

Report of the Director of Finance & IT to the meeting of Governance and Audit Committee to be held on 21st September 2023

L

Subject:

Information Governance performance and activity report for the financial year 2022/23

Summary Statement:

The purpose of the report is to present the information governance performance and activity outcomes to provide assurance that the Council's information governance arrangements are effective.

Equality & Diversity:

This report concludes there are no equality and diversity implications which negates the need for an Equality Impact Assessment.

Christopher Kinsella
Director of Finance & IT

Portfolio:
Leader of the Council & Corporate

Report Contact: Tracey Banfield / Harry Singh
Head of Corporate Investigations, Information
Governance and Complaints
Phone: 07582 101209 / 102740
E-mail: tracey.banfield@bradford.gov.uk /
harry.singh@bradford.gov.uk

1. SUMMARY

The purpose of this report is to present the information governance performance and activity outcomes, in the form of the Senior Information Risk Owner (SIRO) report for 2022/23, providing assurance that the Council's information governance arrangements are effective.

2. BACKGROUND

Information is a valuable asset to the Council and managing it well is essential to support both service delivery and efficiency and the Council needs to be confident that all legal obligations are being fulfilled and that expectations around privacy and security of information are being met.

Information Governance is a holistic approach to managing information by implementing processes, roles, controls, and metrics.

3. OTHER CONSIDERATIONS





3.1 The following represents a summary of key information arising from the 2022/23 SIRO report (*shown in full at Appendix 1*); -


1. Over the last 4 financial years the Council has received, on average, **1462** Freedom of Information and **117** Environment Information requests per year. In 2022/23 Planning, Transportation & Highways received the most FOI and EIR requests, as a single service, with 173 and 30 respectively.
2. In 2022/23, the right of access to personal data (*Article 15 UK General Data Protection Regulation (UK GDPR)*) was the most utilised individual right, with **98%** of all the Data Protection requests, received by the Council, being requests for access to personal data. Requests for the Council to rectify data and erase data made up the remaining **2%**.
3. Over the last 4 financial years the Council has received, on average, **381** Subject access requests per year. In 2022/23 the number of requests for access to personal data, received by the Council, was above the yearly average, with the Council receiving **409** in year, an increase of **9%** on the number received the previous year. In 2022/23 Department of Childrens Services received the most requests receiving **44%** of the Council total.
4. Over the last 4 financial years, the Council has recorded, on average, **279** data security incidents per year with **228 (82%)** of those incidents resulting in a personal data breach. In 2022/23 the number of personal data breaches recorded by the Council was above the yearly average with the Council recording **257** personal data breaches in year, an increase of **16%** on the number recorded in the previous year.
5. In 2022/23 the Council has improved compliance in completing the mandatory learning "Information and the UKGDPR" to **82%** of all employees. Whilst this remains below the ICO expectation of 90% there has been an increase of **2%** compared to the previous year.

6. In 2022/23 **25%** of the data security incidents recorded involved employees who had not completed the annual mandatory “Information and the UK GDPR” training. Key actions are being progressed to ensure compliance improves including this information being regularly cascaded to Information Asset Owners and the Data Protection Officer making recommendations, in response to personal data breaches, that all non-compliant employees must complete the training within a 10-working day deadline.

7. A total of **14** complaints relating to the Council’s handling of Data Protection, Freedom of Information and Environment information requests were made to the Information Commissioners Office (ICO), in 2022/23, of which **2** (1 SAR and 1 FOI case) were upheld by the ICO. The SAR case was both complex and voluminous which resulted in Officer re-training and whilst the FOI case was complex this ultimately resulted in an ICO investigation which determined the outcome. The Council duly complied with the recommendations made by the ICO in resolving both matters.

3.2 The table below represents a summary of key performance outcomes, arising from the 2022/23 SIRO report, compared with the previous 3 financial years and also gives an indication of the direction of travel in the first quarter of 2023/24.

	2019/20	2020/21	2021/22	2022/23	2023/24 (Q1)
% of information requests responded to within the statutory timescale					1st April 2023 to 30th June 2023
Freedom of Information / Environment Information	88%	92%	91%	92%	97% 
Data Protection Subject Access	79%	96%	91%	95%	96% 
Data Security Incidents					
High risk personal data breaches reported to the ICO. (As a % of all personal data breaches recorded)	12 (6%)	9 (4%)	7 (3%)	7 (3%)	0 (0%) 
	2019/20	2020/21	2021/22	2022/23	2023/24 (Q1)
% of employees involved in a data security incident who had not completed the annual mandatory training	N/K	N/K	N/K	25%	21% 
Information & UK GDPR Learning					

% of employees who have completed the mandatory learning	N/K	66%	74%	82%	85%	
--	-----	-----	-----	-----	-----	---

3.3 The table below represents the 2022/23 key activity and outcomes compared with two of the Council's neighbouring West Yorkshire Council's.

	No. of FOI/EIR requests received	% responded to within statutory timeframe	No. of Complaints to ICO in relation for FOI/EIR	No. of SARs received	% responded to within statutory timeframe	No. of Complaints to ICO in relation for SAR	No. of Data Security Incidents recorded	No. of Data Security Incidents reported to the ICO
Bradford	1520	92%	7	409	95%	6	345	7
Council A	1155	99%	0	414	80%	3	342	1
Council B	1122	94%	2	208	92%	1	79	2

4. FINANCIAL & RESOURCE APPRAISAL

Compliance with Information Governance / UK GDPR legislation, including the provision of effective, complete, and accurate responses to information requests is governed through the Information Commissioner's Office (ICO).

The ICO is a non-departmental public body which reports directly to the United Kingdom Parliament and is sponsored by the Department for Science Innovation and Technology. It is the independent regulatory office dealing with the Data Protection Act 2018 and the UK General Data Protection Regulation, the Privacy and Electronic Communications Regulations 2003 across the UK; and the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

The ICO has the power to impose monetary penalties on organisations for non-compliance with the legislation and also to prosecute individuals for serious breaches of the legislation. Monetary penalties for Organisations can be up to a maximum of £17.5 million or 4% of turnover, whichever is the greater.

In the financial year 2022/23, the ICO took action against 74 organisations, including 6 Councils, who were issued with 5 reprimands and 1 enforcement notice as follows:-

- LB of Lewisham issued with an enforcement notice for overdue FOI requests.
- LB of Lambeth issued with a reprimand for only responding to 74% of SARs within the statutory timeframe.

- LB of Hackney issued with a reprimand for only responding to 60% of SARs within the statutory timeframe – the oldest being over 23 months old.
- LB of Croydon issued with a reprimand for responding to less than 50% of SARs within the statutory timeframe.
- North Yorkshire County Council issued with a reprimand for failing to complete a print to post process resulting in two envelopes containing multiple letters being sent to two different recipients.
- Wakefield Council issued with a reprimand as they sent papers in relation to Child Protection Legal proceedings (intended for the Court) to the parents of the child in question.

The risks to the Council of non-compliance with the legislation and consequential fines from the ICO would have a significant impact not only financially but also upon the reputation of the Council.

5. RISK MANAGEMENT AND GOVERNANCE ISSUES

Information Governance has a set of specific risks included on the Departmental Risk Register and these are regularly reviewed at the Information Assurance Group.

The Councils CMT receive regular updates on the status of information governance related issues and monitor key performance data monthly.

6. LEGAL APPRAISAL

Data Protection

The Data Protection Act 2018 (DPA) and the UK GDPR sets out the framework for data protection law in the UK.

Rights of a Data Subject under DPA

Section 45 DPA - data subject's right of access. A data subject is entitled to confirmation as to whether their personal data is being processed by the Council as a data controller and where this is the case they can ask for copies of the personal data. The data should be provided within 1 month.

Personal Data Breaches

Section 67 DPA - If the Council as a data controller becomes aware of a personal data breach in relation to personal data, for which the Council is responsible, which is likely to result in a risk to the rights and freedoms of individuals the Council must notify the breach to the Information Commissioner no later than 72 hours after becoming aware of it.

Section 68 DPA - Where a potential data breach is likely to result in a high risk to the rights and freedoms of individuals the Council as data controller must inform the data subject of the breach without undue delay.

Freedom of Information Act 2000

Section 1 (1) Freedom of Information Act 2000 - Any person making a request for information to a public authority is entitled :-

(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, **and**

(b) if that is the case, to have that information communicated to them.

The information must be provided within 20 working days of receipt of the request unless exceptionally an exemption under the Freedom of Information Act applies.

