City of BRADFORD METROPOLITAN DISTRICT COUNCIL

Report of the Director of Finance & IT to the meeting of Governance and Audit Committee to be held on 22nd July 2021

F

Subject:

Information Governance performance and activity report

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

Report Contact: Tracey Banfield / Harry Singh
Head of Corporate Investigations, Information Governance and Complaints
Phone: (01274) 434794 / 437256
E-mail: tracey.banfield / harry.singh @bradford.gov.uk

Portfolio:
Leader of the Council & Corporate

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 2020/21, 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.

As the Committee will recall from the information presented in January 2021, relating to the financial year ending March 2020, approximately two years ago a number of information compliance concerns were identified with many requiring immediate improvement if the Council was to avoid intervention and possible financial penalty from the Information Commissioner.

The Senior Information Risk Owner report for 2019/20 presented at the January Committee demonstrated how the Council had taken appropriate and timely action to ensure that performance in 2019/20 improved and the risks to the Council compliance with information governance legal obligations were mitigated.

3. OTHER CONSIDERATIONS

As the 2020/21 SIRO report (shown at Appendix 1) demonstrates, performance in key areas has continued to improve, despite the impact the pandemic has had on the Council's resources in this financial year.

Key performance data summarised from the 2020/21 SIRO report demonstrates both continuous improvement and areas for focus in 2021/22 as follows; -

Information Requests	**2019/20**	**2020/21**	**2021/22** (1st April – 31st May)
% of requests responded to within the statutory timescale			
Freedom of Information / Environment Information	88%	92%	93%

Data Protection Subject Access	79%	96%	98%
% of information requests completed which resulted in a request for a review	**2019/20**	**2020/21**	**2021/22** (1st April – 31st May)
Freedom of Information / Environment Information	3%	3%	3%
Data Protection Subject Access	4%	7%	5%
% of Complaints to the ICO which were not upheld			
Freedom of Information / Environment Information	31%	67%	
Data Protection	67%	83%	
Data Security Incidents			
High risk personal data breaches reported to the ICO (as a % of total incidents)	12 (19%)	9 (3%)	1 (2%)
Protecting Information Learning			
% of employees who have completed the mandatory learning			
Employees with access to a PC	90%	81%	86%
Employees without access to a PC	54%	39%	61%

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 2019/20, the ICO imposed 26 monetary penalties and 8 enforcement notices on organisations, however no monetary penalties or enforcement notices have been imposed on Councils in the last financial year.

The ICO has not prosecuted any UK Council employees in the last financial year, however a motor industry employee was prosecuted for passing on the personal information of service users to an accident claims management company without authorisation. The employee was sentenced to eight months' imprisonment, suspended for 2 years.

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) sets out the framework for data protection law in the UK. alongside the General Data Protection Regulation EU 2016/679, both setting out the key principles, rights and obligations for most processing of personal data. The UK's exit from the EU has resulted in changes to the principal legislation which makes up the UK's data protection regime. The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 amend the EU General Data Protection Regulation 2016 (EU GDPR) and the DPA. The revision of the EU GDPR is now known as the UK GDPR. The recitals form part of the UK GDPR pursuant to section 3 of the European

Union (Withdrawal) Act 2018. Technical changes have been made to enable it to work effectively 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

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 not 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 him.

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 should 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

Annual Report of the Senior Information Risk Owner (SIRO) 2020/2021

Contents

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 2021** 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 Asset Operational Network** (IAON) supports the strategic IAG, and the individual service Information Asset Owners, to fulfil their obligations in relation to information.

Service Champions are in each Service and assist the Corporate Information Governance team to co-ordinate all requests for information.

