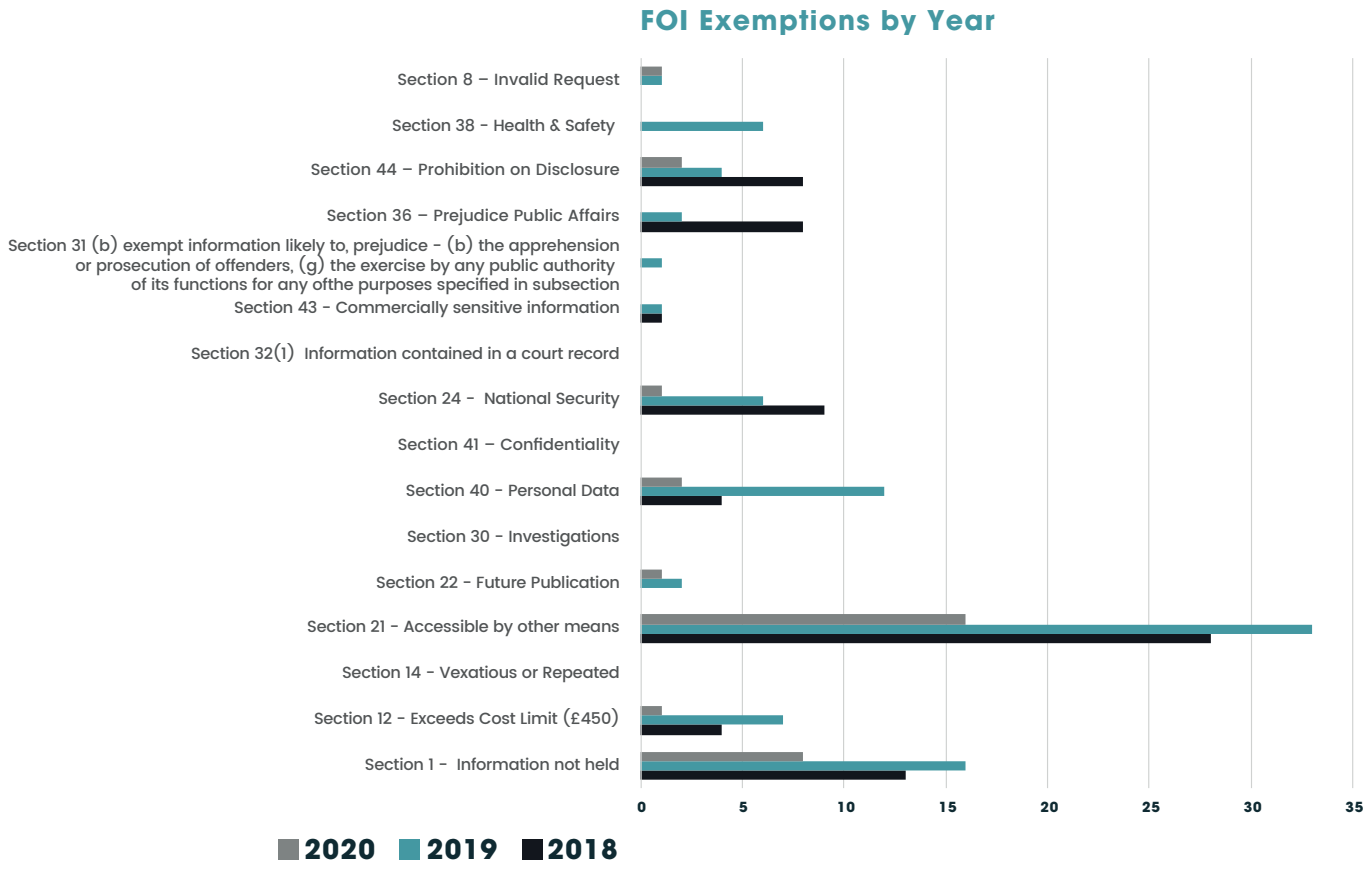


There has been an increase in the percentage of requests processed within the statutory time limit. It was identified during an internal audit in 2019 that a significant number of requests were not being processed within the statutory time limit and this was considered as part of the restructure within Digital and Data. The reorganisation of resources and the creation of a Governance Team has delivered this improvement. The strategy to proactively publish information has meant that some requests are easier to process. The complexity of the remaining requests and possibly due to remote working, the time elapsed to gather information is longer. The process is currently predominantly manual and reliant on the Governance Team to retrieve information to fulfil requests from other sections who may not always appreciate the statutory time scale for response.

