City of BRADFORD METROPOLITAN DISTRICT COUNCIL

Report of the Director of Finance & IT to the meeting of the Governance & Audit Committee to be held on 21st January 2021

W

Subject:

Information Governance performance and activity report

Summary statement:

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

Chris Chapman
Director of Finance & IT

Portfolio:

Leader of the Council & Corporate

Report Contact: Tracey Banfield
Head of Corporate Investigation & Information Governance
Phone: (01274) 434794
E-mail: tracey.banfield@bradford.gov.uk

1. SUMMARY

The purpose of this report is to present the information governance performance and activity outcomes 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.

At the beginning of the financial year 2019/20, the Council had a number of information compliance concerns;-

- **Freedom of Information (FOI) and Environment Information (EIR) response rates** were low with only 74% responded to in time
- **Subject Access Request (SAR) response rates** were low with only 69% responded to in time
- **Council governance processes** were not effective, e.g. Compliance rates for mandatory "Protecting Information" training were at 74%
- **Council response to data breaches** was slow and inadequate

The Senior Information Risk Owner report for 2019/20 (shown at Appendix 1) demonstrates how the Council has taken appropriate and timely action to ensure that performance in 2019/20 has improved significantly. Given the key outcomes for Quarter 1 and Quarter 2 of 2020/21 show further improvements this report aims to provide assurance for this Committee that the Council is managing information related matters effectively.

3. OTHER CONSIDERATIONS

As the SIRO report (shown as Appendix 1) contains only information for the financial year ended 31st March 2020 the following table represents a summary of key performance outcome data for Q1 and Q2 of the current financial year 2020/2021 to demonstrate that performance has further improved and to give the Committee assurance that the Council continues to manage information efficiently and effectively.

Table 1

Freedom of Information / Environment Information	2019/20	2020/21 Q1 & Q2
No. of requests received	1767	691
% of Freedom of Information / Environment Information requests	88%	93%

responded to within the statutory timescale		
No. of FOI / EIR referrals to ICO (as a % of received)	13 (0.74%)	2 (0.30%)
No. of ICO decision notices	6	3
Subject Access Requests	**2019/20**	**2020/21 Q1 & Q2**
No. of requests received	386	168
% of subject access requests responded to within the statutory timescale	79%	94%
No. of SAR referrals to ICO (as a % of received)	6 (1.55%)	2 (1.19%)
Data Security Incidents	**2019/20**	**2020/21 Q1 & Q2**
No. of data security incidents, where personal data has been breached	222	147
Breaches reported to the ICO (as a % of total incidents)	12 (19%)	4 (3%)

4. FINANCIAL & RESOURCE APPRAISAL

Compliance with Information Governance / 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 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 fines on organisations for non-compliance with the legislation and also to prosecute individual Council employees for serious breaches of the legislation. Fines for Organisations can be up to a maximum of 20 million euros or 4% of turnover, whichever is the greater.

In the last financial year the ICO imposed fines on two London Borough Council's – Newham were fined £145,000 for unlawfully disclosing the personal information of more than 200 people and Kensington & Chelsea £120,000 for unlawfully publishing details of 943 people who owned empty properties.

Additionally in 2019/20 the ICO prosecuted 2 Council employees for breaches of the legislation – a Town Clerk from Whitchurch Town Council for intentionally blocking records to prevent disclosure and a Reablement Officer at Walsall Metropolitan Borough Council for accessing Social Care records without authorisation. Both were given fines, ordered to pay costs and a victim surcharge was applied.

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 Chief Executives Management Team receives regular updates on the status of information governance related issues and recently approved written guidance and mandatory training for Information Asset Owners.

6. LEGAL APPRAISAL

Data Protection

The Data Protection Act 2018 (DPA) sets out the framework for data protection law in the UK. It sits alongside the General Data Protection Regulation (EU) 2016/679 (GDPR). It sets out the key principles, rights and obligations for most processing of personal data – but it does not apply to processing for law enforcement purposes, or to areas outside EU law such as national security or defence.