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

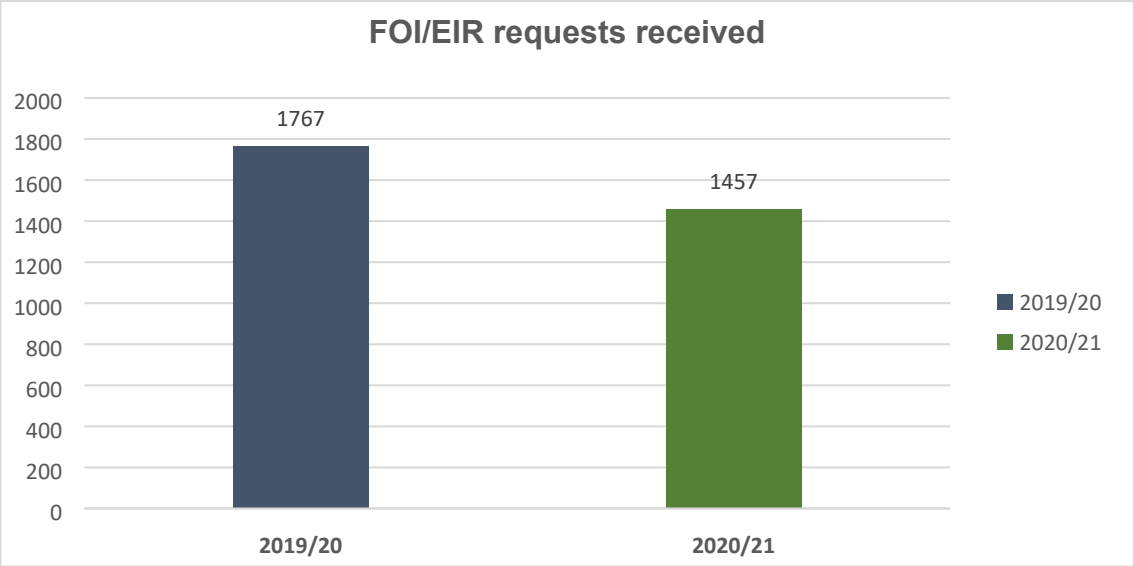
4.1 Freedom of Information / Environment Information

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 2020/21 compared with 2019/20



4.1.2 Exemptions

Both the Freedom of Information (FOI) Act and Environmental Information Regulations (EIR) contain exemptions that allow the Council to withhold specific information, for example, if the information is commercially or legally privileged.

Under the FOI Act there are **23** exemptions that may prevent the right of access to information and the exemptions fall into two categories:

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

- 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, the applicant must be issued with a Refusal Notice within the relevant statutory timescale of 20 working days.

The Council applied **254** exemptions during the financial year 2020/21.

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

Additionally, the Council has not provided information in a further **61** requests for the following reasons; -

Section 1 - Information not held	58
Section 3 - Data held by the Public Authority on behalf of another person	1
Section 14 - Vexatious or Repeated	2

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 charges during 2020/21.

However, where the Council estimates that a Freedom of Information Act request will incur unreasonable cost then it can issue a Refusal Notice under Section 12 of the Act. 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 to determine whether the information is held; to locate the information or appropriate documents; to retrieve the information or document containing it; to extract the information and process the request.

The Council issued **59** refusal notices, during 202/21, on the grounds that it estimated that unreasonable cost would be incurred.

