

Report of the Director of Finance & IT to the meeting of Governance and Audit Committee to be held on 22nd September 2022

Subject:

K

Information Governance performance and activity report for the financial year 2021/22

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.

Chris Chapman
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: (01274) 434794 / 437256
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 2021/22, 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



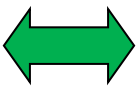
The following represents a summary of key information arising from the 2021/22 SIRO report (*shown in full at Appendix 1*); -

1. Over the last 3 financial years the Council has received, on average, **1476** Freedom of Information and **124** Environment Information requests per year. In 2021/22 the number of Freedom of Information requests received was below average with the number of Environment Information requests received being above average. The Department of Place being the Council Department who received the most Freedom of Information requests and the most Environment Information requests of all the Council Departments (**15%** of the total received).
2. In 2021/ 22, the right of access to personal data (Article 15 UK General Data Protection Regulation (UK GDPR)) was, by far, 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 3 financial years the Council has received, on average, **372** Subject access requests per year. In 2021/22 the number of requests for access to personal data, received by the Council, was slightly below average with the Department of Childrens Services receiving the most access to personal data requests of all Council Departments (**45%** of the total received).

4. In 2021/22 there has been a significant increase in the number of Data Protection Impact Assessments being carried out across the Council following the delivery of training and the introduction of a detailed process for employees to follow. These impact assessments are vital in ensuring that the Council has identified any risks in relation to the processing of personal data.
5. Over the last 3 financial years, the Council has recorded, on average, **257** data security incidents per year with **218 (85%)** of those resulting in a personal data breach. In 2021/22 the personal data breaches recorded by the Council were slightly below average.
6. In 2021/22 **75%** of the personal data breaches recorded were due to data being posted, emailed or delivered (by any other means) to the incorrect recipient or address and also made up **86%** of the high risk personal data breaches reported to the ICO.
7. The Council has assessed itself against the new ICO Accountability Framework where organisations check their existing General Data Protection Regulation and Data Protection practices against the ICO’s expectations and this resulted in a **90%** compliance across all areas. It is understood that the ICO would rate any organisation with this level of compliance as “fully meeting” its Data Protection and GDPR obligations.
8. There have been minimal interventions from the Information Commissioners Office (ICO), in 2021/22, and the few complaints lodged relating to the Council’s handling of Data Protection, Freedom of Information and Environment information requests have not been upheld by the ICO as shown below.

The table below represents a summary of key performance outcomes arising from the 2021/22 SIRO report and an indication of the direction of travel in the first quarter of 2022/23.

	2019/20	2020/21	2021/22	2022/23 (Q1)
% of information requests responded to within the statutory timescale				1st April 2022 to 30th June 2022
Freedom of Information / Environment Information	88%	92%	91%	89% 
Data Protection Subject Access	79%	96%	91%	92% 

% of complaints to the ICO which were not upheld				
Freedom of Information / Environment Information	31%	67%	100%	Not applicable (No complaints)
Data Protection	67%	83%	100%	50% 
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%)	2 (3%) 
Protecting Information Learning				
% of employees who have completed the mandatory learning	Not known	66%	74%	74% 

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 Digital, Culture, Media and Sport. 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 million or 4% of turnover, whichever is the greater.

In the financial year 2021/22, the ICO imposed 65 monetary penalties and 35 enforcement notices on organisations. No monetary penalties or enforcement notices were imposed on Councils; however, the Cabinet Office was fined £0.5m for disclosing the postal addresses of the 2020 New Year Honours recipients online. The Ministry of Justice was issued with an enforcement notice for contravention of Article 15 of the UK GDPR for failing to provide without undue delay 7,753 data subjects with a copy of their data in accordance with its legal obligations.

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 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 or not 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 GREENHOUSE GAS EMISSIONS IMPACTS

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 ASSESMENT

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 2020/21

12. BACKGROUND DOCUMENTS

None
Appendix 1

Report of the Senior Information Risk Owner (SIRO)



2021/2022

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 2022** 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, in particular, information security and that this is embedded as part of the Council's culture.

2.0 Key Roles and Responsibilities

Appendix 1 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 officer 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 is able to 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** (IGC) 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 (at least quarterly) 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

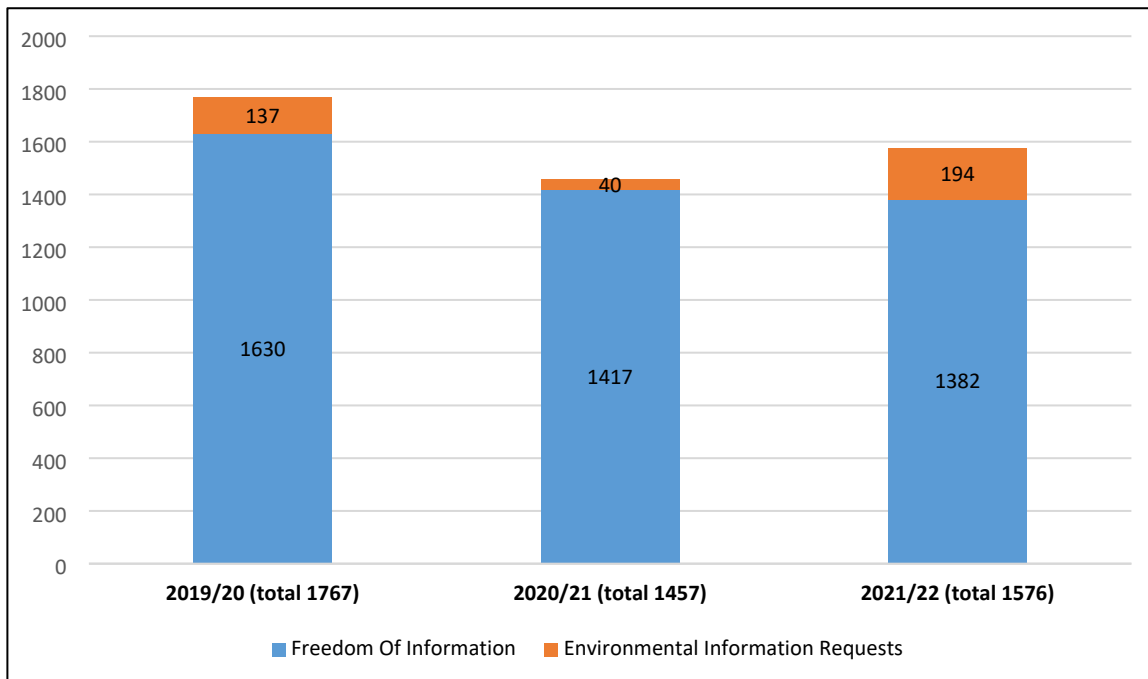
4.1 Freedom of Information / Environment Information