The GDPR came into effect on 25 May 2018. As a European Regulation, it has direct effect in UK law and automatically applies in the UK until the end of the transition period 31 December 2020. After this date, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

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 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 EQUALITY & DIVERSITY

There are no equality and diversity implications

7.2 SUSTAINABILITY IMPLICATIONS

There are no sustainability implications

7.3 GREENHOUSE GAS EMISSIONS IMPACTS

None

7.4 COMMUNITY SAFETY IMPLICATIONS

None

7.5 HUMAN RIGHTS ACT

There are no Human Rights implications

7.6 TRADE UNION

There are no trade union issues arising from the contents of this Report.

7.7 WARD IMPLICATIONS

None

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

N/A

7.9 IMPLICATIONS FOR CORPORATE PARENTING

N/A

7.10 ISSUES ARISING FROM PRIVACY IMPACT ASSESSMENT

None

8. NOT FOR PUBLICATION DOCUMENTS

None

9. OPTIONS

N/A

10. RECOMMENDATIONS

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

11. APPENDICES

Appendix 1 – Senior Information Risk Owner (SIRO) Annual Report

12. BACKGROUND DOCUMENTS

Annual Report of the Senior Information Risk Owner (SIRO)

2019 / 2020

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 2020 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 **Chief Executives 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 and is responsible for advising the Chief Executives Management Team (CMT) about information risk and 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, removed, how information is moved, and who has access and why and to be 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 General Data Protection Regulation (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 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 supported by the Heads of Information Governance and IT Services, the Data Protection Officer, the Information Governance Manager and a senior lawyer with experience of information related matters.

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

4.0 Information Access

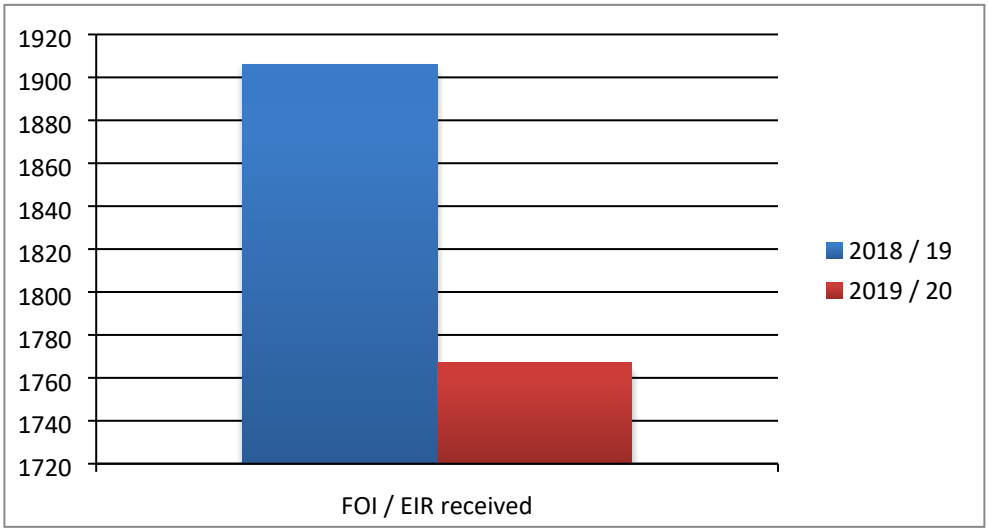
4.1 Freedom of Information / Environment Information

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

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

4.1.1 Provision of the information requested

Graph 1 below demonstrates the number of Freedom of Information and Environment Information requests received in 2019/20 compared with 2018/19



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.

Whilst the Council did apply exemptions during the financial year 2019/20 records of those applied were not maintained however recording of this information is in place for the 2020/21 financial year.

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.

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 the expected time to determine whether the information is held; locate information or appropriate documents; retrieve the information or document containing it; extract the information and process the

request.

