INFORMATION GOVERNANCE
SENIOR INFORMATION RISK OWNER ANNUAL REPORT
APRIL 2019 – MARCH 2020

1. Purpose

This report provides an overview of Wiltshire Council's adherence to regulatory requirements relating to the processing of personal identifiable data under the General Data Protection Regulation and the Data Protection Act 2018 and its duty to be transparent through its compliance with the Freedom of Information Act 2000.

It ensures that the Council's Corporate Leadership Team (CLT) and Cabinet are advised of the most significant current and emerging Information Governance (IG) issues and the measures being taken by the organisation to ensure it meets the national and mandatory standards.

Specifically, this report will:

- Outline activity and performance related to information governance during the 2019/2020 financial year.
- Document organisational compliance with the regulatory requirements relating to the handling of information and provide assurance of ongoing improvement in relation to managing risks to information.
- Provide a status update on the Data Security and Protection Toolkit (DSPT).
- Detail how data incidents have been handled, including the learning from incidents.
- Review compliance with IG mandatory e-learning training.
- Give an overview of key achievements in 2019/2020.
- Priorities for IG going forward in 2020/2021.

It is important to understand that information is an organisational asset and that a strong information governance culture enables the Council to operate lawfully, efficiently and effectively.

2. Introduction

As with any project or programme, it is crucial to have an executive sponsor at board level to support, to champion the effort, to secure the resources and to execute the strategic plan.

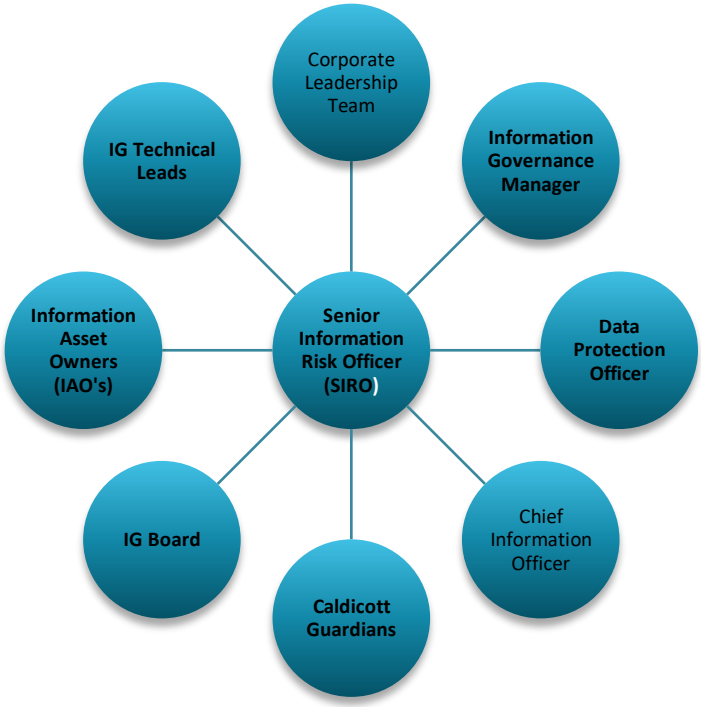
The SIRO, as part of his portfolio, understands how the strategic business goals of the organisation may be impacted by information risks.

The SIRO provides an essential role in ensuring that identified information security risks are followed up and incidents managed and has ownership of the Information Risk Policy, Risk Management Strategy and associated processes. He provides leadership and guidance to Information Asset Owners.

The SIRO's responsibilities can be summarised as:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its residents.
- To maintain sufficient knowledge and experience of the organisation's business goals with emphasis on the use of and dependency upon internal and external information assets.
- To act as the focal point for information risk management in the organisation including resolution of any escalated risk issues raised by the Information Governance Manager, the Data Protection Officer and Information Asset Owners.

Diagram of SIRO Relationships with officers across the Council



In the 2019/2020 reporting year and previous years, the Senior Information Risk Officer (SIRO) has been the Director of Corporate Resources. For the 2020/2021 reporting period, the SIRO role will transfer over to the Director for Legal and Governance.