Environmental Information Regulations 2004

The Environmental Information Regulations 2004 provide public access to environmental information held by public authorities. Environmental information includes the state of the elements of the environment, such as air and atmosphere, water, soil, land, landscape and natural sites including wetlands, coastal and marine areas, biological diversity and its components, including genetically modified organisms, and the interaction among these elements.

Environmental information must be provided within 20 working days.

The Environmental Information Regulations contain exceptions that allow you to refuse to provide certain requested information.

7. OTHER IMPLICATIONS

7.1 SUSTAINABILITY IMPLICATIONS

None.

7.2 TACKLING THE CLIMATE EMERGENCY IMPLICATIONS

None.

7.3 COMMUNITY SAFETY IMPLICATIONS

None.

7.4 HUMAN RIGHTS ACT

None.

7.5 TRADE UNION

None.

7.6 WARD IMPLICATIONS

None.

**7.7 AREA COMMITTEE ACTION PLAN IMPLICATIONS
(for reports to Area Committees only)**

N/A

7.8 IMPLICATIONS FOR CORPORATE PARENTING

N/A

7.9 ISSUES ARISING FROM PRIVACY IMPACT ASSESSMENT

None

8. NOT FOR PUBLICATION DOCUMENTS

None

9. OPTIONS

N/A.

10. RECOMMENDATIONS

That the Committee notes the performance and activity information contained within this report.

11. APPENDICES

Appendix 1 – Senior Information Risk Owner (SIRO) Report 2022/23

12. BACKGROUND DOCUMENTS

None.

Appendix 1

Annual Report of the Senior Information Risk Owner (SIRO) 2022/2023

1.0 Introduction

This annual report, provided by the City of Bradford Metropolitan District Council's Senior Information Risk Owner (SIRO), outlines the activity and performance related to information governance and provides assurance that all information related matters across the Council are being effectively managed.

The report reflects on the work undertaken during **the financial year ending 31st March 2023** and highlights the progress made; where improvements are required to ensure compliance with the legislation and details the plans in place to minimise risk and improve performance.

The Council continues to be committed to effective information governance and the governance arrangements are closely monitored to ensure systems, policies and procedures are fit for purpose; and that all Council staff and elected members understand the importance of information security and that this is embedded as part of the Council's culture.

2.0 Key Roles and Responsibilities

Appendix A represents the Information Management, Assurance and Governance strategic framework in operation, across the Council.

The **Corporate Management Team** (CMT) has overall accountability for all information governance related matters Council wide.

The **Senior Information Risk Officer** (SIRO) is accountable for the oversight and prioritisation of Information Governance activities Council wide; responsible for advising the Chief Executives Management Team (CMT) about information risk; providing direction and guidance to Information Asset Owners to ensure they understand their responsibilities.

The Director of Finance & IT holds the position of SIRO.

The **Information Asset Owner** (IAO) is accountable to the SIRO and will provide the necessary support to ensure full visibility of information asset management across the Council. The IAO role is to understand what information is held, added and/or removed; how information is moved; who has access and why. The IAO is also responsible for ensuring Data Protection impact assessments are completed in advance of any new systems or processing.

IAO's must be able to understand and address risks to the information, ensure that information is fully used within the law, for the public good, and provide written input to the SIRO, annually, on the security and use of their asset.

The Directors and Assistant Directors (3rd tier officers) hold the position of IAO and are each responsible for their own Service.

The **Data Protection Officer** (DPO) is responsible for monitoring the Council's internal compliance with the UK General Data Protection Regulation (UK GDPR), other data protection legislation and

data protection policies in addition to informing and advising the Council on data protection obligations. All Local Authorities are required to have a DPO.

The DPO sits within the Information Governance area of Finance, IT and Procurement.

The **Records Management Officer** (RMO) is responsible for the effective and appropriate management of the Council's information developing and supporting a culture of high quality records management practice across the Council and ensuring compliance with the requirements of the Public Records Act, the Freedom of Information Act and the Data Protection Act

The RMO sits within the Information Governance area of Finance, IT and Procurement.

The **Caldicott Guardian** (CG) is the senior person responsible for protecting the confidentiality of health and care information and making sure that it is used properly. All Local Authorities are required to have a CG.

The Assistant Director (Operational Services) within the Department of Health and Well Being holds the position of CG.

The **Corporate Information Governance** (CIG) team are responsible for ensuring that the Council's individual Service areas comply with the requirements of all information legislation by co-ordinating all information governance activities centrally and providing expert advice and guidance to ensure the Council can fulfil statutory obligations.

The team are located within the Finance, IT & Procurement Service reporting to the Director of Finance & IT, thereby providing direct management responsibility and accountability to the SIRO.

The **Information Governance Champions Network** (IGCN) is made up of Information Governance Champions from each Service who support and assist the service Information Asset Owners to fulfil their obligations in relation to information.

Information Governance Support Officers are in each Service and support and assist the Information Governance Champion.

IT Services provide a key role in providing advice and assurance on all technical aspects of information security.

Legal Services provide a key role in advising on all legal aspects of information related matters.

3.0 Governance and Monitoring Arrangements

The Council's **Information Assurance Group** (IAG) is responsible for assisting the SIRO to maintain oversight and prioritise all information activities for the Council.

The IAG is a strategic group made up of the SIRO, 3rd tier Information Asset Owners (1 from each of the Council's 5 Departments) and is supported by the Heads of Information Governance and IT Services, the Data Protection Officer, the Information Governance Manager and a senior lawyer with experience of information related matters.

The IAG meet on a regular basis and members of the group adopt a strategic role in promoting and embedding effective information governance. They are the champions for information governance in their respective Departments and cascade key messages to develop a culture that values, protects and uses information to deliver improved services.

4.0 Information Access

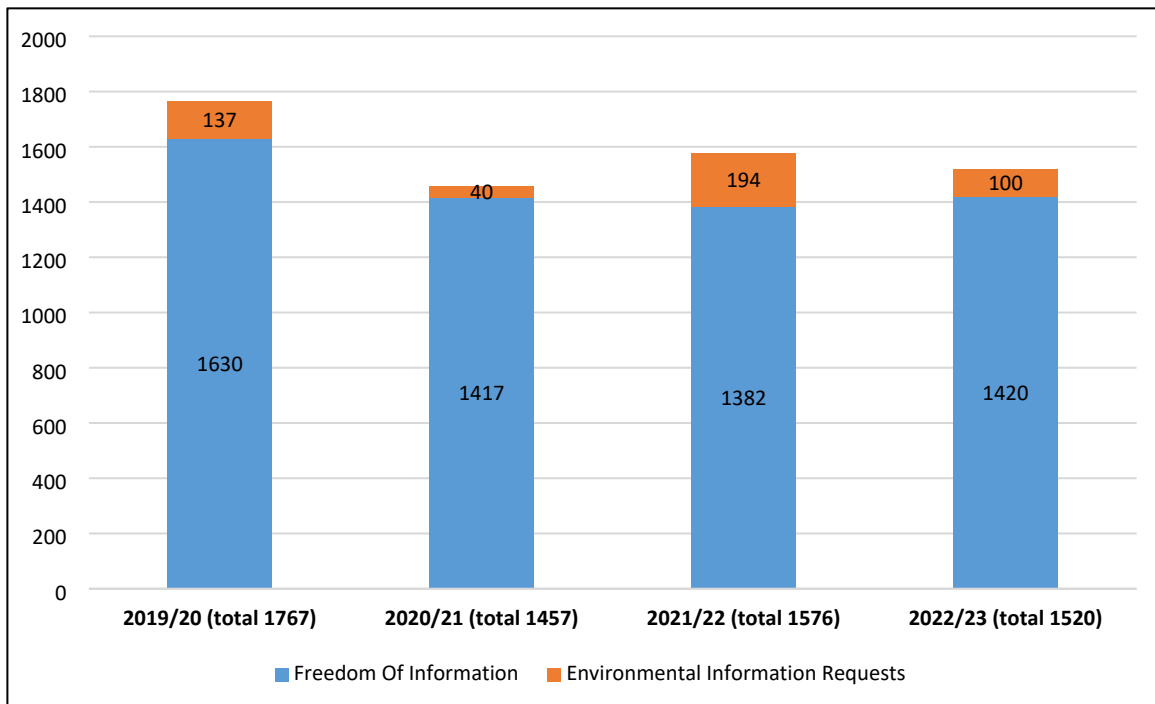
4.1 Freedom of Information / Environment Information

In accordance with the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 the Council is obliged to; -