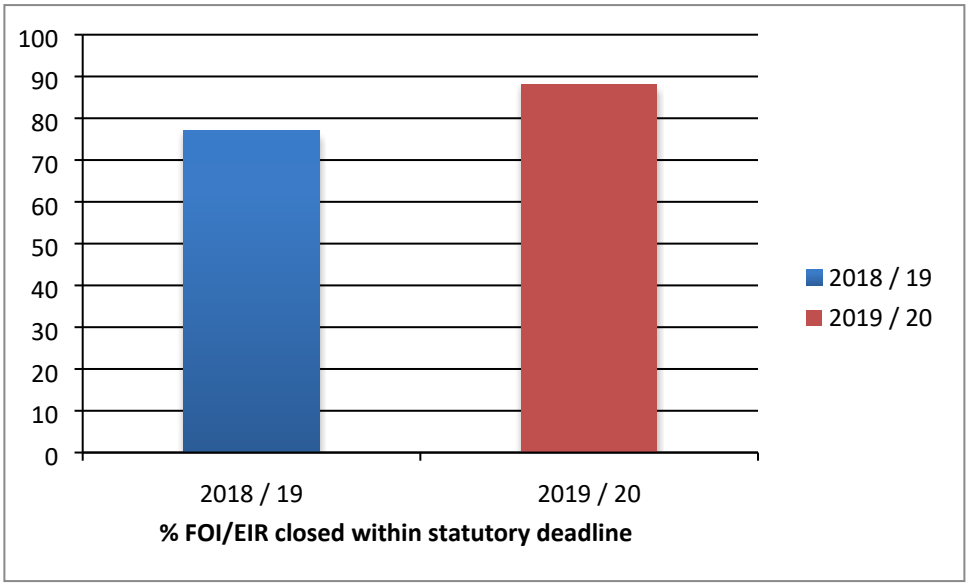
The Council did not apply any charges during 2019/20.

4.1.4 Responses

Requests for information under the Freedom of Information or Environment 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, any extension is only in exceptional circumstances and decisions always taken in conjunction with the Corporate Information Governance team.

In 2019/20 the Council applied an extension to **115** of the requests (6.5% 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 statutory timescale in 2019/20 (88%) compared with 2018/19 (77%)



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

Internal Reviews	**2019/20**	**% of all requests**
Freedom of Information / Environmental Information Regulations	53	3%

4.1.6 Referrals 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 referrals about the way public bodies have handled requests for information.

Referrals are normally made to 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 make recommendations on best practice and in some cases, take enforcement action i.e. issue the Council with a decision notice requiring, for example, that information the Council has previously refused to disclose, be disclosed..

Table 2 below demonstrates the number of FOI/EIR referrals made to the Information Commissioner and the number of cases where a decision notice and/ or recommendations for further action were made.

	2019/20
No. of FOI / EIR referrals to ICO	13
No. of ICO decision notices	6
No. of ICO recommendations	4

Of the 6 decision notices issued by the Information Commissioner 5 were due to a failure by the Council to respond to the requests in the statutory timeframe and 1 for incorrectly applying a "commercial interest" exemption to a request and not supplying the information requested.

The ICO made recommendations to the Council within the 6 decision notices and all were implemented within the 35 day timeframe set by the ICO.

4.1.7 Publishing information proactively

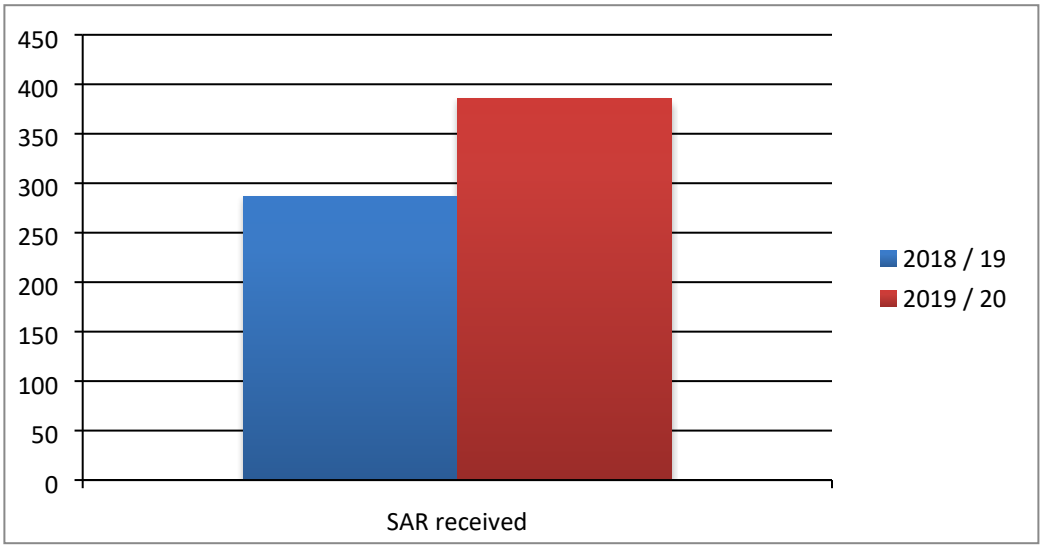
The FOI Act requires every public authority to have a publication scheme approved by the ICO and to publish information covered by the scheme. The Council has adopted the ICO's model publication scheme and this is made available on the Council's website. https://www.bradford.gov.uk/open-data/publication-scheme/publication-scheme/