3. Physical Records Storage

The contract with Iron Mountain has now been running since 2016 and teams have fully engaged with the IM Connect web portal when requesting or returning files from the storage facility in Kemble. As referred to in the last report, records are delivered to and collected from service teams' areas within the hubs, ensuring a secure chain of custody is maintained.

The IG team continues to monitor the activity and associated costs in maintaining the volume of physical storage. The current position is that we have 33,485 boxes in storage which equates to 38,847.59 cubic feet, costing £ 5,827 at £0.15 per cubic foot. There has been a small reduction in storage capacity from last year when the figure was 38,901.49 cubic feet.

It is important that services actively review their storage requirements and ensure that if the information can be stored electronically, is no longer current, relevant or required for statutory reasons, that they take steps to arrange for the destruction of those records.

Part of the ongoing work for the IG team will be to work with services to define their ongoing storage requirements and challenge the need to continue to produce paper. Effective management of the Council's physical records supports the drive to migrate paper-based processes on line as set out in the Council's digital strategy and will contribute to cost savings.

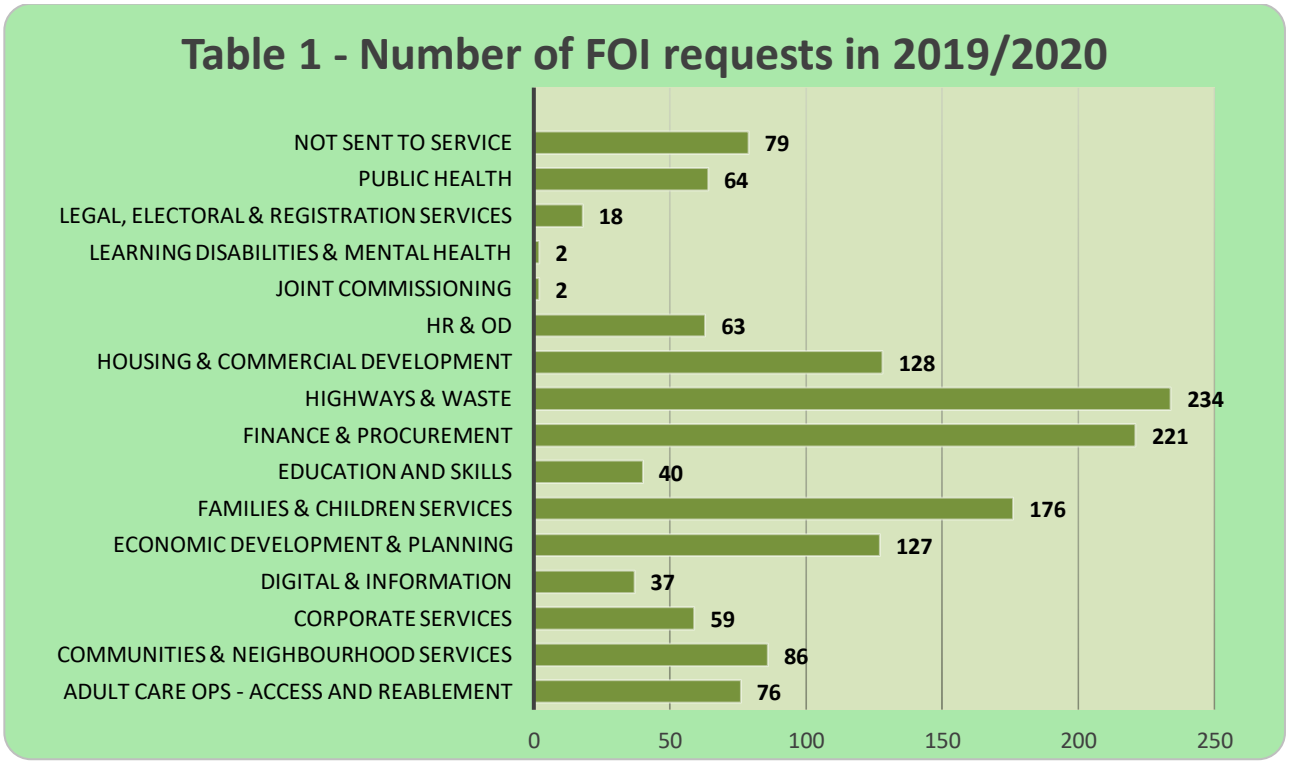
4. Requests Under Freedom of Information and Environmental Information Regulations