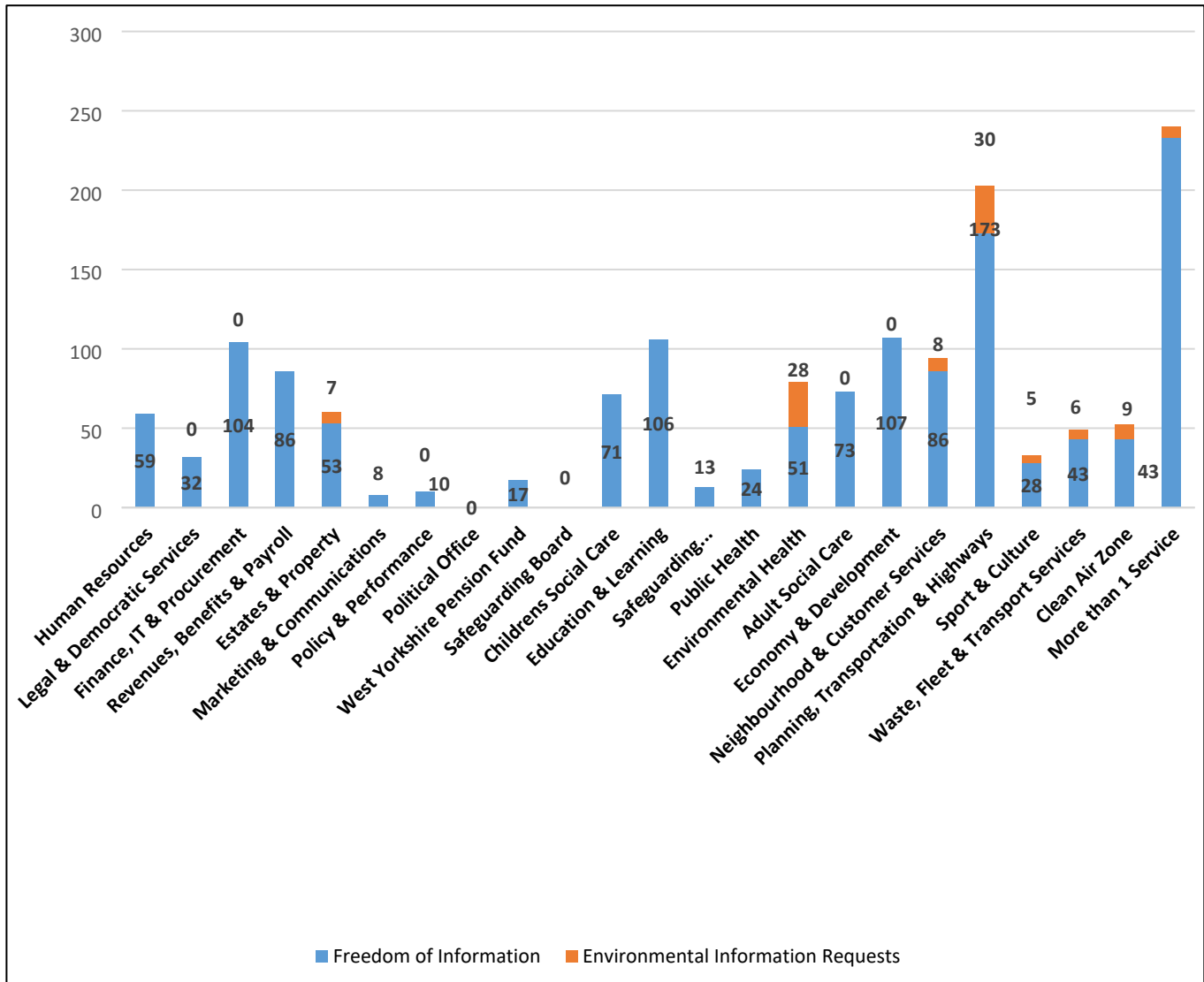
- a. provide information requested by members of the public and
- b. to publish information proactively

4.1.1 Provision of the information requested

Graph 1 below demonstrates the **number of Freedom of Information and Environment Information requests received** in the last 4 financial years.



Graph 2 below demonstrates the **number of FOI and EIR requests received in 2022/23** broken down by Council Service



4.1.2 Exemptions

The Freedom of Information (FOI) Act contains exemptions, and the Environmental Information Regulations (EIR) contains exceptions that allow the Council to withhold specific information.

Under the legislation exemptions and exceptions prevent the right of access to information and fall into two categories:

1. Absolute - the requested information does not need to be disclosed under any circumstances.

2. Qualified - this category of exemption is subject to a public interest test and the Council must consider whether the balance of public interest is weighted in favour of disclosure or not. Some qualified exemptions may also be subject to a prejudice test, to consider whether harm will, or is likely to be caused, if the information is released.

When the Council wishes to rely on an exemption or an exception, the applicant must be issued with a "Refusal Notice" within the relevant statutory timescale of 20 working days.

Table 1 below demonstrates the number of exemptions and exceptions the Council applied during the financial year 2022/23.

Exemptions (FOI)	414
Exceptions (EIR)	24
GRAND TOTAL	438

Table 2 below demonstrates the number of instances in 2022/23 where the Council has not provided the information requested in accordance with the Freedom of Information Act and details the type and number of specific exemptions and exceptions applied broken down into absolute and qualified.

Exemption - FOI	Times Applied	Type of Exemption
Section 1(1)(a) – Information not held by the Council	145	N/A
Section 12 – Appropriate cost limit	33	Absolute
Section 21 - Reasonably Accessible by other means	117	Absolute
Section 22 - Future Publication	10	Qualified
Section 29 – Economic Interests	6	Qualified
Section 30 - Investigations and proceedings	1	Qualified
Section 31 - Law Enforcement	35	Qualified
Section 38 – Health & Safety	2	Qualified
Section 40 - Personal Information	40	Absolute
Section 41 - Confidentiality	4	Absolute
Section 42 – Legal Professional Privilege	1	Qualified
Section 43 - Commercially Sensitive	20	Qualified
TOTAL	414	
Exception- EIR	Times Applied	Type of Exemption
Regulation 6(1)(b) - Information publicly available	9	Qualified
Regulation 12(4)(a) - Information not held	8	Absolute
Regulation 12(4)(b) - The request is manifestly unreasonable	1	Qualified
Regulation 12(4)(d) - Request relates to unfinished documents	2	Qualified
Regulation 12(4)(e) - The request concerns internal communications	2	Qualified
Regulation 12(5)(b) - Course of justice	1	Qualified
Regulation 13 – Personal Data	1	Qualified
TOTAL	24	

4.1.3 Charges

The Council, in accordance with the legislation, can only apply a charge for photocopying and postage, commonly referred to as a disbursement.

The Council did not apply any disbursement charges during 2022/23.

Where the Council estimates that a Freedom of Information Act request will incur unreasonable cost then a “refusal notice” under Section 12 of the Act can be issued.

The threshold, set by the Act, is 18 hours (equivalent to £450 at a notional hourly rate of £25).

On deciding whether to apply a Section 12 exemption and whether the request would exceed the threshold set, the Corporate Information Governance Team works with the relevant service area to estimate and evidence the expected time taken to: -

- Determine whether the requested information is held.
- Locate the information or appropriate documents.
- Retrieve the information or document containing it.
- Extract the information and process the request.

The Council issued 33 Section 12 refusal notices during 2022/23, on the grounds that it estimated that unreasonable cost would be incurred.