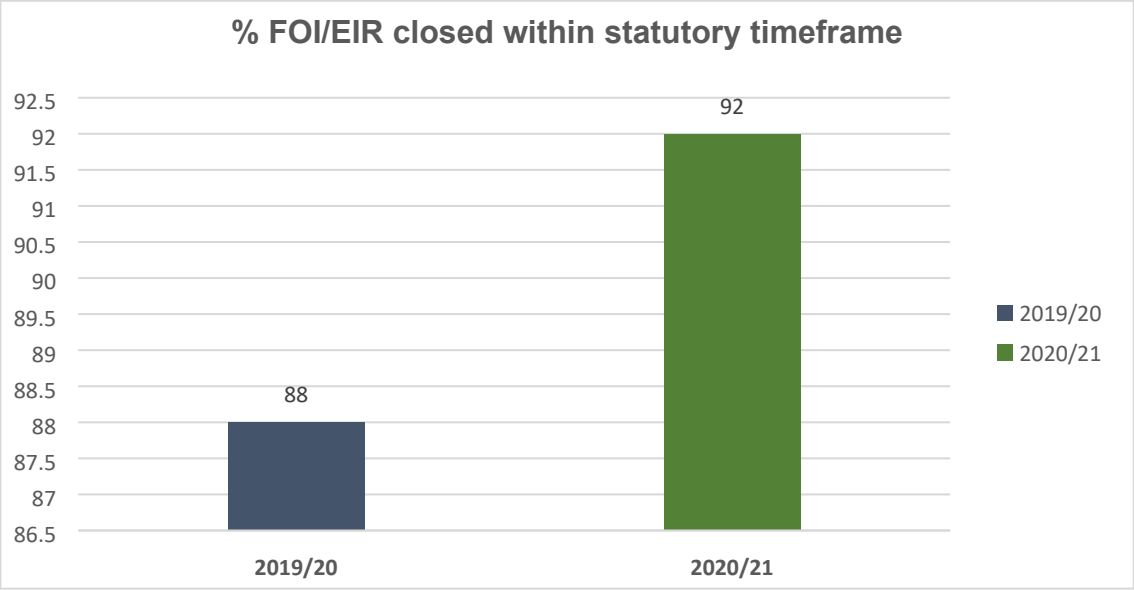
4.1.4 Responses

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.

In 2020/21 due to the impact of the pandemic on Council resourcing and in accordance with the guidance from the Information Commissioner, the Council took a pragmatic approach to responses to FOI and EIR and extended the response times, for any requests received between 1st April 2020 and 2nd August 2021, to within a maximum of 30 working days i.e. an increase of 10 working days.

Additionally, in 2020/21 the Council applied a further extension to **117** of the requests (8% of all requests received); predominantly due to the complexity of some of the requests.

Graph 2 below demonstrates the % of Freedom of Information / Environment Information request responded to within the agreed timescales in 2020/21 (92%) compared with 2019/20 (88%)



Had the Council not extended the allowable time taken to respond to requests in accordance with guidance from the ICO, as referred to above, then **79%** of FOI/EIR would have been closed within the timeframe in 2020/21.

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 1 below demonstrates the number of internal reviews processed by the Council compared with 2019/20

Internal FOI/EIR Reviews	**2020/21** (as a % of all requests completed)	**2019/20** (as a % of all requests completed)
Freedom of Information / Environmental Information Regulations	42 (3%)	53 (3%)

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 2 below demonstrates the number of FOI/EIR complaints made to the Information Commissioner and the number of cases where a decision notice and/ or recommendations for further action were made compared with 2019/20.

	2020/21	**2019/20**
No. of FOI / EIR complaints to ICO in year	3	13
No. of ICO decision notices received in year	3	6
No. of ICO recommendations in year	1	4
No. of ICO complaints requiring no further action by the Council (*no decision notice*)	2	0
No of ICO complaints awaiting a decision	1	0

The 3 decision notices, issued by the Information Commissioner in 2020/21, related to complaints made in the previous financial year. 2 of these decision notices confirmed that the Council had complied with the duty to advise and assist and had correctly applied the relevant exemptions and 1 required recommendations to be implemented within a 35-day timeframe which the Council complied with.

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.

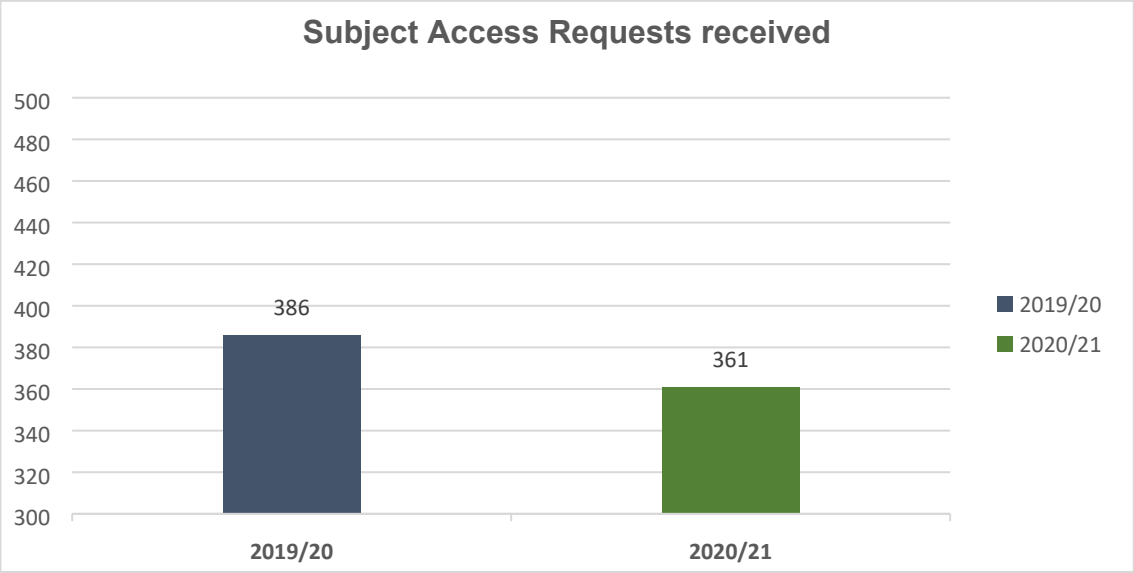
https://www.bradford.gov.uk/open-data/publication-scheme/publication-scheme/