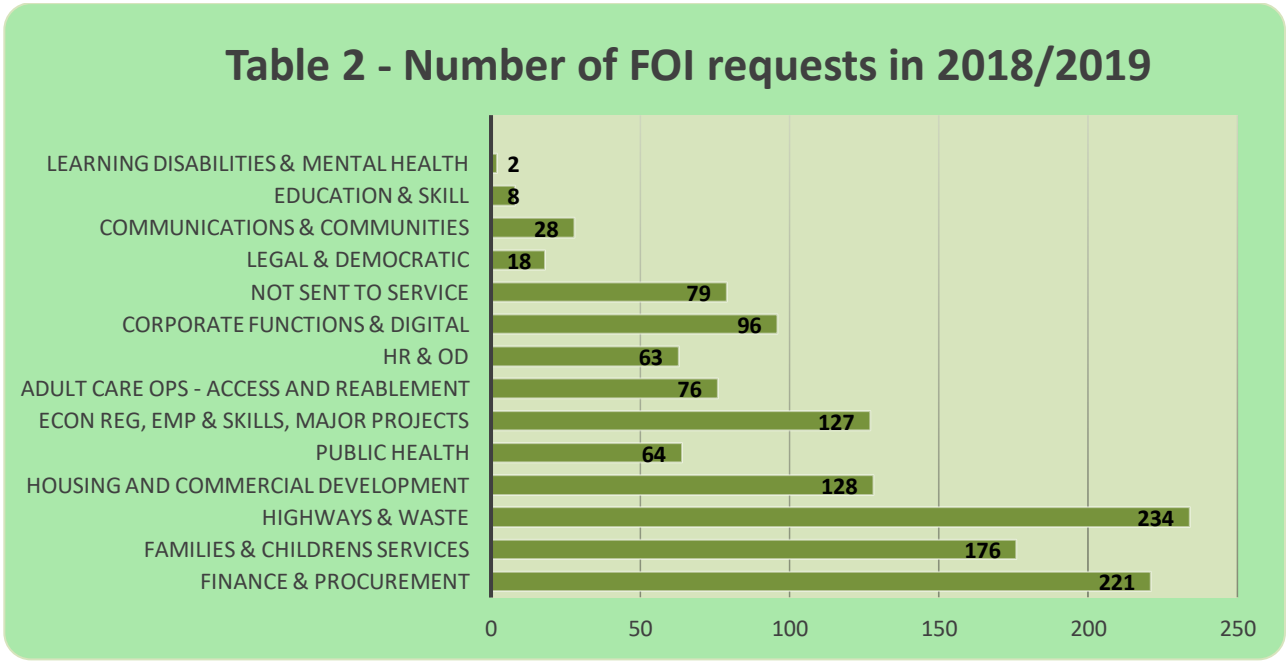
The table below shows the number of FOI and EIR requests received by the Council for 2019/2020. In comparison to last year, the total has decreased by 22% from 1,818 in 2018/2019**.** The most significant reduction in requests came in March 2020 which is believed to be because of the Covid-19 pandemic.

FOI and EIR requests 2019/20	Number of requests received	% of responses within 20 working days	Number of requests where information was granted	Number of requests where information was refused	Number of internal reviews	Number of complaints to the ICO
Apr	124	99%	98	8	3	1
May	127	93%	92	16	4	0
Jun	116	89%	77	15	1	0
Jul	143	98%	104	22	2	0
Aug	108	98%	88	7	3	1
Sep	91	95%	68	12	1	1
Oct	116	98%	83	20	1	0
Nov	124	91%	93	9	2	0
Dec	91	93%	67	8	1	1
Jan	151	97%	115	13	3	0
Feb	148	96%	114	17	4	0
Mar	73	98%	53	6	2	1
Total	1412	96%	1052	153	27	5

Of the total 1,412 requests received, 96% were responded to within the statutory time limit of 20 working days compared to 98% in the previous reporting period.