4.2 Subject Access Requests (SAR)

In accordance with the 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 shows the number of subject access requests received in 2019/20 compared with 2018/19



42% of the subject access requests received in 2019/20 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 2019/20 the Council applied such exemptions but the data on the number of cases where an exemption was applied was not collected. Processes have been amended to now collect this data

4.2.3 Charges

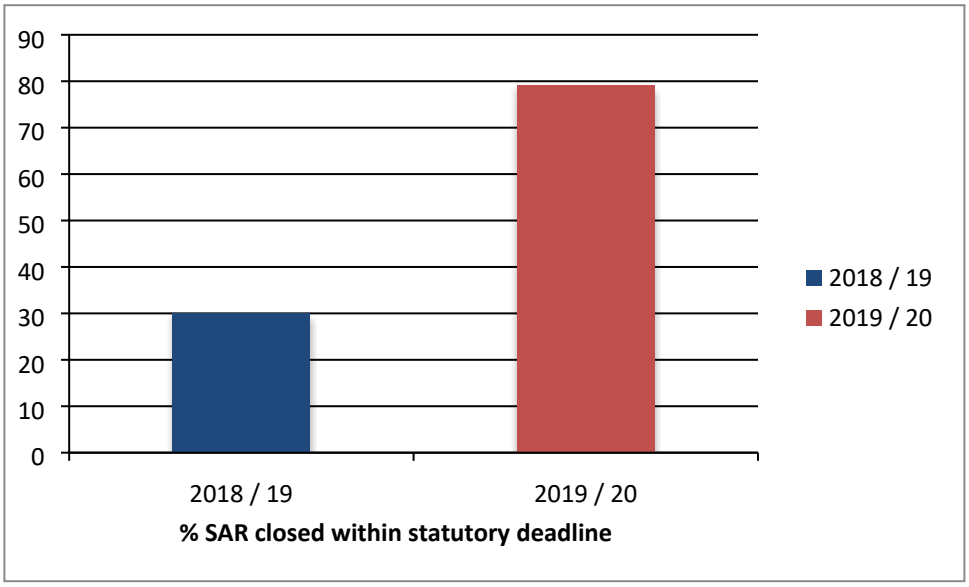
The Council, in accordance with the legislation, does not charge a fee to deal with Subject Access requests.

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 2019/20 the Council applied an extension to **80** of the requests (21% 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 GDPR legislation.

Graph 4 shows the % of subject access requests responded to within the statutory timescale of 1 calendar month compared with 2018/19



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 3 below demonstrates the number of internal reviews processed by the Council

Internal Reviews	**2019/20**	**% of all requests**
Data Protection Act	16	4%

4.2.6 Referrals 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 were not issued any of the above by the ICO during 2019/20.

Table 4 below demonstrates the number of SAR referrals made to the Information Commissioner and the number of cases where follow up actions were requested

	2019/20	**% of all requests**
No. of SAR referrals to ICO	6	2%
No. of ICO requests for follow up action	2	
No. of warnings, reprimands, enforcement notices or penalty notices	0	

Of the 6 referrals made to the ICO – the Council failed to meet the statutory timeframe on 5 of the cases and withheld disclosable information on the other. As a result the ICO requested that the Council provide a satisfactory response in one case and that the Council disclose withheld information on the other.

No formal sanctions were taken against the Council in 2019/20 as a result of these referrals.

5.0 Data Protection (DP) Act 2018 & 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 General Data Protection Act which came into effect on 25th May 2018

5.1 Individual rights under the GDPR

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

- To access their personal data (GDPR Article 15).
- To correct their personal data (GDPR Article 16).
- To erase their personal data (GDPR Article 17).
- To restrict personal data processing about them (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, (GDPR Article 20).
- To object to personal data processing (GDPR Article 21).
- Not be subject to automated decision-making in certain circumstances (GDPR Article 22).