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

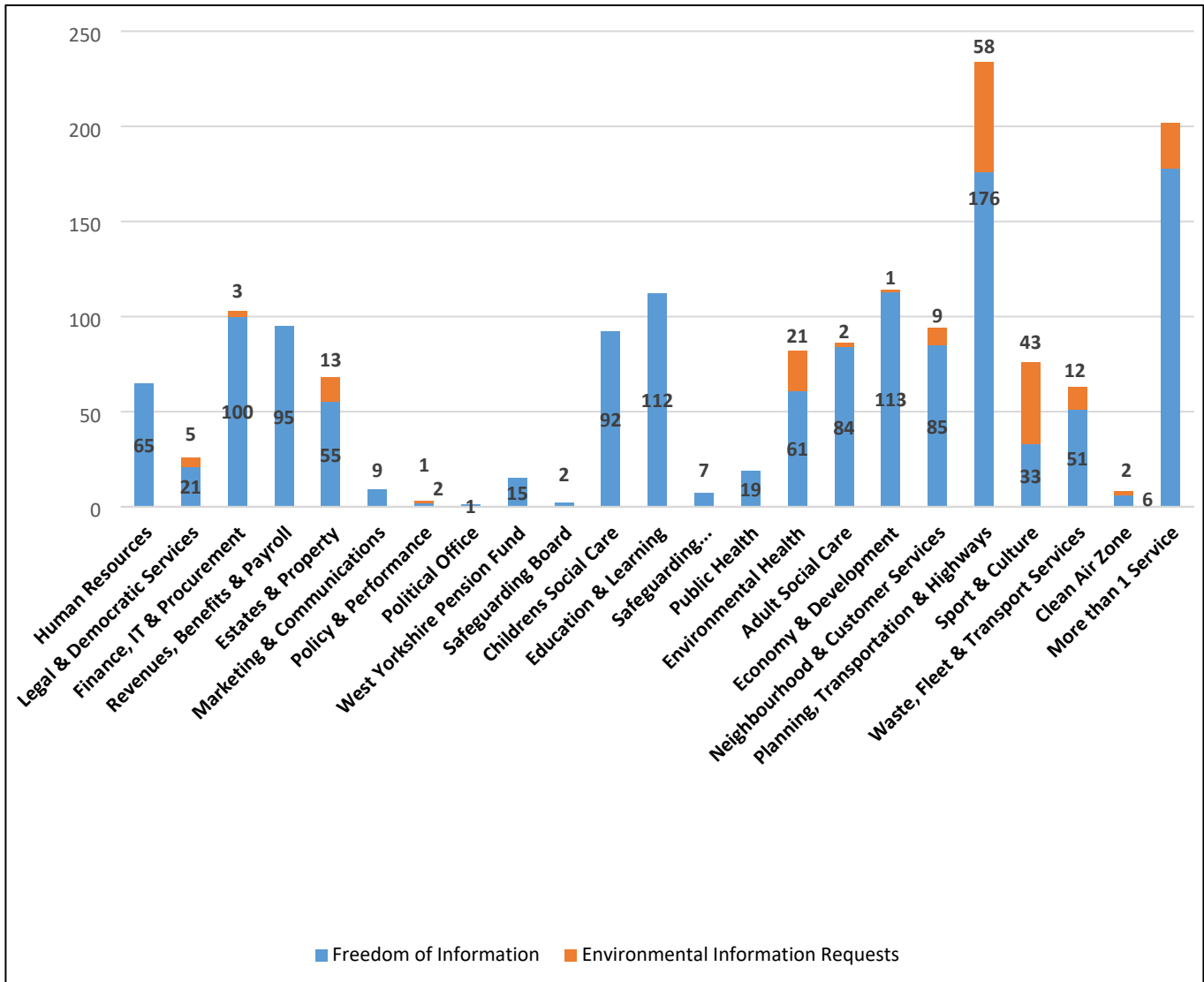
- a. provide information requested by members of the public and
- b. to publish information proactively

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 3 financial years



Graph 2 below demonstrates the number of FOI and EIR requests received in 2021/22 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 2021/22.

Exemptions (FOI)	199
Exceptions (EIR)	20
GRAND TOTAL	219

Appendix 2 demonstrates the type and number of specific exemptions and exceptions applied by the Council broken down into absolute and qualified.

Table 2 below demonstrates the number of instances in 2021/22 where the Council has not provided the information requested in accordance with the Freedom of Information Act and the reasons; -

Section 1 - Information not held	75
Section 3 - Data held by the Public Authority on behalf of another person	2
GRAND TOTAL	77

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 2021/22.

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).

To reach a decision about whether or not 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 43 Section 12 refusal notices during 2021/22, on the grounds that it estimated that unreasonable cost would be incurred.