There are automation improvements planned for FOI to automatically flag and escalate elapsed time and improve the number of requests that are completed within the statutory time limit of 20 days. 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 achieve the 90% threshold by Q4 2021.

Exemptions

Exemption Times Applied:	2018	2019	2020
Section 1 - Information not held	13	16	8
Section 12 - Exceeds Cost Limit (£450)	4	7	1
Section 14 - Vexatious or Repeated	0	0	0
Section 21 - Accessible by other means	28	33	16
Section 22 - Future Publication	0	2	1
Section 30 - Investigations	0	0	0
Section 40 - Personal Data	4	12	2
Section 41 – Confidentiality	0	0	0
Section 24 - National Security	9	6	1
Section 32(1) Information contained in a court record	0	0	0
Section 43 - Commercially sensitive information	1	1	0
Section 31 (b) exempt information likely to, prejudice - (b) the apprehension or prosecution of offenders, (g) the exercise by any public authority of its functions for any of the purposes specified in subsection	0	1	0
Section 36 – Prejudice Public Affairs	8	2	0
Section 44 – Prohibition on Disclosure	8	4	2
Section 38 - Health & Safety	0	6	?
Section 8 – Invalid Request	0	1	1
Total	75	91	32


FOI Exemptions by Year
Section 8 – Invalid Request
Section 38 - Health & Safety
Section 44 – Prohibition on Disclosure
Section 36 – Prejudice Public Affairs
Section 31 (b) exempt information likely to, prejudice - (b) the apprehension or prosecution of offenders, (g) the exercise by any public authority of its functions for any ofthe purposes specified in subsection
Section 43 - Commercially sensitive information
Section 32(1) Information contained in a court record
Section 24 - National Security
Section 41 – Confidentiality
Section 40 - Personal Data
Section 30 - Investigations
Section 22 - Future Publication
Section 21 - Accessible by other means
Section 14 - Vexatious or Repeated
Section 12 - Exceeds Cost Limit (£450)
Section 1 - Information not held
0
5
10
15
20
25
30
35
2020
2019
2018

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
2018	4	£443,833	None
2019	7	£17,750	None
2020	1	£6,250	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
2018	6
2019	3
2020	1

Outcomes of Internal Reviews

Year	Decision upheld	Fee notice	Further information
2018	4	1	1
2019	1	2	0
2020	0	1	0

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
2018	0
*2019	*1
2020	0

*This was due to late response and then a Fees Notice were issued.

Referrals to the First Tier Tribunal (FTT)

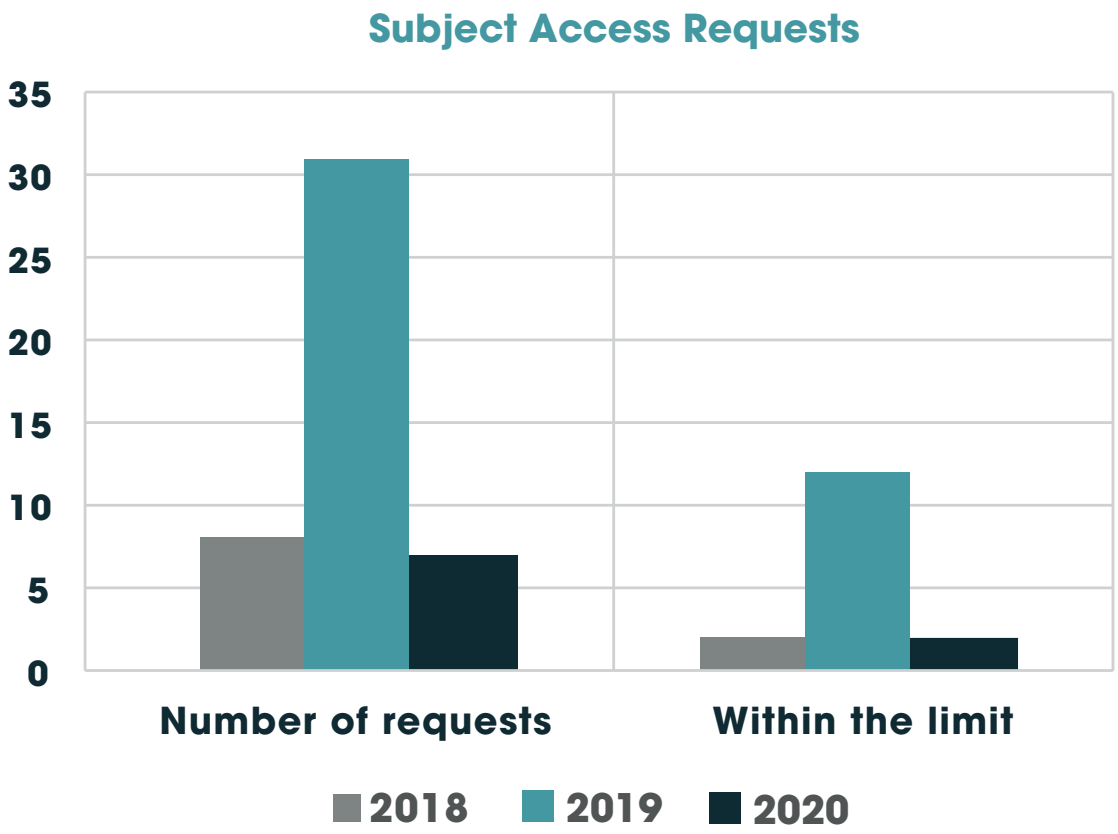
If an applicant is dissatisfied with the Information Commissioner's decision, they have the right to refer the matter to the First Tier Tribunal (FTT). WMFS can also appeal fines issued for data breaches and enforcement notices to the FTT. The FTT is independent of the Government and listens to representation 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.