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

In 2019/20 the Council received **386** requests for access under Article 15 of the GDPR (see paragraph 4.2.1) and **4** requests for rectification under Article 16 of the 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 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 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 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 assessed and signed off by the Data Protection Officer. In 2019/20 **19** DPIA's were carried out and signed off 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, 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 2019/20 the Council had **61** data sharing agreements in place.

5.4 Records Management

The Council recognises that effective records management supports effective data governance and

data protection and has recognised that further work is required in this area if the Council is to meet the requirements of the ICO's Accountability Framework in full.

In 2019/20 to improve compliance in this area the Council has taken action as follows and in the current financial year has started the process to recruit to a full time Records Management Officer post ;-

5.4.1 Information Asset Register

The register holds details of all information assets (software and hardware) including asset owners, the location, details of the retention periods 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 2019/20 the Council began to compile comprehensive asset registers which are now completed with the exception of Childrens Services which remains a work in progress. It is anticipated that this will be completed in the current financial year (2020/21).

There were no periodic reviews carried out on asset registers during 2019/20 but these will be scheduled during the current financial year (2020/21).

5.4.2 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, 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 the Council's 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.

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.

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.

.

6.4 Cyber security incident

On the 16th January 2020 the Council lost all public facing web services, smartphone, e-mail services and the vast majority of officer remote access channels for a total of 85 hours due to an attempted hacking of Council systems.

Following this incident key improvements to improve security were identified and have been implemented in the current financial year

- 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 Centre
- Active participation and collaboration with the Yorkshire and Humber Warning Alerts and Response Point (YHWARP) and other WARP colleagues
- New ITIL Change Management Process put in place
- New Storage Infrastructure Environment e.g. Backup snapshot *(specifically protects against malware restoration)*

6.5 Data Security Incident Reporting (Personal Data Breaches)

The 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.

In December 2019 the Council introduced 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.

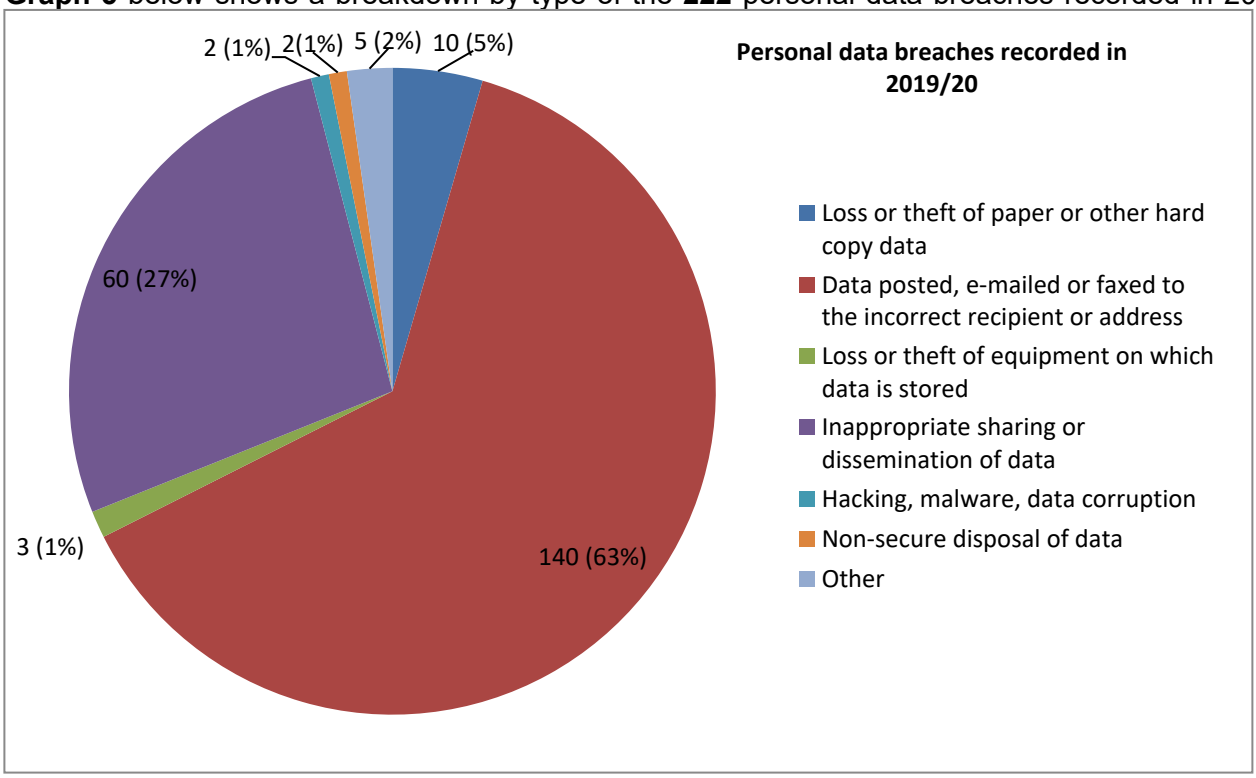
The policy standardises the Council's response to any personal data breach and sets out how the Council will manage reports of suspected data security incidents ensuring that all data security incidents are;-