4.1.4 Responses

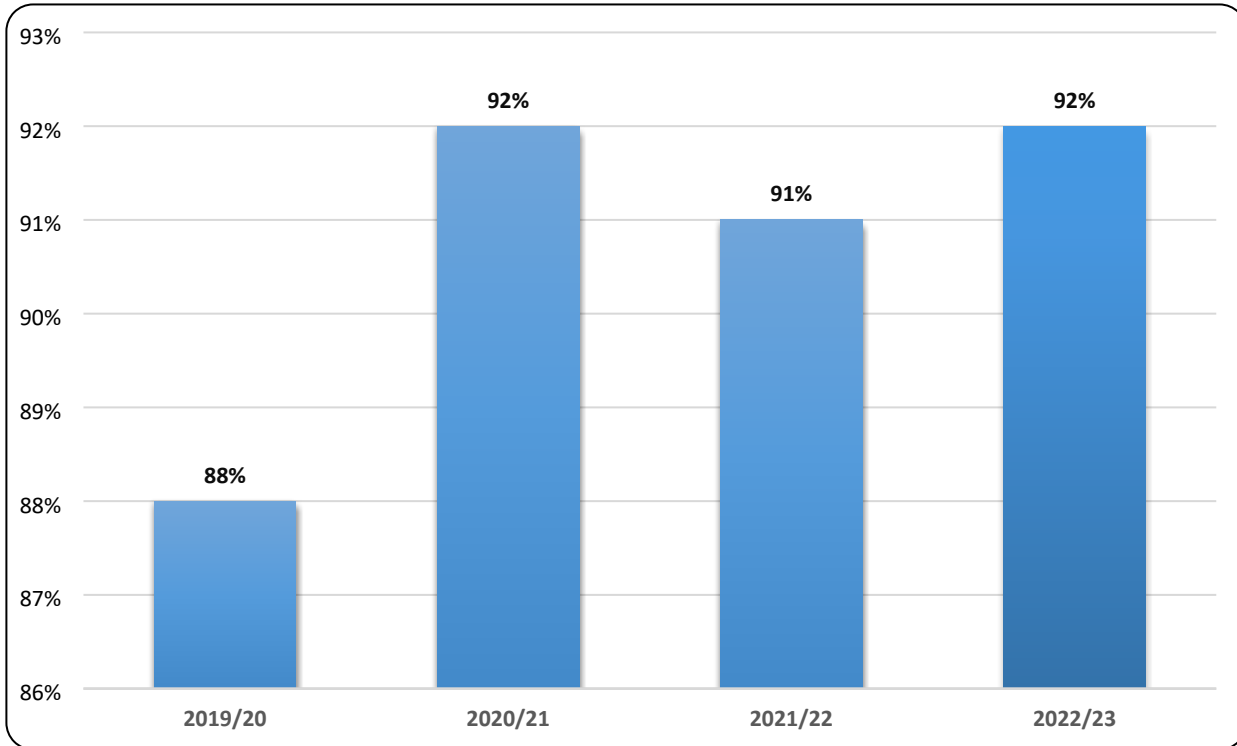
Requests for information under the Freedom of Information or Environmental Information legislation must be responded to within a statutory timescale of **20 working days**.

Whilst there is provision, under the legislation, for the Council to extend or vary this time limit to consider the public interest test or where, under the Environmental Information Regulations, there is a lot of complex information which makes it more difficult to respond, any extension is only granted in exceptional circumstances and decisions are always taken in conjunction with the Corporate Information Governance team.

Table 3 below demonstrates the number of occasions when the Council extended the time limit predominantly due to the complexity of the requests.

	TOTAL
Freedom of Information	27
Environment Information	3
GRAND TOTAL	30

Graph 3 below demonstrates the % of Freedom of Information / Environment Information requests responded to within the legislative timescale over the last 4 financial years.



4.1.5 Internal Reviews

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

Table 4 below demonstrates the **number of internal reviews processed** by the Council over the last 4 financial years (*and as a % of all requests completed*)

	2019/20	2020/21	2021/22	2022/23
Freedom of Information	51	42	59	73
Environmental Information	2	0	5	6
Grand Total	53 (3%)	42 (3%)	64 (4%)	79 (5%)

4.1.6 Complaints to the Information Commissioner's Office (ICO)

The ICO is the UK's independent body set up to withhold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. One of the roles of the Information Commissioner is to investigate complaints about the way public bodies have handled personal data and requests for information.

Complaints are normally received by the ICO following the outcome of an internal review. The ICO will assess the complaint and make an independent decision about the way the Council has handled the request. The ICO can issue a decision notice in favour of the Council or the complainant, make recommendations on best practice and in some cases, take enforcement action. All ICO decision notices are made public.

Table 5 below demonstrates the number of FOI/EIR complaints made to the Information Commissioner; the number of cases where the ICO upheld the complaint and the % uphold rate over the last 4 years.

	2019/20	2020/21	2021/22	2022/23
No. of FOI complaints made to ICO	13	3	3	7
No. of EIR complaints made to ICO	Included in above	Included in above	1	1
TOTAL NUMBER OF COMPLAINTS MADE TO ICO	13	3	4	8
No. of FOI complaints upheld by the ICO (% uphold rate)	7 (54%)	1 (33%)	0 (0%)	1 (13%)
No. of EIR complaints upheld by the ICO (% uphold rate)	Included in above	Included in above	0 (0%)	0 (0%)
TOTAL NUMBER OF COMPLAINTS UPHELD BY THE ICO (% UPHOLD RATE)	7 (54%)	1 (33%)	0 (0%)	1 (13%)

4.1.7 Publishing information proactively

The FOI Act requires every public authority to have a publication scheme approved by the ICO and to publish information covered by the scheme. The Council has adopted the ICO's model publication scheme, and this is made available on the Council's website.

<https://www.bradford.gov.uk/open-data/publication-scheme/publication-scheme/>

4.2 Subject Access Requests (SAR)

In accordance with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 an individual has a right to access and receive a copy of their personal data, and other supplementary information, verbally or in writing. This is called "the right of access" and is more commonly referred to as making a subject access request or SAR. A 3rd party can also make a SAR on behalf of another person, but the Council must take steps to identify the person making the request.

4.2.1 Provision of the information requested

Graph 4 below demonstrates the **number of subject access requests received** over the last 4 financial years.

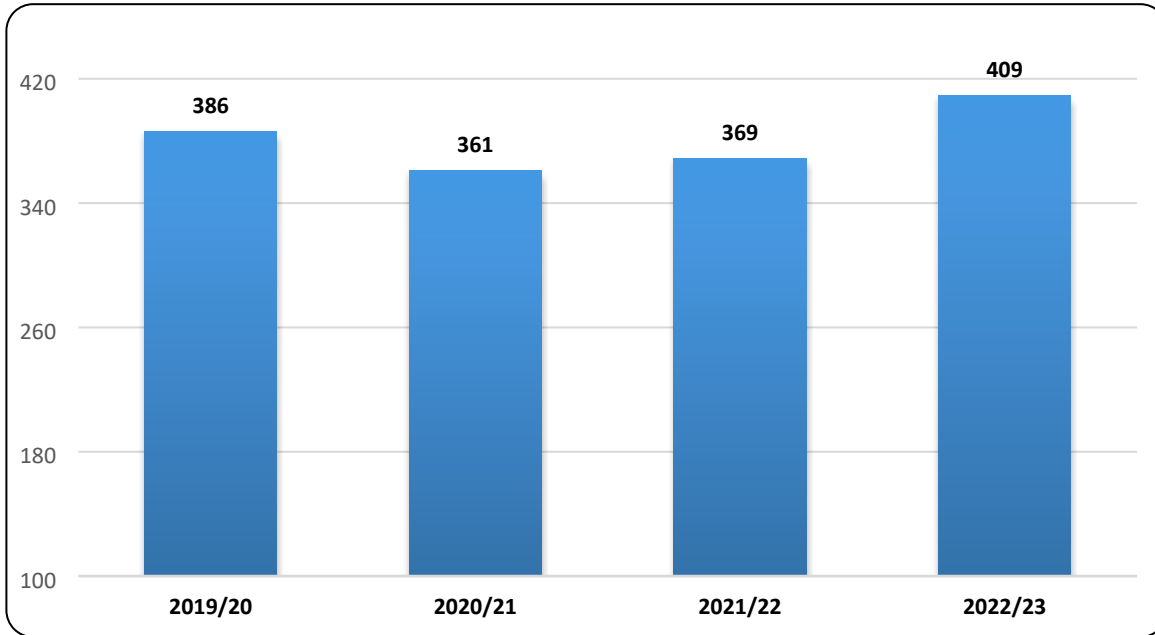
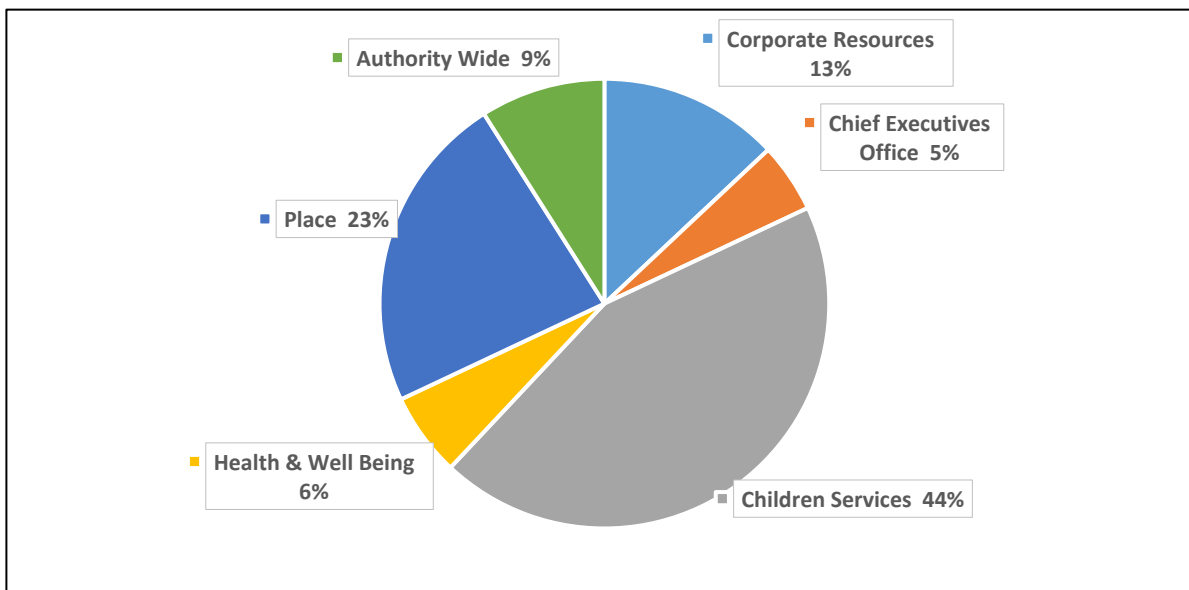