4.2 Subject Access Requests (SAR)

In accordance with the UK General Data Protection Regulation and 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 commonly known 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 3 below demonstrates the number of subject access requests received in 2020/21 compared with 2019/20



45% of the subject access requests received in 2020/21 required access to Children's Services data.

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 2020/21 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.

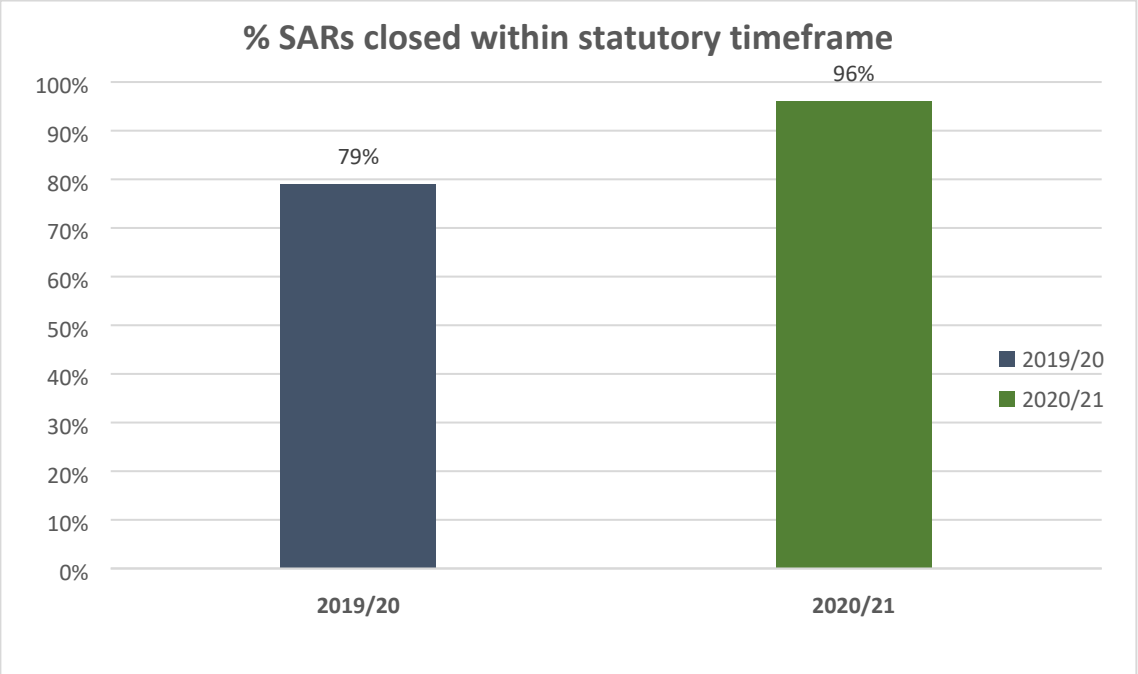
4.2.4 Responses

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 2020/21 due to the impact of the pandemic on Council resourcing and in accordance with the guidance from the Information Commissioner, the Council took a pragmatic approach to responses to SAR and extended the response times, for any requests received between 1st April 2020 and 2nd August 2021, to within a maximum of 2 months i.e. an increase of 1 month.