4.1.4 Responses

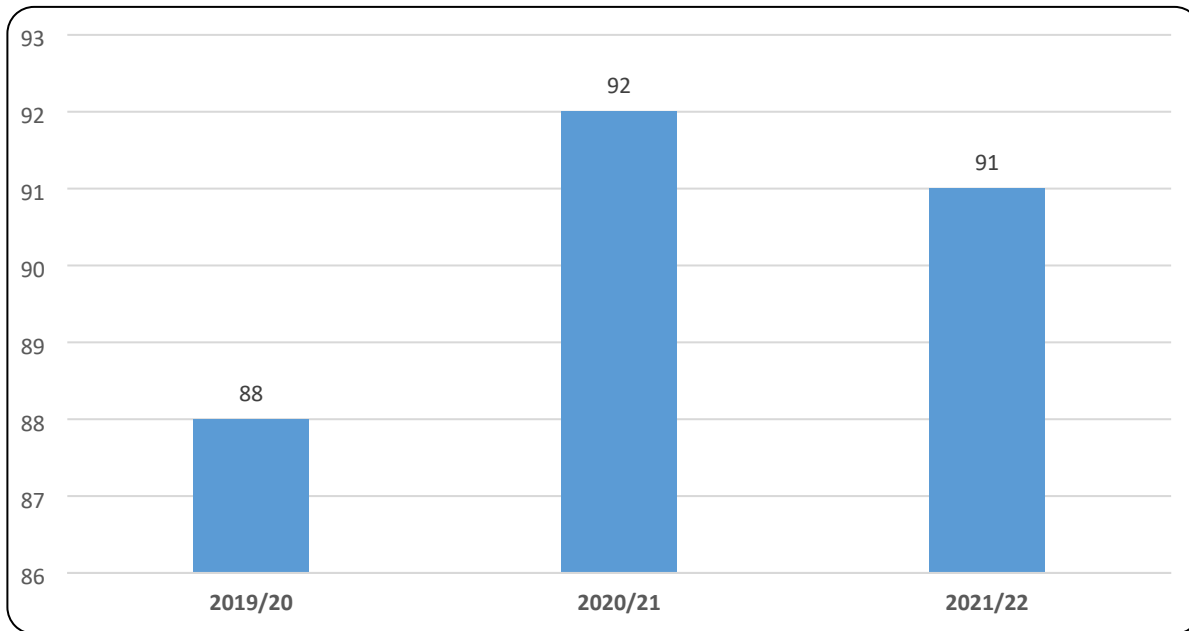
Requests for information under the Freedom of Information or Environmental Information legislation must be responded to within a statutory timescale of 20 working days. Whilst there is provision under the legislation for the Council to extend or vary this time limit to consider the public interest test or under the Environmental Information Regulations where there is a lot of complex information which

makes it more difficult to respond, any extension is only in exceptional circumstances and decisions 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	58
Environment Information	14
GRAND TOTAL	72

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



In 2021/22 **92%** of EIR requests and **90%** of FOI requests were responded to within the legislative timescale but for 2019/20 and 2020/21 this data was not collected.

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 3 financial years (*and as a % of all requests completed*)

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

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 and the Information Commissioner, 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 3 years

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

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 3 financial years

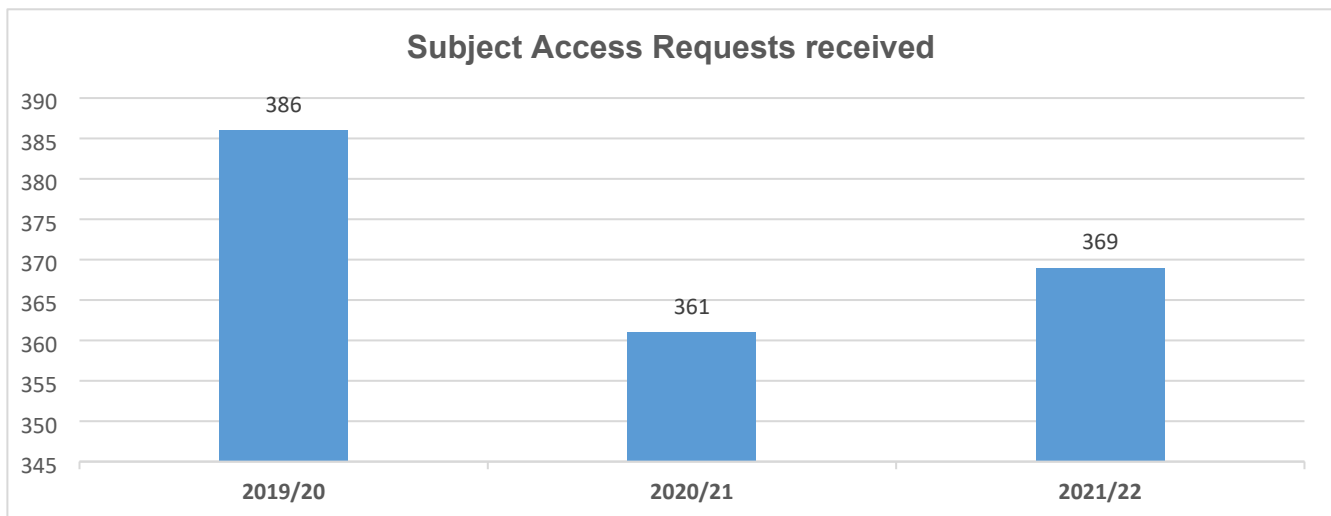
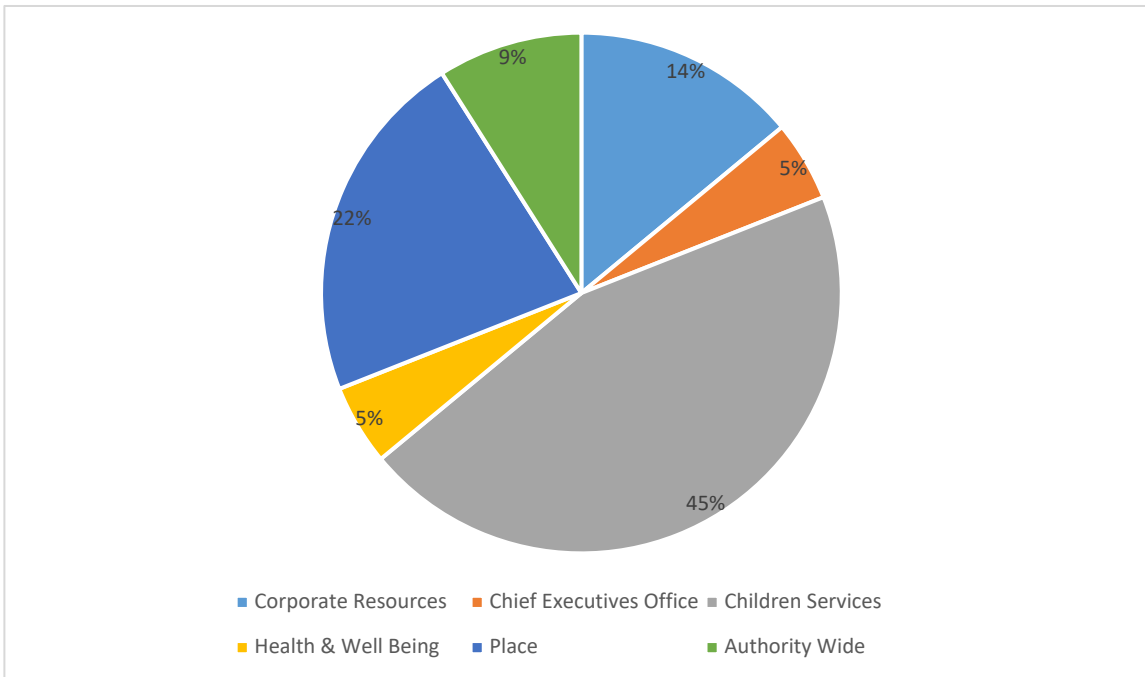


Chart 1 below demonstrates the % of SAR's received for each Council Department in 2021/22



4.2.2 Exemptions

Whilst a number of 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.