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
2018	8	2
2019	31	12
2020	7	2



Automation Improvements are being considered to support the retrieval of information for SARs as currently the process is predominantly manual searches and redaction. It is reliant upon employees responding promptly to requests from the Governance Team, but this can be impacted by availability and capacity.

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 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.

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 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
2017	**6**
DM Security Incident : Hardware Loss / Theft : Personal Information - Not Breached	1
DM Security Incident : Human Error : Personal Information - Breached	3
DM Security Incident : Unauthorised Access : Personal Information - Breached	1
DM Security Incident : Unforeseen Circumstances : Personal Information - Breached	1
2018	**31**
DM Security Incident : Hardware Loss / Theft : Personal Information - Not Breached	1
DM Security Incident : Human Error : Personal Information - Breached	17
DM Security Incident : Human Error : Personal Information - Not Breached	1
DM Security Incident : Unauthorised Access : Personal Information - Breached	6
DM Security Incident : Unauthorised Access : Personal Information - Not Breached	1
DM Security Incident : Unforeseen Circumstances : Personal Information - Breached	2
DM Security Incident : Unforeseen Circumstances : Personal Information - Not Breached	3
2019	**43**
DM Security Incident - Human error - Personal information - Breached	5

DM Security Incident : Hacking of email accounts : Personal Information Breached	1
DM Security Incident : Hardware Loss / Theft : Personal Information - Not Breached	1
DM Security Incident : Human Error : Personal Information - Breached	30
DM Security Incident : System Error : Personal Information - Breached	1
DM Security Incident : Systems Error : Personal Information - Not Breached	1
DM Security Incident : Unauthorised Access : Personal Information - Breached	4
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
Grand Total	**90**

Consistently across the reporting period 'Human Error' was the single highest factor in data protection breaches. A refresh of the organisational training is currently in progress to reduce the number of these incidents.

There were 4 data protection breaches that classified as High risk to the individual's rights and freedoms:

- Release of recruitment spreadsheet externally containing personal and special category data, financial information, location details and scores. (Reported to ICO)
- External facing website incorrectly configured leading to the exposure of personal, special category and location details contained within an application form. (Reported to ICO)
- Folder containing personal, special category data, location details and access codes of an elderly vulnerable person found at a hospital.
- Officer used personal details of potential new recruits inappropriately.

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.

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 Integrated 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.

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 protected in terms of confidentiality, integrity and availability so that organisation can make data driven decisions as part of its underlying strategy of being evidence led in its approach. 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. Minimum cyber security standards have been published by government and progress is being made against to achieve compliance and where possible exceed what is required. An external audit of information systems, hardware and infrastructure was undertaken, and areas of vulnerability have been addressed. 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. 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.