Chart 1 below demonstrates the **% breakdown of SAR's received** by Council Department in 2022/23



4.2.2 Data Protection Act Exemptions

Whilst several exemptions are available to the Council, for example, crime, law and public protection, health, social work and education data, the Council does not routinely rely upon or apply such exemptions in a blanket fashion and will always consider each exemption on a case-by-case basis.

Competent authorities such as the Police, HMRC, DWP and other Local Authorities or Public Bodies acting under regulatory powers can request the release of personal information held by CBMDC for specified purposes. The Council have considered disclosure with reliance upon Schedule 2, Part 1 of the Data Protection Act for **580** requests during 2022/23.

4.2.3 Charges

The Council, in accordance with the legislation, does not charge a fee to deal with Subject Access requests.

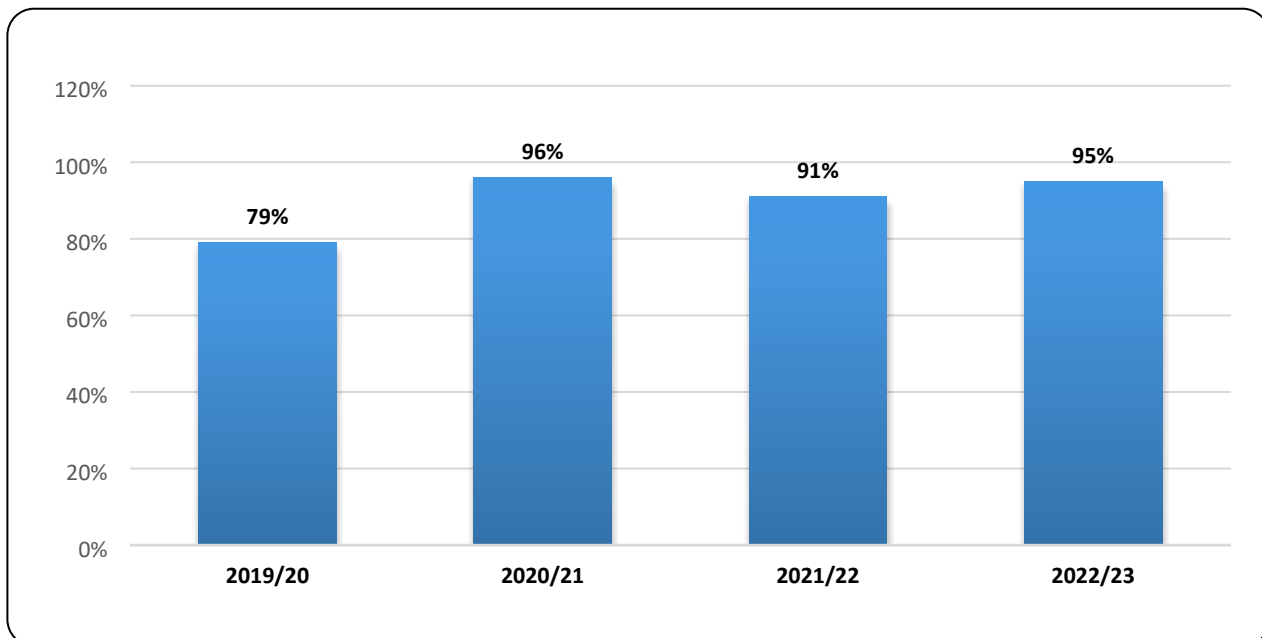
4.2.4 Responses

Subject access requests (SAR) must be responded to within a statutory timescale of **one month** following receipt of the request.

Whilst there is provision, under the legislation, for the Council to extend the time limit by **a further two months**, this extension only applies to complex requests or if several requests have been received from the same individual. Decisions on extension are always taken in conjunction with the Corporate Information Governance team.

In 2022/23 the Council extended the time limit in **133** of the requests (*33% of all requests received*). This has been predominantly in complex Childrens Services cases going back over several years and needing a significant amount of review and redaction of data to comply with the UK GDPR legislation.

Graph 5 below shows the % of subject access requests responded to within the statutory timescale over the last 4 years.



4.2.5 Internal Reviews

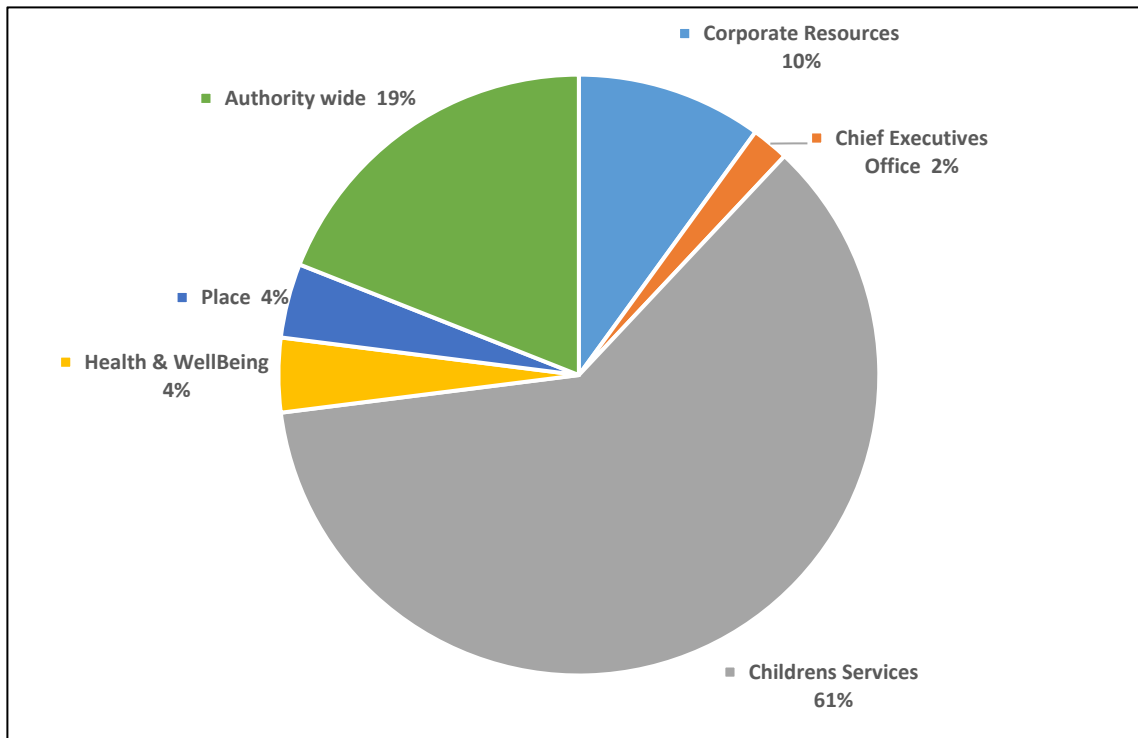
Requesters who submit a SAR can request an internal review if they are not satisfied with the response provided.

Internal reviews provide the Council with an opportunity to review the request handling process prior to any potential complaint to the ICO by the requester.