In 2021/22 the Council applied such exemptions but the data on the number of cases where an exemption was applied is currently not collected centrally. Work is ongoing to ensure that this data will soon be available.

4.2.3 Charges

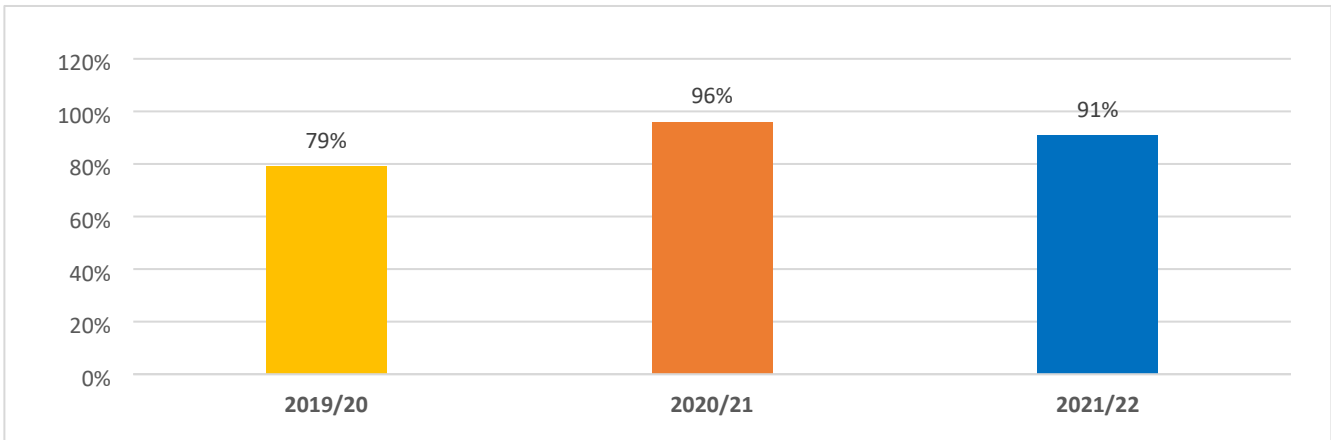
The Council, in accordance with the legislation, does not charge a fee to deal with Subject Access requests.

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 a number of requests have been received from the same individual. Decisions on extension are always taken in conjunction with the Corporate Information Governance team.

In 2021/22 the Council extended the time limit in **100** of the requests (*27% of all requests received*). This has been predominantly in complex Childrens Services cases going back over a number of 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 3 years



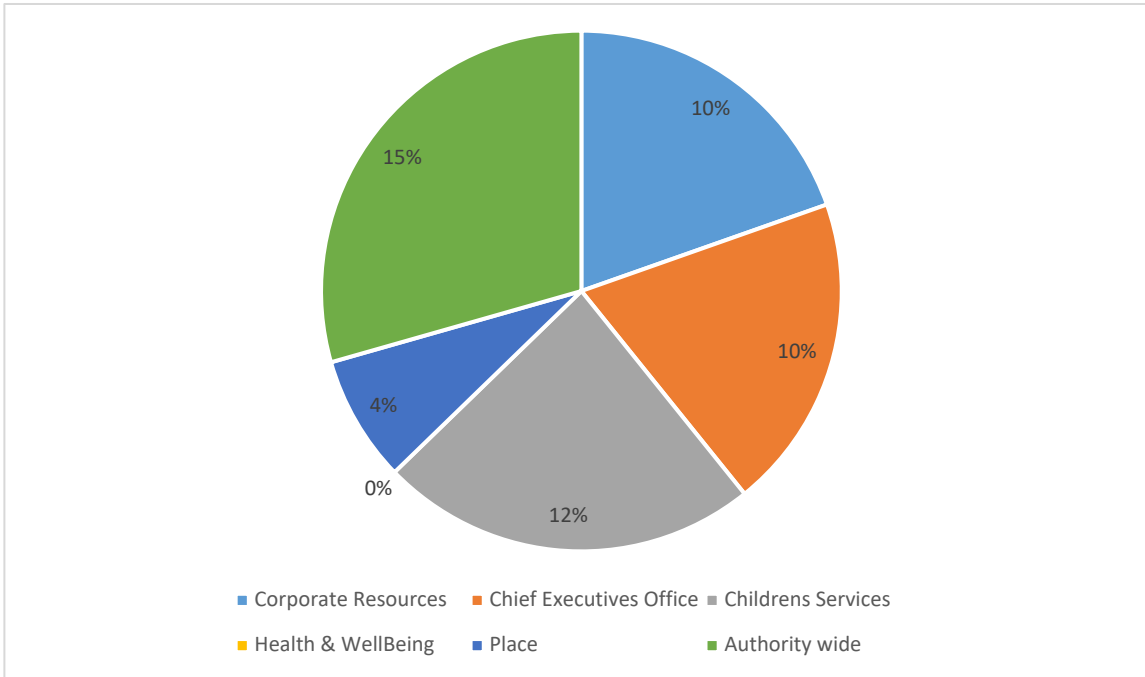
4.2.5 Internal Reviews

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 Information Commissioner's Office by the requester.

Table 6 below demonstrates the number of internal reviews processed by the Council in the last 3 financial years and as a % of all requests responded to

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

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 2021/22.

Table 7 below demonstrates the number of SAR complaints made to the Information Commissioner and the number upheld over the last 3 years

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

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 Information Commissioners Office (ICO) Accountability Framework

Accountability is one of the key principles in data protection law and makes the Council responsible for complying with the legislation and demonstrating compliance.

The ICO have recently developed an Accountability Framework for organisations to check their existing General Data Protection Regulation (GDPR) and Data Protection practices against the ICO’s expectations. The framework is divided into 10 categories with each category displaying the ICO’s key expectations and a list of how these expectations can be met.

In 2021/22 the Council has used this framework to carry out a “self – assessment” resulting in 90% compliance across all areas which the ICO would rate as the Council “fully meeting” its obligations. The areas assessed as partially or not meeting the expectation were minimal however they have been included in the 2022/23 Information Governance Service Improvement Plan for action.