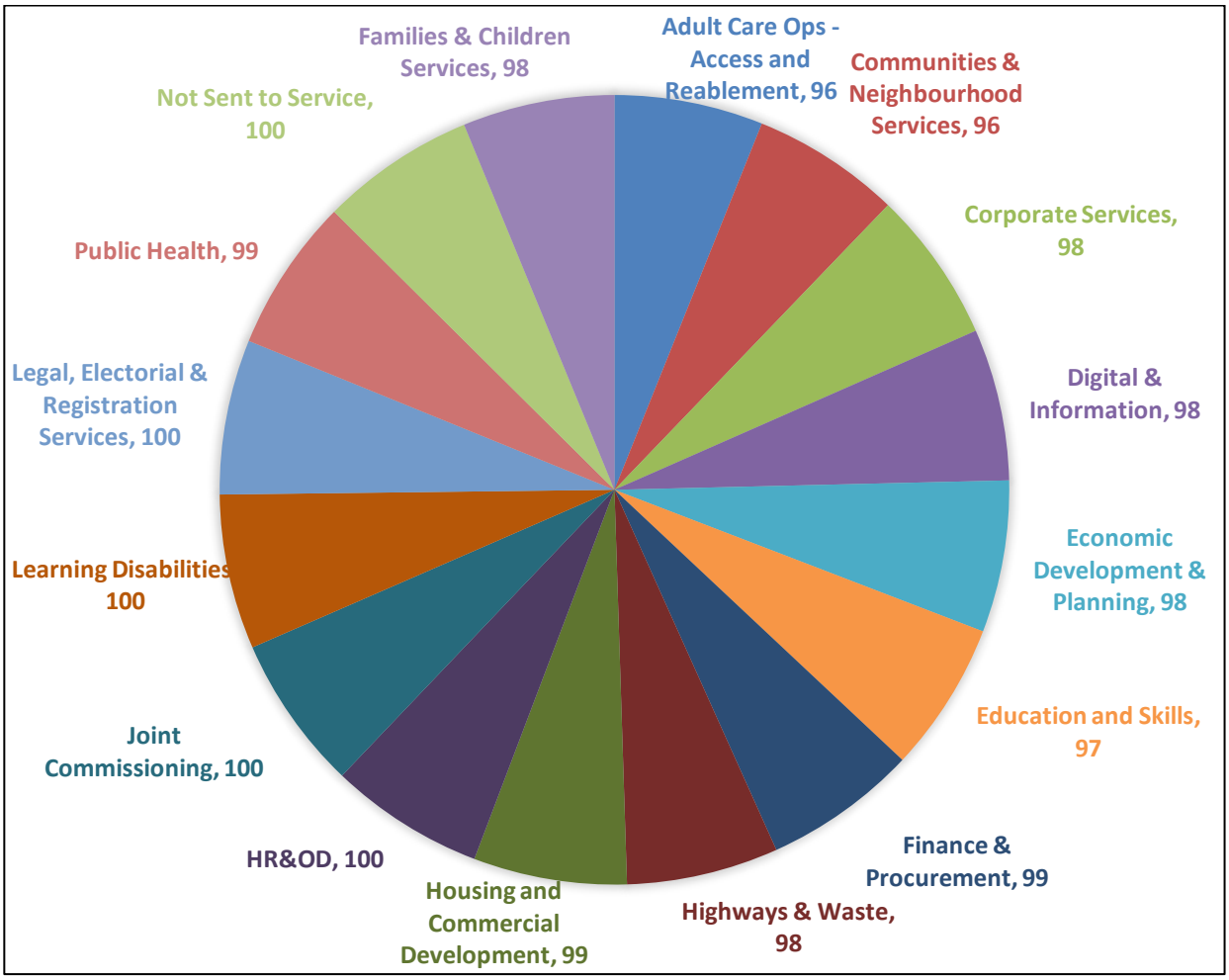
Table 1 and 2 below shows, by service team, the number of requests received. The second table shows the percentage of those requests that were dealt with within the 20-working day statutory timescale.