Table 6 below demonstrates the number of internal reviews processed by the Council in the last 4 financial years and as a % of all requests responded to

	2019/20	2020/21	2021/22	2022/23
Internal SAR Reviews (as a % of all SAR's received)	16 (4%)	24 (7%)	35 (9%)	51 (12%)

Chart 2 below demonstrates the **number of SAR reviews as a % of SARs received** broken down by Council Department



4.2.6 Complaints to the Information Commissioner's Office (ICO)

In appropriate cases, the ICO may ask the Council to take follow up action and can in some cases take specific action against the Council if they fail to comply with the Data Protection legislation. This could be in the form of an official warning, reprimand, enforcement notice or penalty notice.

The Council was not issued any of the above, by the ICO, during 2022/23.

Table 7 below demonstrates the **number of SAR complaints made to the Information Commissioner** and the **number upheld** over the last 4 years.

	2019/20	2020/21	2021/22	2022/23
No. of SAR complaints investigated by the ICO	6	6	7	6
No. of complaints upheld by the ICO (% uphold rate)	2 (33%)	1(17%)	0 (0%)	1 (17%)

5.0 Data Protection (DP) Act 2018 & UK General Data Protection Regulation (GDPR)

Data Protection is the fair and proper use of information about people. As the Council holds information about people to carry out its business (known as a “controller”) then the legislation applies to the collecting, recording, storing, using, analysing, combining, disclosing, or deleting (known as “processing”) of this personal data.

The Data Protection Act 2018 sets out the data protection framework for the UK alongside the UK General Data Protection Regulation (UK GDPR).

5.1 Individual rights under the UK GDPR

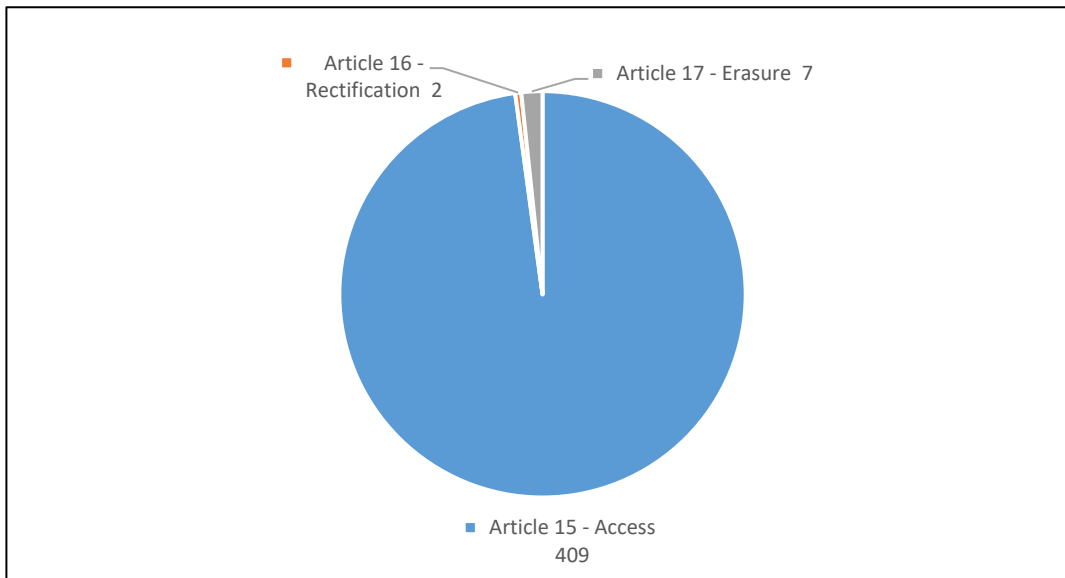
The UK GDPR grants a data subject certain rights regarding their personal data including the right:

- To access their personal data (UK GDPR Article 15).
- To rectify their personal data (UK GDPR Article 16).
- To erase their personal data (UK GDPR Article 17).
- To restrict personal data processing about them (UK GDPR Article 18).
- To receive a copy of certain personal data or transfer that personal data to another data controller, also known as the data portability right, (UK GDPR Article 20).
- To object to personal data processing (UK GDPR Article 21).
- Not be subject to automated decision-making in certain circumstances (UK GDPR Article 22).

The Council has a policy to address procedures for handling data subject requests and objections under the UK General Data Protection Regulation (UK GDPR).

*In 2022/23 the Council received **418** requests from data subjects regarding their personal data*

Chart 3 below demonstrates a breakdown of the requests



5.2 Data Protection Impact Assessment (DPIA)

Conducting a DPIA is a legal requirement and a key part of the Council's accountability obligations under UK GDPR. The process is designed to help a data controller to systematically analyse, identify and minimise the data protection risks of a project or plan, and helps ensure that they are processing data in line with the UK GDPR principles. Whilst it does not have to eradicate all risk it should help minimise and determine whether the level of risk is acceptable considering the benefits of what the Council wants to achieve.

The Council has a DPIA "Screening" questionnaire which assists data controllers to decide whether a full DPIA is required and if it is then a DPIA specific template is completed to enable risks and mitigating actions to be captured. If a DPIA is considered to contain any potentially high risks, it is reviewed by the Council's Data Protection Officer.

In 2022/23 **23** DPIA Screening questionnaires and **56** DPIA's were completed.

5.3 Data Sharing

Agreements are required between all parties with whom the Council routinely shares personal data. These agreements should include details about the parties' role, the purpose of data sharing, data security, what is going to happen to the data at each stage and the standards set (with a high privacy default for children). Regular review processes are required to ensure that the information remains accurate and to examine how the agreement is working.

In 2022/23 the Data Protection Officer reviewed **28** data sharing agreements.

All approved Data Sharing Agreements (DSA) / Information Sharing Agreements (ISA) are uploaded to the Corporate Information Governance SharePoint Site where automated review triggers are enabled to ensure that DSAs and ISAs are reviewed and refreshed annually.

5.4 Records Management

Effective records management supports effective data governance and data protection and is a necessary requirement to ensure that the Council meets the information obligations in full.

The Council has a Records Management Policy and Records Retention and Disposal Policy which reflects the Council's commitment to ensuring Council records are managed, used for the purpose they were created and then securely destroyed in a timely manner.

To ensure transparency these policies are available to all employees via Bradnet and the Corporate Information Governance SharePoint site and for anyone else on the Records Management page of the Council's external website.

5.4.1 Information Asset Register (Record of Processing Activity)

The Council is required to hold a register which details all information assets (software and hardware); asset owners; the assets location; the retention periods; data sharing agreements and any security measures deployed. The register must be reviewed periodically to make sure it remains up to date and accurate and assets within the register must be periodically risk assessed with physical checks.

A full suite of Council Information Asset Registers is now held on the Corporate Information Governance SharePoint site where they are monitored and reviewed on an annual basis.

5.4.2 Retention Schedule

A requirement of the ICO's Accountability Framework is that a retention schedule exists which provides sufficient information to identify all records and to implement disposal decisions. The retention periods for records and documents must be set based on business need with reference to statutory requirements and other principles (e.g., National Archives guidelines).

The Council maintains a full comprehensive retention schedule which lists all record types for Departments and Services across the Council and the related legislation applicable to each individual record. This is available to view on both the Council's internal and external websites. The retention schedule is reviewed and updated on an annual basis.

5.4.3 Email Retention Policy

The Council has an email retention policy to ensure that all archived Council emails are deleted in line with the agreed retention period of 3 years. There are currently a small number of emails which have been held longer than 3 years and they continue to be monitored for relevance.

5.4.4 Privacy Policy

In order to comply with the first principle of UK GDPR, individuals have the right to be informed about the collection and use of their personal data. This information is set out in the Council's Privacy policy which explains, in easy format, why the Council collects and processes personal data.

Additionally, the Council has 65 active privacy notices, which are specific to individual services and are to be read in conjunction with the Council's Privacy policy. These notices give individuals a clear view of what data is being collected and how the Council's services manage it and keep it safe and also who data may be shared with.

Both the Policy and the accompanying notices provide clear detail on how individuals can exercise their rights under UK GDPR and are published on Council's external website and the Corporate Information Governance SharePoint site where automated review triggers are enabled to ensure that the privacy notices remain up to date.

6.0 Information Security

As the importance of digital information and networks grow, information security is of high importance and reducing the risk of cyber-attacks remains a corporate priority. The type of risks posed include theft of sensitive corporate and personal data, theft or damage to data and IT infrastructure, threat of hacking for criminal or fraud purposes and potential disruption to infrastructure such as council ICT systems, intranet, and public facing websites, these can be clearly seen with the number of cyber-attacks, known as Ransomware, that have hit a number of local authorities and public organisations.