Appendix 3 shows a more detailed breakdown of the self-assessment.

5.2 Individual rights under the UK GDPR

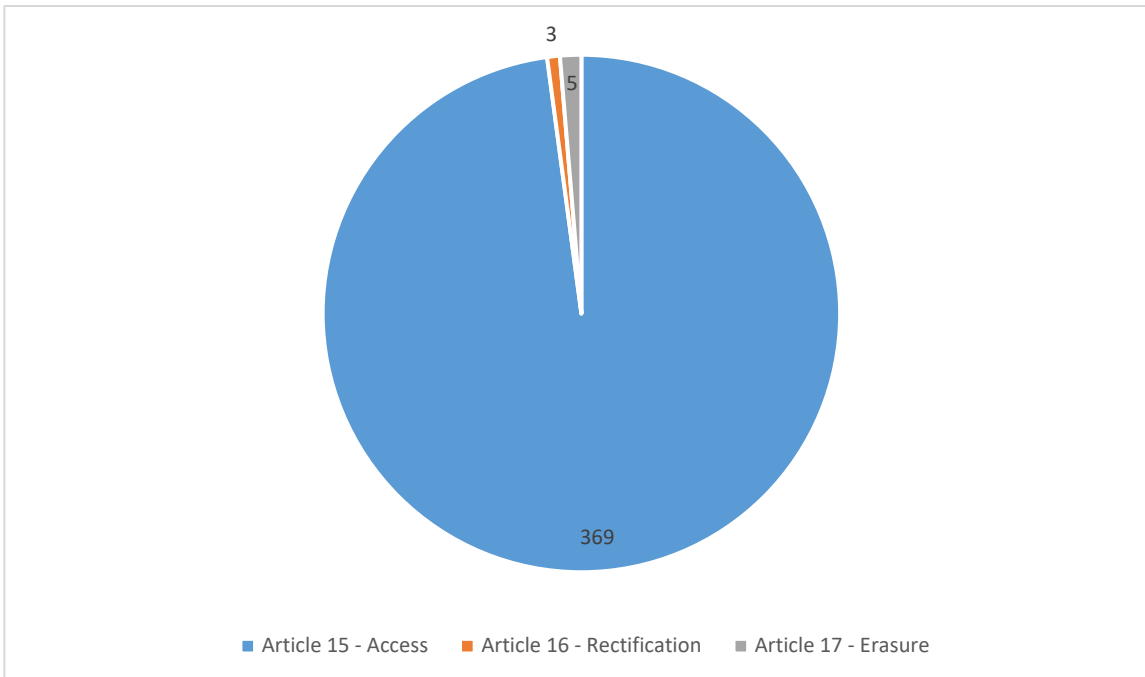
The UK GDPR grants data subjects certain rights regarding their personal data including the right:

- 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 2021/22 the Council received 377 requests from data subjects regarding their personal data

Chart 3 below demonstrates a breakdown of the requests



5.3 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 or not the level of risk is acceptable taking into account 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 2021/22 **37** DPIA Screening questionnaires and **59** DPIA's were completed. This is a significant increase from the 39 DPIAs completed in 2020/21 and reflects the work carried out to raise awareness of the legal requirement to complete a DPIA across Council Services and Departments.

In 2021/22 the Corporate Information Governance SharePoint site was extended to allow for all completed DPIA's to be loaded onto SharePoint where automated review triggers are enabled to ensure that DPIAs are reviewed and refreshed annually.

5.4 Data Sharing

Agreements are required between all parties with whom the Council routinely shares personal data which 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 2021/22 the Data Protection Officer reviewed **32** 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 ISA's are reviewed and refreshed annually.

5.5 Records Management

Effective records management supports effective data governance and data protection and is a necessary requirement to ensure that the Council meets the ICO's Accountability Framework in full.

Following the creation of a Council's Records Management Policy in the financial year 2020/21, the Council's Records Retention and Disposal Policy was reviewed and updated in 2021/22 and sets out the functions, activities and transactions which either generate, or necessitate, the keeping of records and their recommended disposal. This will be supported by a comprehensive retention schedule which is being compiled to clearly list documents and information held for all Council services, referencing the legislative reasons and timescales applied to the retention of Council records.

Work is progressing across all Council Services and Departments to ensure the effective management of all records and information held in both electronic and physical formats. In 2021-22 a number of service specific privacy policy statements were created, and others were reviewed, to ensure Service Users are fully aware of the personal data the Council collects, the reasons for processing and details of any personal data shared with other organisations.

All Council privacy notices are held on the Council's external website and also uploaded to the Corporate Information Governance SharePoint site where automated review triggers are enabled to ensure that the privacy notices remain up to date.

5.5.1 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.

In 2021-22, the Council's Records Management Officer reviewed all Information Asset Registers held in Council Services to ensure that they were up to date; that they provide the necessary information, as recommended by the ICO, and are a true record of information held within the Council's systems and assets.

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.

5.5.2 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 is committed to creating a comprehensive list of retention periods relating to all documents and information held which enable the Council to carry out its business. This relates to all paper, digital and electronic documents.

Following work undertaken in conjunction with the Council's Records Management Officer in 2021-22, **36** service specific retention schedules have been created which reflect the diverse range of records and documents held across the Council.

The retention schedules give clear guidance to Council employees on the retention and destruction of records within their Service area and also details the related legislation applicable to individual records. A published version of the Council's retention schedule will be posted on the Council's external website which will demonstrate the Council's continued commitment to transparency.

5.5.3 Email Retention Policy

In November 2021 the Council's IT Service in conjunction with the Council's Records Management Officer introduced an email retention policy to ensure that all archived Council emails are deleted in line with the agreed retention period of 3 years.

In exceptional circumstances, where it is necessary to retain emails for longer than 3 years then this can be agreed, for a temporary period, by the Council's Records Management Officer; Head of IT Services or the Council's Senior Information Risk Owner.

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.

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

In May 2021, to ensure compliance with UK GDPR, for any Council employees intending to temporarily work from outside the UK, a new process was introduced which requires Council Managers 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 a 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 2021/22 **18** requests to work abroad were received of which 10 were approved. The **8** 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 and the Council have line of sight of the device 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 complex passwords/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, a new MDM solution is now in place for new devices which has far greater functionality and security and rollout will be starting in August 2022.