In terms of identifiable patterns or trends, there is nothing significant. The nature and number of requests are spread out across the organisation. Those service teams dealing with high numbers of requests are ones where we would expect there to be a high level of demand for information.

The pie chart below shows the percentage of responses met within the 20-day statutory deadline, under each directorate.



5. Publication of Information

Information over and above that defined by the publication scheme and the Local Government Transparency Code continues to be published to the Council's website adding to the wide range of material available to the public without the need to make a request to the Council.

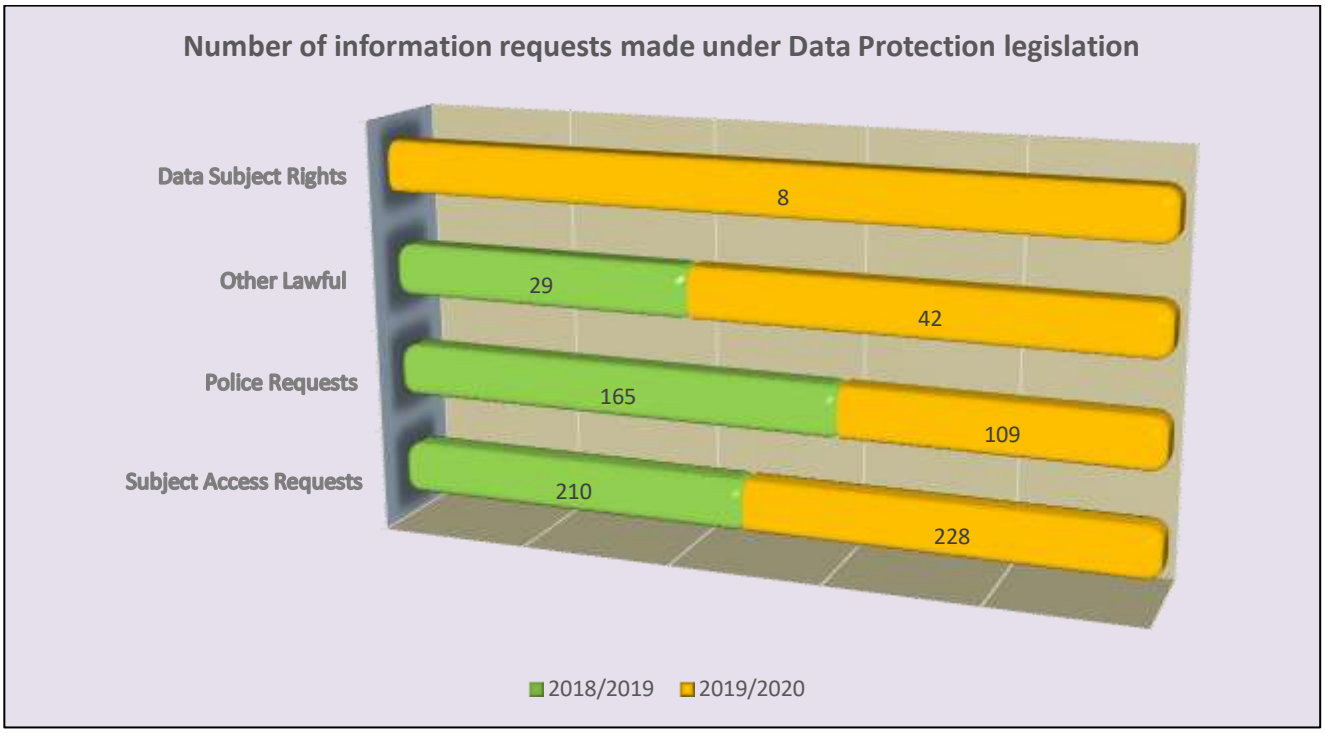
The FoI pages contain a list of standard responses to some of the most frequently submitted requests meaning that service areas no longer need to deal with a proportion of requests as the IG team can signpost requestors to the FAQ's which satisfies the legislation.