- 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 2019/20 **222** data security incidents, where personal data had been breached, were reported to the Corporate Information Governance team.

The Data Protection Officer took the decision, on behalf of the Council, to refer **12** 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.

Graph 5 below shows a breakdown by type of the **222** personal data breaches recorded in 2019/20



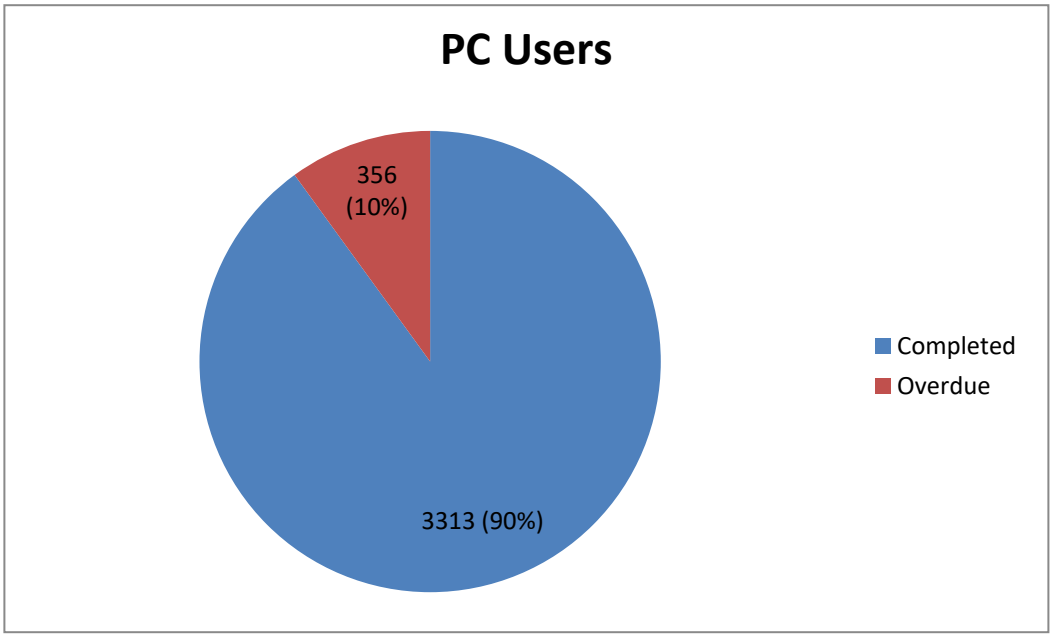
In response to the 12 referrals from the Council, the ICO concluded that all were low risk and did not require any formal intervention but the ICO made recommendations about the Council's monitoring of procedures and policy. The following actions were taken as a result:

- A new policy on Data Security Incidents
- A revised online reporting form with an instruction to Information Asset Owners to ensure all Data Security Incidents are reported to the Corporate IG team within 24 hours of the incident occurring or being discovered.
- Guidance for Investigating Officers on how to respond to an incident
- Relevant Services (with high levels of data being posted or emailed to an incorrect address or recipient) to review their procedures and where appropriate any checking procedures to ensure that the correct details such as the correct name and address is being used on correspondence.
- To use a secure method of postage or secure email or personal delivery collection of any highly sensitive information
- All reports of data security incidents are circulated to Information Asset Owners at least once a quarter and data security incidents are a standing item on IAG agendas.