Additionally, in 2020/21 the Council applied a further extension to **111** of the requests (31% 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 4 shows the % of subject access requests responded to within the statutory timescale compared with 2019/20



Had the Council not extended the allowable time taken to respond to requests in accordance with guidance from the ICO, as referred to above, then **81%** of FOI/EIR would have been closed within the timeframe in 2020/21.

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 referral to the Information Commissioner's Office by the requester.

Table 4 below demonstrates the number of internal reviews processed by the Council compared to 2019/20

Internal SAR Reviews	**2020/21** (as a % of all requests completed)	**2019/20** (as a % of all requests completed)
Data Protection Act	24 (7%)	16 (4%)

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 2020/21.

Table 5 below demonstrates the number of SAR complaints made to the Information Commissioner

and the number of cases where follow up actions were requested

	2020/21	2019/20
No. of SAR complaints to ICO	6	6
No. of complaints investigated by the ICO	3	2
No. of ICO investigations requiring no further action by the Council	2	0
No. of ICO investigations requiring follow up action by the Council	1	2

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) which came into effect on 25th May 2018

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

In 2020/21 the Council received **361** requests for access under Article 15 of the UK GDPR (see paragraph 4.2.1) **1** request for rectification under Article 16 and **4** requests for Erasure under Article 17 of the UK GDPR.

5.2 Data Protection Impact Assessment (DPIA)

Conducting a DPIA is a legal requirement and a key part of the Councils 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 developed a UK DPIA template for data controllers 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 Data Protection Officer.

In 2020/21 **39** DPIA's were carried out and reviewed by the Data Protection Officer.

5.3 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 2020/21 the DPO reviewed **40** data sharing agreements.

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 ICO's Accountability Framework in full.

In January 2021 to improve records management across the Council, a full time Records Management Officer was recruited

In 2020/21 a new Council Records Management Policy was created, demonstrating the Council's commitment to use, manage and dispose of information held securely and safely and in accordance with the UK GDPR for managing personal data.

The creation of a robust records management infrastructure is underway and this will enable the Council to effectively manage the records and information held in all electronic and physical formats.

5.4.1 Information Asset Register (Record of Processing Activity)

The register holds details of all information assets (software and hardware) including asset owners, the location, details of 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.

The Records Management Officer is currently reviewing Information Asset Registers held in all services across the Council to ensure that these remain up to date, that they provide the necessary information recommended by the ICO and are a true record of information held within the Council's systems and assets.

5.4.2 Retention Schedule

The retention schedule gives details of storage periods for all personal data, which are regularly reviewed and is a requirement of the ICO's Accountability Framework. Retention periods of records and documents held are based on business need with reference to statutory requirements and other principles (e.g. National Archives guidelines). The schedule must provide sufficient information to identify all records and to implement disposal decisions.

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. The UK GDPR state that personal data must not be excessive and must not be retained any longer than necessary. All records should be identified and managed by a retention schedule advising officers throughout the Council of expiry dates for data held.

In March 2021, work commenced to create service specific retention schedules which will continue throughout 2021/22.

5.4.3 Acceptable Software Use

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

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 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 is able to ensure that all information stored on the device can be wiped and this can be done remotely.

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.

6.2 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)

6.3 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.

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.

6.4 Cyber security incident

Key improvements to improve security and the threat of incidents were identified and have been implemented as follows;

- Procurement of a managed service to actively manage the traffic and trends on the Councils perimeter, blocking traffic and devices as appropriate
- Changes to the patching process
- Closer working with the National Cyber Security Centre (NCSC)
- 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.
- New ITIL Change Management Process put in place
- New Storage Infrastructure Environment e.g. Backup snapshot *(specifically protects against malware restoration)*
- New perimeter firewalls to protect against hackers accessing the Council network
- A security tool to be more proactive in finding vulnerabilities on the Council network
- 2 dedicated posts of ISP Service Operations (Security) that will focus primarily on patching vulnerabilities so that the Council can mitigate and reduce the risk of any potential hacks
- Approval of purchasing a DDoS (Dedicated Denial of Services) solution to protect all external websites that Bradford Council controls. This will stop systems being overloaded with request that are generated by Bots.

6.5 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.

In 2020/21 **275** data security incidents, where personal data had been breached, were reported to the Corporate Information Governance team.