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 new Security IT review panel has been created to review all patches and security requirements. The Panel meet on a weekly basis or 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 Response 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 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 a number of local authorities. 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 also ensuring 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;

- The procurement of a Managed Security Service Provider (MSSP) to work in partnership with the Council to protect the Council's hybrid ICT environment (On-Prem, Cloud and Multi Tenanted) from information and cyber security threats and incidents from both inside and outside the Council.
- Continual assessment of solutions to further protect the Council; - Secure self-serve DNS management; Cloud DDOS services; Web Security headers; Improved SSL certificate management.
- 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. Our Enterprise Architect and Systems Service Manager is the Chair for the YHWARP, which gives us a heads up on any potential attacks or vulnerabilities across the UK and also part of the North, South, West Yorkshire and Humberside (Local Resilience Forum) LRF's to immobilise any responses during a cyber-attack and to develop strategies, communications, protocols etc during peacetime. 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.
- New Storage Infrastructure Environment e.g. Backup snapshot (*specifically protects against malware restoration*)
- New perimeter firewalls to protect against hackers accessing the Council network
- 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.
- The procurement of a Microsoft AD monitoring service which alerts to any malicious activity occurring within the Council's Active Directory environment

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 3 financial years, the number of data security incidents; the number where personal data was breached and the number where personal data was breached and were reported to the ICO.

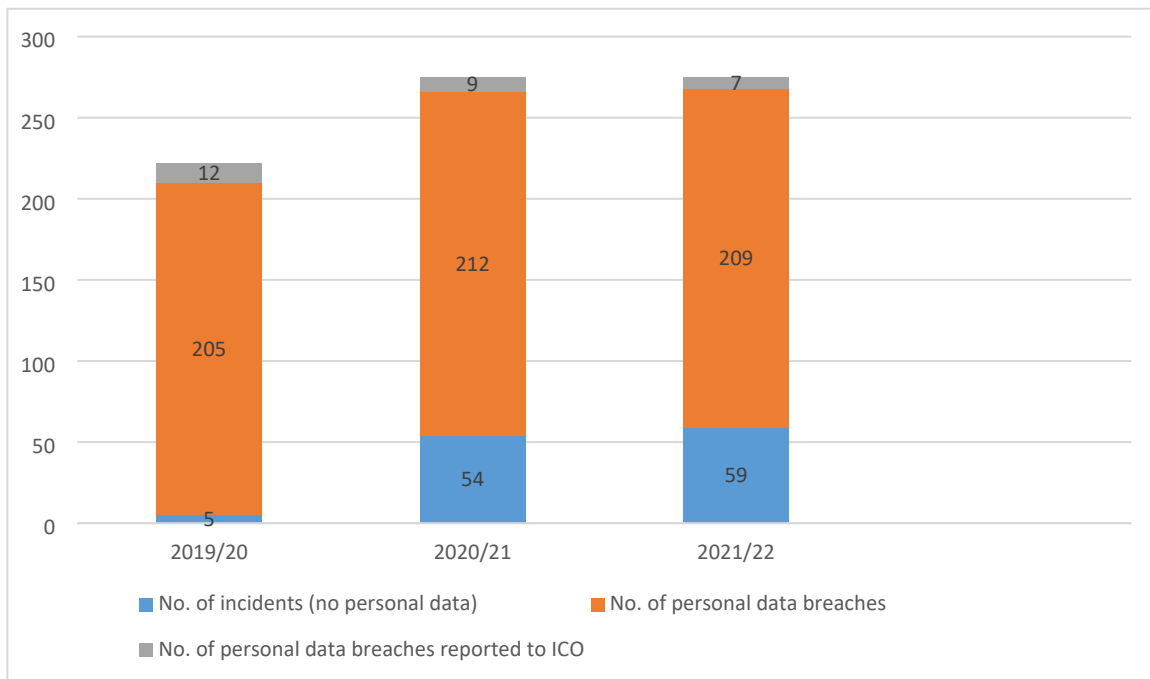
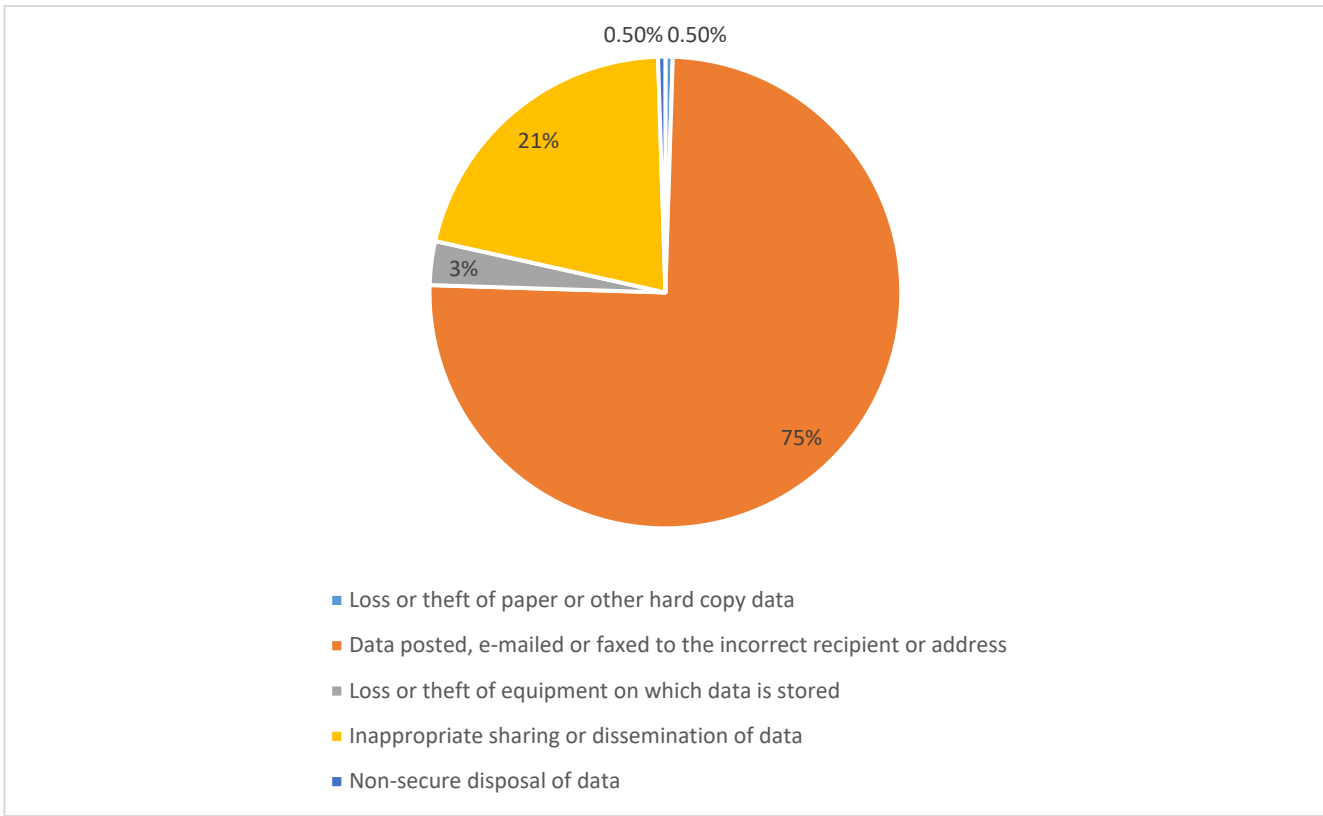