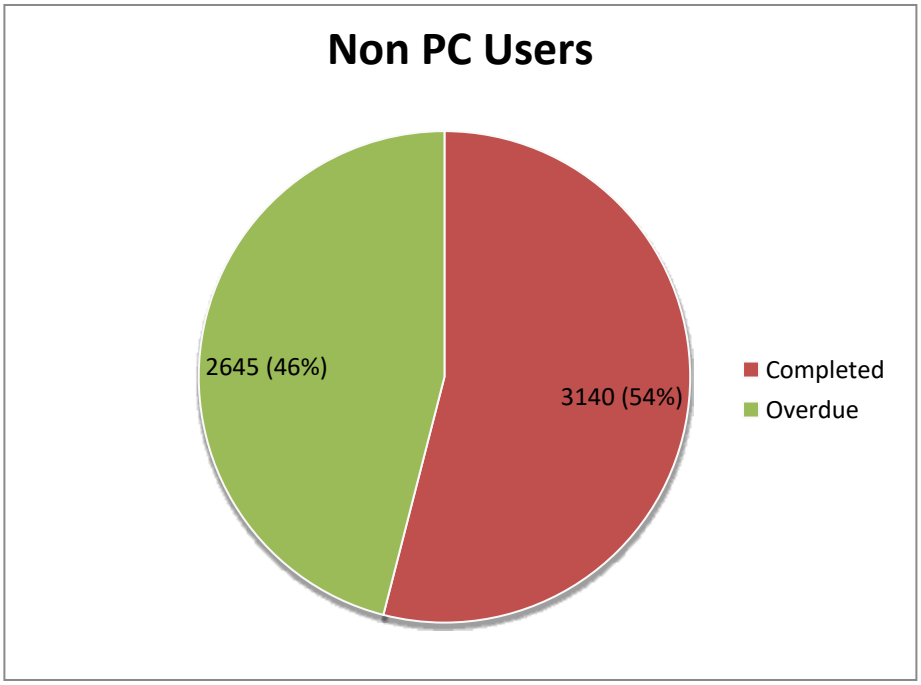
6.6 Protecting Information Training

In 2019/20 the Council launched a bespoke eLearning mandatory annual training package for all employees of the Council who had access to a PC. Later in the year this was followed by a Protecting Information leaflet for all staff without access to a PC.

Graph 6 below demonstrates the number of PC users who have completed the learning in 2019/20



Graph 7 below demonstrates the number of non PC Users who have completed the learning in 2019/20



7.0 Progress against key improvement actions

In 2019/20 The Corporate Information Governance team created a series of action plans to support on going improvement and during the financial year have completed the following key actions to strengthen the Council's management, assurance and governance of information;-

- Updated the Councils external website for requesting CCTV footage and created an online request form
- Introduced a verification process for Subject Access Request

- Developed policies on Data Security Incidents, Handling Data Subject Requests
- Improved work processes introduced for risk assessing Data Security Incidents
- Produced staff guidance on handling Freedom of Information requests, Environmental Information requests, Subject Access Requests, Reporting Data Security Incidents, Investigating Data Security Incidents, risk assessing Data Security Incidents, completing a Data Protection Impact Assessment
- Development and implementation of a Civica Document Workflow system for Freedom of Information & Environmental requests and Data Security Incidents
- Creation of an “Information Governance Matters” Newsletter for all Council employees

The following actions are progressing or to be progressed in the 2020/21 financial year;-

- Review and redesign of Information Governance internal and external website offerings
- Procurement of Redaction software to assist with Subject Access Requests
- Review of the quality and accuracy of responses to information requests
- Creation of new online forms to enable a more efficient process to request information through the Council’s external website
- Develop a data sharing process for recording authority wide projects
- Develop a specific FOI/EIA Policy
- Development of SharePoint site for Information Asset Registers, DP impact assessments and Data sharing Agreements
- Development of SharePoint site for Service Champions communication and updates
- Audit of DP impact assessments and asset registers
- Develop an online form for reporting data security incidents for the Council’s external website
- Recruitment of a new Records Management Officer for the Council
- DP impact assessment training for IT Services – Will be rolled out across the council in 21/22
- Development and implementation of a Civica Document Workflow system for processing Subject Access Requests
- Training for Information Asset Owners on their responsibilities in relation to FOI/EIR and GDPR.

8.0 Conclusion

In summary, this report has demonstrated the progress made during 2019-20 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.

Appendix 1

Information Management, Assurance & Governance (IMAG) Framework