The Council is committed to ensuring all personal information it holds is kept secure and the following paragraphs summarise the protocols the Council has in place to maximise information security.

6.1 Acceptable Software Use

The Council has a dedicated policy which is regularly updated and available to staff on the internal website – Bradnet.

6.2 Working outside the UK – Council employees.

To ensure compliance with UK GDPR, for any Council employees intending to temporarily work from outside the UK, Council Managers are required to ensure that employees detail their case for approval before leaving the UK using a dedicated application form. The completed application is reviewed by both IT Security and the Councils DPO and will require a UK and EU GDPR Adequacy Finding being in place for the host country. This ensures that the host country meets the data security standards required in the GDPR. Should a proposed country not have adequate IT Security measures in place, or the country is deemed a risk to UK data and/or the GDPR adequacy finding in place, then whilst the legislation does allow for the development of "Appropriate Safeguards", this will only be used by the Council in exceptional circumstances and most applications where the host country does not have a GDPR adequacy finding will not be approved.

In 2022/23 **77** requests to work abroad were received of which **67** were approved. The **10** which were not approved were because there was no GDPR adequacy finding for the country the employee intended to visit.

6.3 Data encryption

All laptop hard drives are encrypted to ensure the safety of the information, and should a laptop be lost or stolen, the Council have line of sight of the device, and it can be wiped remotely to ensure that all information stored on the device is removed.

All Smartphones / mobile tablet devices, supplied by the Council, have automatic screen locks and a PIN/passphrase to ensure data is protected. A mobile device management (MDM) is utilised so that devices are managed corporately, and only approved APPs can be installed. Additionally, if a device is

lost or stolen a “kill switch” can be activated so that all the data on the device is wiped. In addition, an MDM solution for new devices is currently being rolled out and this provides greater functionality and security.

6.4 Patching

Critical security patches protect the Council’s network from recently discovered threats. Windows operating systems are typically updated at least monthly, and the server estate (Production Servers) are “patched” on the last Sunday of every month to make sure that these systems have the latest patches and hackers are unable to exploit these vulnerabilities. Where emergency patches are released, these are quickly reviewed and implemented, often within hours of being provided.

A Security IT Review Panel meets weekly to review all patches and security requirements. The Panel will meet more regularly if there are critical or emergency patches that need to be implemented following communication from the National Cyber Security Centre (NCSC) and/or the Yorkshire and Humberside Warning, Alerts and Reporting Point (YHWARP).

6.5 Firewalls & IDS / IPS

Firewalls assist in blocking dangerous programs, viruses or spyware before they infiltrate the network, and the Council has a number of perimeter firewalls managed all day every day to make sure that any unusual activity is identified. Threats prevention are continually being added automatically to maintain current threat protection.

The Council also utilises some IDS & IPS intrusion devices, these devices while automatically dealing with known threats or suspicious activities are also managed and monitored 24/7 by a 3rd party security supplier., There are plans to strength this element with the creation of a regional Security Operational Centre (SOC) comprising of several Councils. Details are currently being worked up between Councils but most importantly it will involve sharing of information to ensure everyone is prepared should Councils come under attack.

6.6 Multi Factor Authentication

The Council has introduced Microsoft Multi Factor authentication across the whole estate. This secures the environment and dramatically reduces the risk of unauthorised access to Council accounts from outside the Councils network and ensures that access is confined to the UK.

6.7 Cyber security incident

Key improvements to improve security and the threat of incidents were identified and have been implemented in this financial year as follows.

- Seeking a Managed Security Service Provider (MSSP), to work in partnership with the Council, to protect the Council’s hybrid ICT environment from information and cyber security threats and incidents.
- Continual assessment of solutions to further protect the Council, through the solutions architect team.
- New Partner Organisation Access policy and Process to streamline access for Partners that need access to council application and data e.g., NHS, police other Council’s.
- Implemented a full DDoS (Distributed Denial of Service) Attack which now covers all websites and services that are hosted within the Council’s data centre.

- Closer working with the National Cyber Security Centre (NCSC). The Council uses the following alerting services; - Protective DNS, Early Warning, Mail Check and Web Check.
- Active participation and collaboration with the Yorkshire and Humber Warning Alerts and Response Point (YHWARP) and other WARP colleagues.
 - A Council IT Service Manager chairs the YHWARP, which allows the Council to receive early warning of any potential attacks or vulnerabilities across the UK.
 - The YHWARP arranges regular Cyber Attack simulation exercises to help members understand the potential risk and what measures should be put in place, not only help to protect against an attack, but also how to deal with an attack.
 - As members of the North, South, West Yorkshire and Humberside LRF (Local Resilience Forum) the Council can immobilise any responses during a cyber-attack and to develop strategies, communications, and protocols.
- Currently developing a CyberApp.
- Storage Infrastructure Environment e.g., Backup snapshot (*specifically protects against malware restoration*)
- Core firewalls, to protect against hackers accessing the Council network will be implemented soon.
- Collaborative working between IT Services and the Corporate Information Governance team to ensure that the necessary security measures arising from Data Protection Impact Assessments are implemented.
- The implementation of a Vulnerability Management solution which helps identify and track any outstanding system vulnerabilities.
- Implementing a security software to safeguard the council from internal threats.
- Currently rolling out a software to protect us from ransomware attacks, that help disable the user account and shut down the infected devices within a few seconds to minimize the risk to council data.
- Purchase of a Cyber Security Training Platform
- Roll out of vulnerability software to end points to help identify devices that are vulnerable to attacks and remediate.
- All devices now either running Windows 10 21H2 or 22H2 which is supported until October 2025, plans already in place to roll out Windows 11

6.8 Data Security Incident Reporting (Personal Data Breaches)

The UK GDPR introduced a duty on all organisations to keep a record of any data security incidents resulting in a personal data breach; to report certain personal data breaches to the Information Commissioners Office within 72 hours of becoming aware and to have in place robust breach detection, investigation and internal reporting procedures.

The Council has a policy which applies to all Council information, in both paper and electronic format, and is applicable to all employees, members, visitors, contractors, partner organisations and data processors acting on behalf of the Council.

The policy standardises the Council's response to any personal data breach and sets out how the Council will manage reports of suspected data security incidents ensuring that all data security incidents are; -

- Reported swiftly so that they can be properly investigated.
- Appropriately logged and documented.

- Dealt with in a timely manner and normal operations restored.
- Risk assessed to ensure that the impact of the incident is understood, and action taken to prevent further damage.
- Appropriately reported to the ICO, affected data subjects informed or any other appropriate supervisory authority (as is required in more serious cases)
- Reviewed, and lessons learned.
- Managed in accordance with the law and best practice.

Graph 6 below demonstrates, for the last 4 financial years, the **number of data security incidents**; the **number of incidents where personal data was breached** and the **number of personal data breaches reported to the ICO**.