Chart 4 below shows a breakdown of the reasons for the personal data breaches recorded in 2021/22.



The Council's Data Protection Officer took the decision, on behalf of the Council, to refer **7** of the personal data breaches to the Information Commissioners Office as they were considered to be likely to result in a high risk of adversely affecting individuals' rights and freedoms. **6** of these personal data breaches occurred as a result of data posted, emailed or faxed to the incorrect recipient and 1 due to the inappropriate sharing or dissemination of data.

In response to the **7** potential high risk personal data breach referrals from the Council, 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. The following actions were taken as a result of the ICO recommendations:

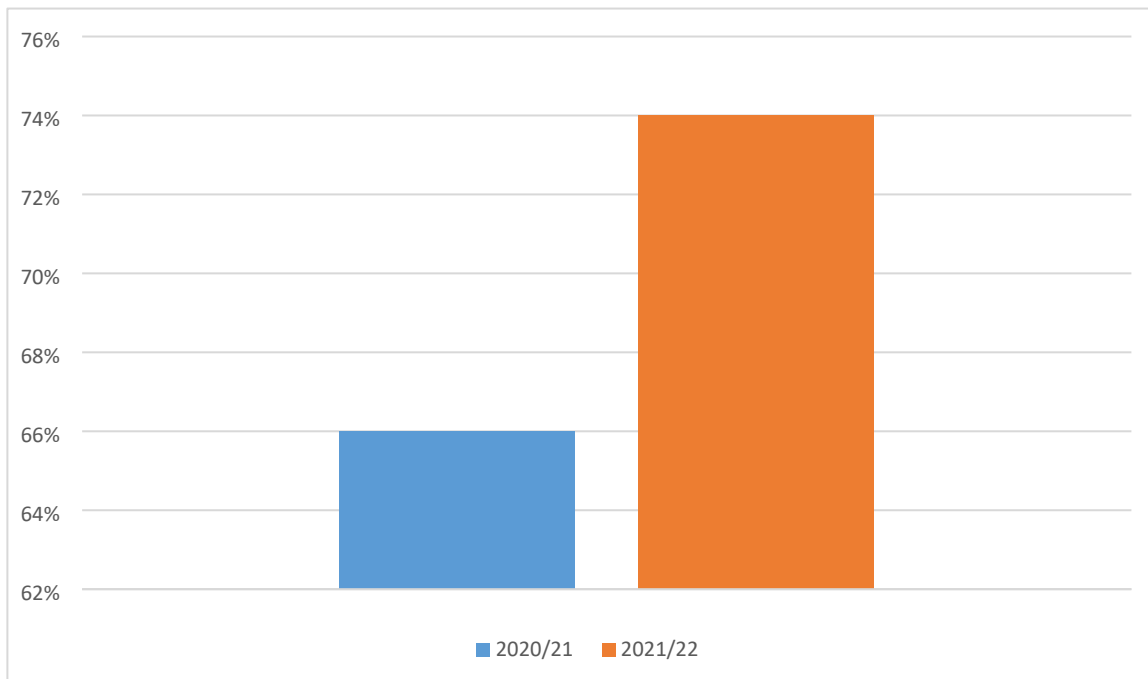
- A review of policies and procedures in Children's social care
- Reminders to all Council staff handling personal data to complete the Council's learning
- Reminders to all Council staff on a regular basis of the importance of data protection, their responsibilities, and the correct processes to follow.
- Created a new process to verify contact details of new members of Council staff prior to sending written or electronic correspondence
- Redesigned the Council's annual training package to include specific examples of personal data breaches which could result in a high risk of adversely affecting individuals' rights and freedoms

6.9 Protecting Information Training

In March 2022 the Council launched a new version of a bespoke eLearning package now known as “Information and the UK GDPR”. This mandatory annual training package, for all Council employees with access to a PC, replaced the “Protecting Information” eLearning and gives information and practical examples on the UK GDPR and how to handle data safely followed by an assessment for which the learner must achieve 80% compliance to gain the “acquired” certificate.

For those employees without access to a PC they are required annually to read a Council developed leaflet on how to protect information whilst carrying out their role for the Council. This leaflet is currently undergoing a refresh.

Graph 7 below demonstrates the % of Council employees, Elected Members and casual employees who have completed the learning in 2021/22 compared with 2020/21.



It is an expectation of the ICO that organisations will achieve at least 90% compliance in ensuring employees who handle person data are adequately trained and whilst compliance has improved in the last 12 months there is still some way to go and this will be progressed and actioned with the Information Assurance Group in the current financial year.

7.0 Progress against key improvement actions

The Corporate Information Governance team have a series of action plans to support on-going improvement and during the financial year 2021/22 have completed the following key actions to strengthen the Council’s management, assurance and governance of information; -

- Refresh of the GDPR Protecting Information training was launched in March 2022. Improved reporting functionality of statistics
- Completion of the ICO Accountability Framework
- Council wide roll out of the IG SharePoint site for IAO’s and key officers involved in Information Governance (now the one stop resource for all IG documents with automated review triggers for DSA, DPIA, IAR and Privacy Notices)

- Introduction of a Records Retention and Disposal Policy and associated retention schedules
- Expansion of the data available in the public domain (on the Council's website) to give greater transparency in relation to the Freedom of Information Act 2000
- Approval and implementation of the Council's Data Protection Policy
- Held the first ever Digital Clean Up Week from March 14-19 as part of the International Digital Clean Up Day on 18 March 2022.