Table 6 below shows a breakdown by type of the **275** personal data breaches recorded in 2020/21

Personal data breaches recorded in 2020/21	**Number**	**%**
Loss or theft of paper or other hard copy data	**4**	**1**
Data posted, e-mailed or faxed to the incorrect recipient or address	**151**	**55**
Loss or theft of equipment on which data is stored	**3**	**1**
Inappropriate sharing or dissemination of data	**60**	**22**
Hacking, malware, data corruption	**1**	**0.33**
Information obtained by deception or "blagging"	**0**	**0**
Equipment failure, fire or flood	**1**	**0.33**
Unescorted visitors accessing data	**1**	**0.33**
Non-secure disposal of data	**0**	**0**
Recordable Incidents	**54**	**20**
TOTAL	**275**	**100%**

The Data Protection Officer took the decision, on behalf of the Council, to refer **9** of the incidents 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.

In response to the **9** referrals from the Council, the ICO concluded that all were low risk and did not

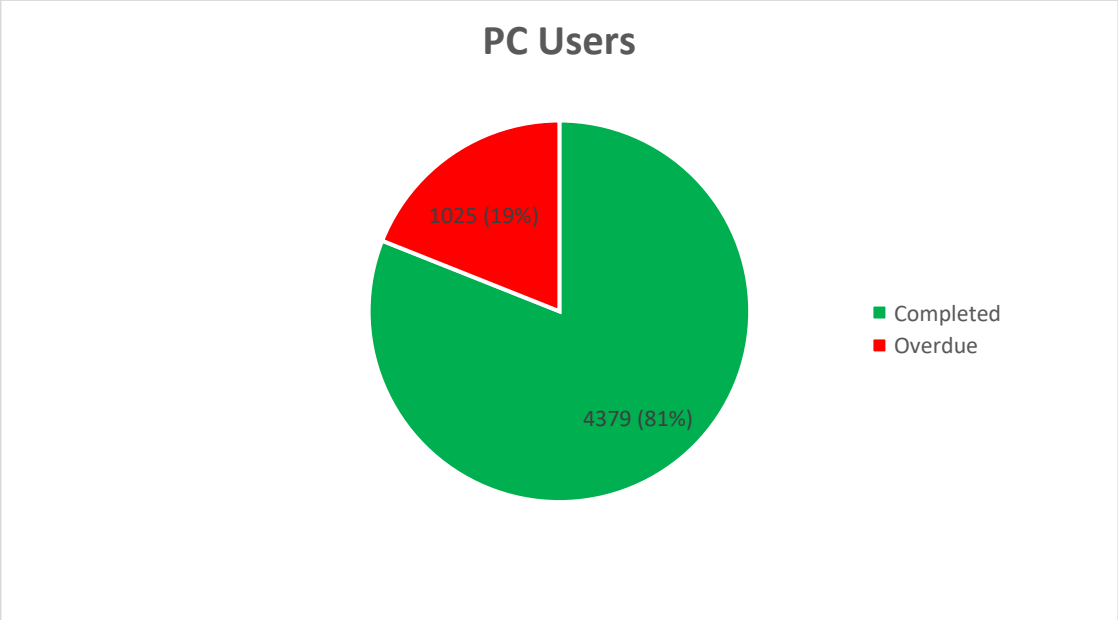
require any formal intervention but the ICO made recommendations about the Council's monitoring of procedures and policy. The following actions were taken as a result:

- A reminder for all staff about the requirements of the Council's Policy on reporting a Data Security Incident
- Reviewing the Council's employee "movers and leavers" process so that access to IT systems can be disabled promptly.
- Changes to Service processes to ensure that information is received by the appropriate party at the correct address.