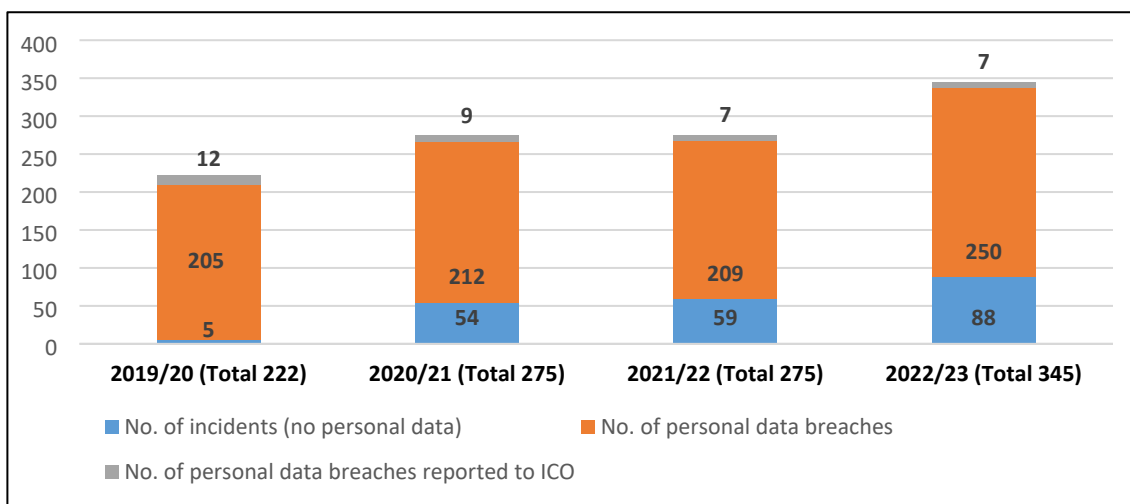
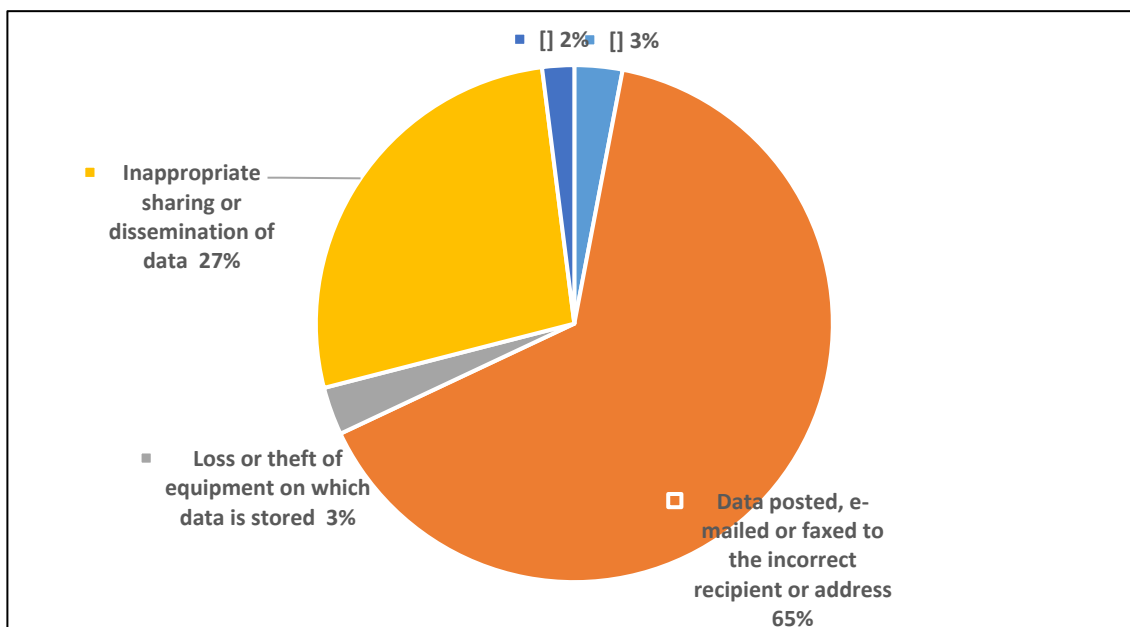


Chart 4 below shows a breakdown of the reasons for the personal data breaches recorded in 2022/23.



6.8.1 “High Risk” Personal Data Breaches

Where a personal data breach is likely to result in a high risk of adversely affecting an individuals’ rights and freedoms, the Council’s Data Protection Officer must report this to the Information Commissioners Office immediately. In 2022/23 7 such reports were made.

In response to the 7 reports, the ICO concluded that all 7 were low risk and did not require any formal intervention but the ICO made recommendations about the Council’s monitoring of procedures and policy. In summary, the ICO request that the Council understand how and why each breach occurred, and what steps are needed to take to prevent it from happening again. The following actions were taken as a result of the ICO recommendations:

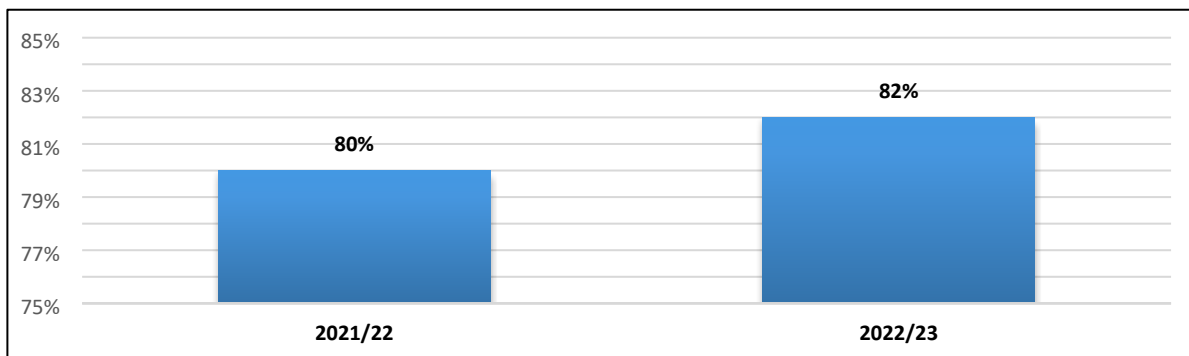
- Regularly reviewing our processes and procedures to ensure they are robust
- Ensuring that all members of staff have received appropriate data protection training
- Review of internal security procedures to identify if any additional preventative measures can be implemented to reduce the risk of a recurrence of incidents
- Ensuring robust technical measures and controls in place
- Routinely testing the effectiveness of the measures we have in place, including spot-checking staff adherence to these measures
- Issue reminders to Information Governance Champions of correct procedures on a regular basis to help ensure best practice within the organisation
- Maintaining awareness of data protection amongst staff via Bradnet

6.9 Protecting Information Training

The Council has a bespoke mandatory annual eLearning package “Information and the UK GDPR” intended for all employees who have access to a PC. Elected Members have a similar eLearning package which is bespoke to their individual role as Council member.

Those employees without access to a PC are required to read a Council developed leaflet on how to protect information whilst carrying out their role for the Council.

Graph 7 below demonstrates the % of Council employees, Elected Members and casual employees who have completed the learning (PC Users only) in the last 2 financial years.



In 2022/23 the Council commenced recording the number of data security incidents which occurred but could have been avoided had the employee been compliant with the mandatory learning (i.e. completed it within the last 12 months prior to the incident).

Table 8 below shows the **number and % of “potentially avoidable” data security incidents involving employees** who had not completed the mandatory learning in 2022/23.

	2022/23
No. of “potentially avoidable” data security incidents recorded <i>i.e., those where the employee involved had not completed the annual mandatory learning</i>	86
No. of “potentially avoidable” data security incidents as a % of all recorded incidents	25%

7.0 Progress against key improvement actions

1. Refresh of the paper based GDPR Protecting Information learning for non PC users to improve overall compliance with mandatory training	Completed and shared with Managers across areas where non PC users are deployed
2. Reviewing the content of all external and internal websites to ensure up to date information is available for employees and Service users	All external websites have been reviewed and updated.
3. Ensuring all Information Governance Champions across the authority have access to specialist advice, support, guidance, and training material	Access to a dedicated area on SharePoint to Council Officers working on Information Governance matters
4. Reviewing all Information Governance policies and procedures	All policies and procedures reviewed and refreshed
5. Continued support of the International Digital Clean Up Day by promoting ‘Digital Diet Week’ across the authority in March 2023	Advice and support to services across the authority in relation to records management and retention schedules
6. Ensuring a smooth transition to the Bradford Children and Families Trust in relation to requests for information	Agreed protocols between the Council and the BCFT in relation to requests for information that affect both organisations

8.0 Conclusion

In summary, this report has demonstrated the progress made during 2022/23 in implementing key actions to strengthen and ensure the Council has a robust approach to the management, assurance and governance of information and this progress will continue to ensure the Council continues to meet its legal obligations.

9.0 Key improvement actions for 2023/24

<p>1. Maintain performance of request responses</p> <ul style="list-style-type: none"> - Ensure that the timescales for responding to requests for information are comparable to neighbouring Councils whilst developing the Council's ambition to improve the quality of responses. - Benchmark performance with other comparable Council's and identify any learning
<p>2. Quality Assurance Process</p> <ul style="list-style-type: none"> - Implementation of robust quality checking process to ensure responses are of required standard and reducing the number of review requests received by 'getting it right first time'.
<p>3. Development of Publication Scheme</p> <ul style="list-style-type: none"> - Collaboration with service areas to determine and analyse frequent requests for information and publish data accordingly and promote transparency
<p>4. Extend the use of corporate EDM platform</p> <ul style="list-style-type: none"> - Create CIVICA processes for all IG Workstreams - Improve reporting functionality
<p>5. Improve archiving of Council records</p> <ul style="list-style-type: none"> - Ensure appropriate use of council buildings to store records and move to central secure archive facility at Birksland

Appendix A
Information Management, Assurance & Governance (IMAG) Framework