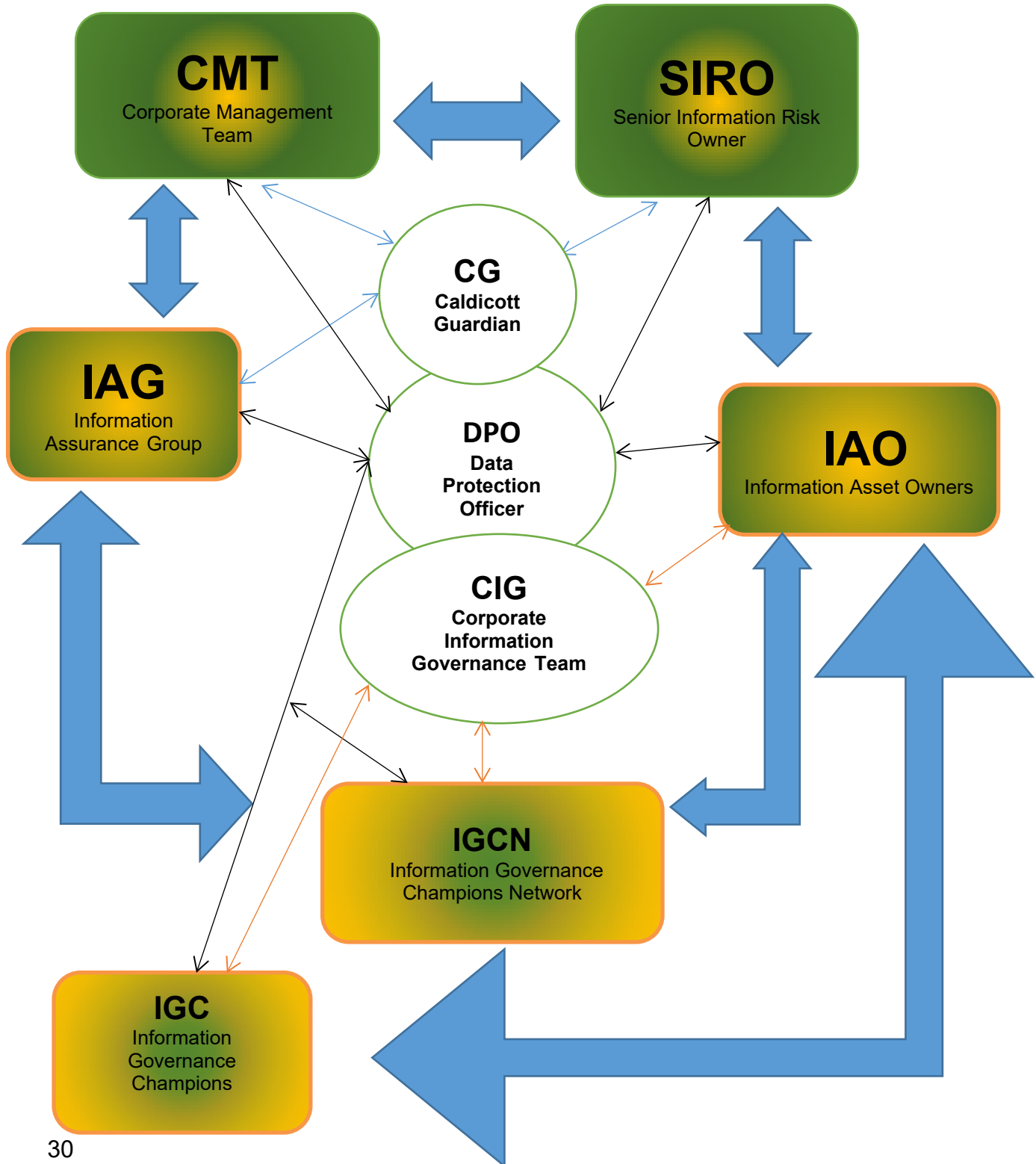
The following actions are progressing or to be progressed in the 2022/23 financial year

- Implementation of a Civica Document Workflow system for processing Subject Access Requests
- Refresh of the paper based GDPR Protecting Information learning for non PC users
- Development of Departmental IG Scorecards building upon the learning from the ICO Accountability Framework
- Refresh of the Members Packs on GDPR compliance
- Development of new training and awareness promotion of the Data Sharing Code of Conduct
- Improving compliance with mandatory training

8.0 Conclusion

In summary, this report has demonstrated the progress made during 2021/22 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.

Appendix 1
Information Management, Assurance & Governance (IMAG) Framework

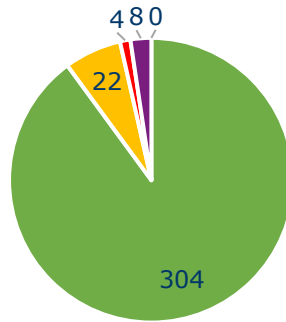


Appendix 2 - Freedom of Information (FOI) Act exemptions and Environmental Information Regulations (EIR) exceptions applied by the Council in 2021/22

<u>Exemption - FOI</u>	Times Applied	Type of Exemption
Section 21 - Reasonably Accessible by other means	90	Absolute
Section 22 - Future Publication	5	Qualified
Section 24 - National Security	3	Qualified
Section 30 - Investigations and proceedings	2	Qualified
Section 31 - Law Enforcement	46	Qualified
Section 36 - Prejudice to effective conduct of public affairs	2	Qualified
Section 40 - Personal Information	37	Absolute
Section 41 - Confidentiality	4	Absolute
Section 43 - Commercially Sensitive	10	Qualified
TOTAL	199	
<u>Exception- EIR</u>	Times Applied	Type of Exemption
Regulation 12(3) & Regulation 13 - Personal Information	5	Qualified
Regulation 12(4)(a) - Information not held	3	Absolute
Regulation 12(5)(b) - Course of justice	8	Qualified
Regulation 12(5)(e) - Confidentiality of commercial information	1	Qualified
Regulation 12(5)(f) - Confidentiality	1	Qualified
Regulation 6(1)(b) - Information publicly available	2	Qualified
TOTAL	20	

Appendix 3 – ICO Accountability Framework data

Breakdown of 'Current status' of all categories



- Fully meeting our expectation
- Partially meeting our expectation
- Not meeting our expectation
- Not Applicable
- Blank

Volume of 'Current Status' per category