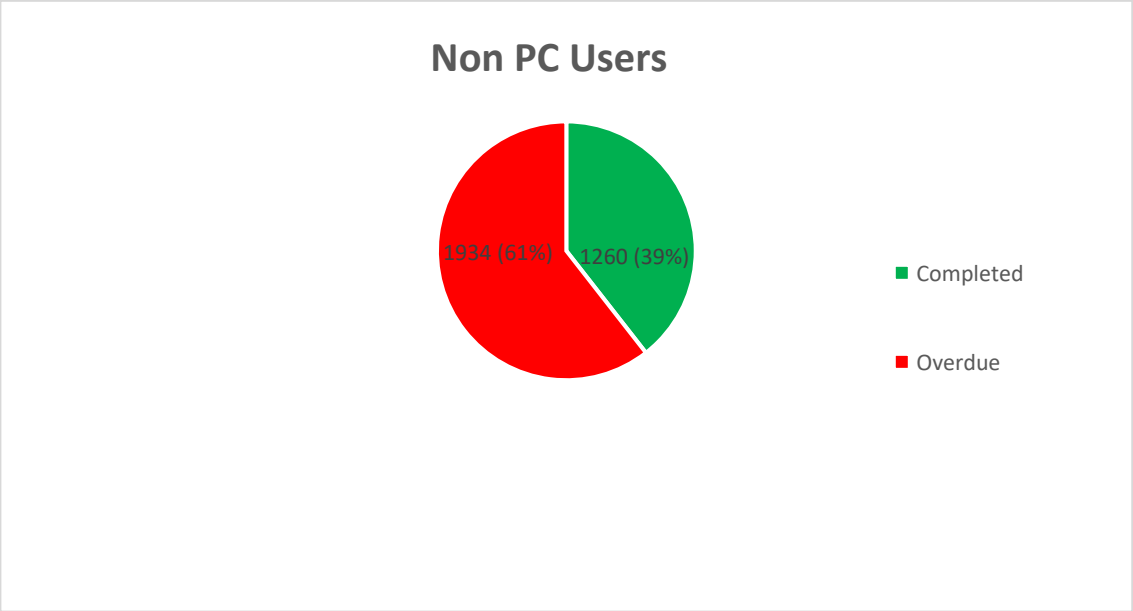
6.6 Protecting Information Training

The Council has a bespoke eLearning mandatory annual training package for all employees of the Council who have access to a PC. 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. Both the eLearning and non-PC leaflet training are currently undergoing a refresh.

Graph 5 below demonstrates the number of PC users who have completed the learning in 2020/21



Graph 6 below demonstrates the number of non PC Users who have completed the learning in 2020/21



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 2020/21 have completed the following key actions to strengthen the Council's management, assurance and governance of information; -

- Produced guidance and arranged a Virtual Training Session for all the Council's Information Asset Owners reinforcing their responsibilities in relation to FOI/EIR and GDPR.
- Refreshed the Information Governance internal website updating the information available for employees
- Introduced new software to assist Council Services to redact, for example, 3rd party information from Subject Access Requests
- Introduced a quality assurance process for all information requests
- Created new online forms to allow Council information to be requested through the Council's external website
- Developed a data sharing process for recording authority wide projects
- Developed specific policies for FOI/EIA and Records Management
- Developed a SharePoint site for Information Asset Registers, DP impact assessments, Data sharing Agreements, Privacy Notices and other resources for Service Champions and IAOs.
- Carried out an audit of DP impact assessments and asset registers
- Delivered DP impact assessment training to employees
- Reviewed and refreshed the Council's Privacy notices

The following actions are progressing or to be progressed in the 2021/22 financial year; -

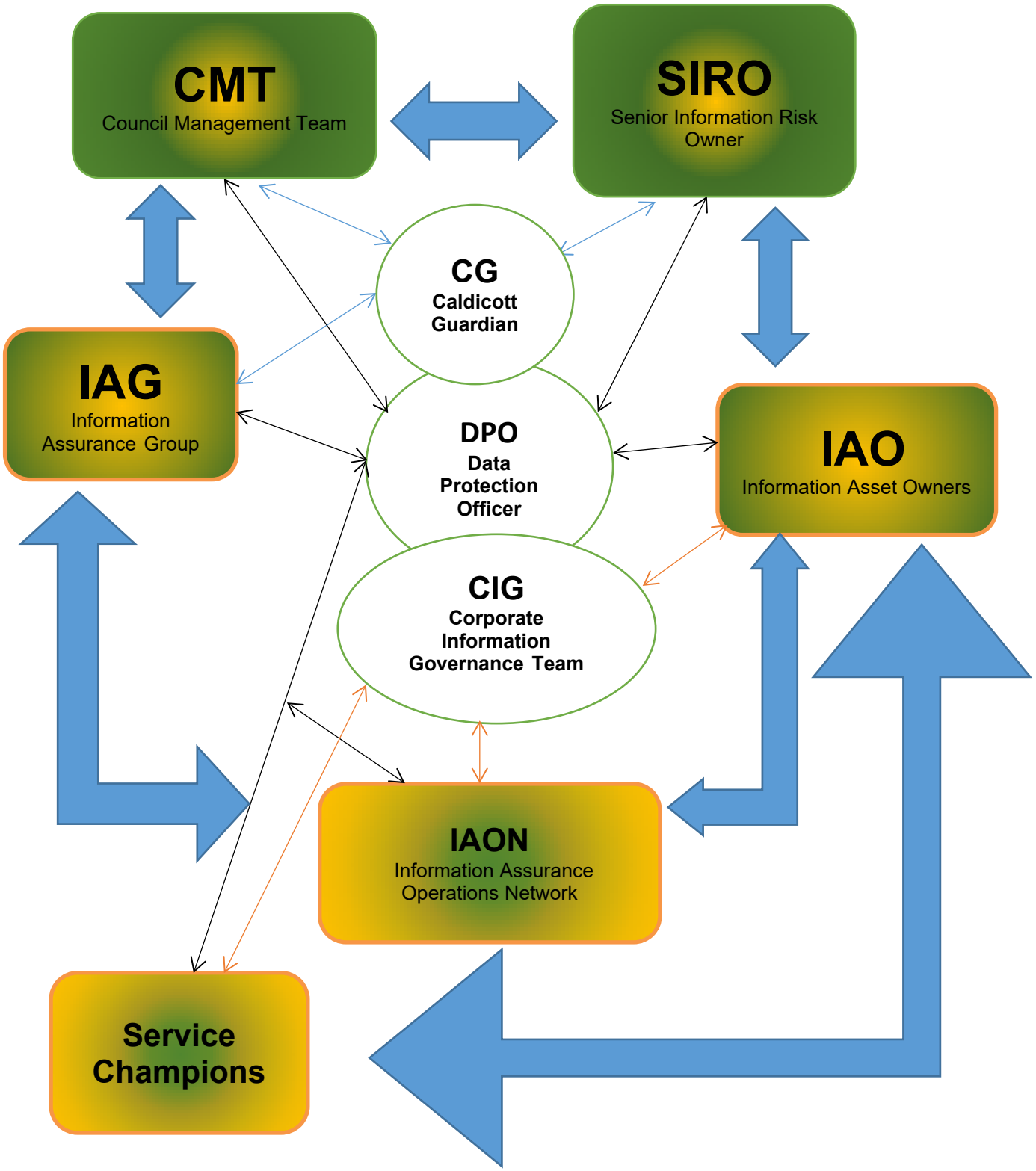
- An online form for reporting data security incidents for the Council's external website
- Implementation of a Civica Document Workflow system for processing Subject Access Requests
- Refresh of the Protecting Information training
- Completion of the ICO Accountability Framework
- Council wide roll out of the IG SharePoint site for IAO's and key officers involved in Information Governance
- 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

8.0 Conclusion

In summary, this report has demonstrated the progress made during 2020/21 in implementing key actions to strengthen and ensure the Council's 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.

Information Management, Assurance & Governance (IMAG) Framework



Appendix 2 - Freedom of Information (FOI) Act and Environmental Information Regulations (EIR) exemptions applied by the Council in 2020/21

Exemption	Times Applied	Type of Exemption
Section 21 - Reasonably Accessible by other means	182	Absolute
Section 22 - Future Publication	11	Qualified
Section 24 - National Security	1	Qualified
Section 29 - The Economy	3	Qualified
Section 31 - Law Enforcement	9	Qualified
Section 36 - Prejudice to effective conduct of public affairs	1	Qualified
Section 38 - Health & Safety	1	Qualified
Section 40 - Personal Information	31	Absolute
Section 41 - Confidentiality	1	Absolute
Section 42 - Legally Privileged	1	Qualified
Section 43 - Commercially Sensitive	13	Qualified
Total	**254**	