Work is ongoing with Services which receive repeat requests for the same or similar information, (e.g. Revenues and Benefits in respect of business rates), to pro-actively publish bulk information on a regular basis removing the need to respond to individual requests as they are received. This type of publication aims to reduce the pressure on Services involved in the recording and processing of requests for information.

In addition to the disclosure log which lists all FoI requests received during the preceding two years a new statistical report, which meets the ICO's expected standards of reporting is published to the website.

6. Requests for information made under Data Protection legislation

The following table shows the number of Subject Access Requests (SAR) made under Data Protection legislation, which were received by the Council for the reporting year. Percentage of SAR on time 91% with an average response time 21 days.



Subject Access requests, which are requests from individuals for their personal information, remain the core of casework. In comparison to last year numbers they have remained at a similar level. Police requests are slightly down, and other lawful requests slightly up. A new statistic gathered this year is the category of accessing other data rights such as rectification, deletion or cessation of processing.

There were eight such requests this year dealt with by the Data Protection Officer. In the majority of such cases the issue is disagreement with report and assessment content that cannot be determined as inaccuracies and the most appropriate course of action is to add to the data subject's records that they disagree with the specific content.

7. Internal Reviews, Self-referrals & complaints raised to the Information Commissioner's Office

In the reporting period, Council interaction with the Information Commissioner's Office (ICO) has differed from last year with four self-referrals for suspected serious breaches, and a further two incidents relating to the actions of a member of staff. The four self-referrals were made in June 2019, October 2019 and two in December 2019. The two incidents related to staff actions were made in September 2019 and November 2019.

In respect of the self-referrals, three were closed by the ICO with the issuing of appropriate recommendations and no punitive action. These recommendations are being implemented across the relevant service and wider where it is applicable.

One referral was considered as more serious and resulted in a formal reprimand which led to an action plan and working group to implement it under the direction of the SIRO, which has now been completed. In the reporting period, the Council's Data Protection Officer has received two letters of concern from the ICO where data subjects have referred their dissatisfaction with our service for them to investigate. The ICO has been satisfied with the Council's compliance in both cases.

8. Changes to legislation during reporting period

There have been no significant changes to primary legislation in the reporting period. We continue to learn how the new regulatory landscape regarding data protection integrates with other activity. We also continue to monitor and share where necessary, guidance and developments that are circulated by the ICO.

Towards the end of this reporting period, the COVID-19 pandemic impacted on normal working practices. Legislation and working practices have developed to facilitate the exchange and sharing of personal data in support of dealing with the emergency. The Council's Data Protection Officer (DPO) and IG Team have been actively engaged in drafting sharing agreements in support of the Council's business activities at this time.

Prior to the current emergency, it has been the intention of the DPO this year to focus on developing tools and conducting internal audits of compliance; and developing Records of Processing Activity (ROPA) which are the most significant area of outstanding compliance work. These have for the time being been put on hold but will be resurrected once recovery is underway.

9. Data Security and Protection Toolkit

Organisations such as Wiltshire Council that process and share NHS patient data and systems are required to satisfy the online self-assessment tool to provide assurance that good data security monitoring is in place and that personal information is handled correctly. Performance will be measured against the National Data Guardian's 10 data security standards.

The normal submission date is the 31st March each year. However, due to the COVID-19 pandemic impacting shortly beforehand NHS Digital advised that the submission date would be extended to September 2020.

10. Information Security/Cyber Security

The perception and understanding of Information Security – or Cyber Security – has changed considerably over the last two years, with organisations like the National Cyber Security Centre (NCSC) and the Ministry of Housing, Communities and Local Government (MHCLG) leading the way with guidance, training and action plans aimed specifically at organisations such as the Council.

The events which took place in Salisbury and Amesbury, incidents like the "WannaCry" attack on the NHS, and the cyber-attack on Copeland Borough Council have not only been high profile cases in the mainstream news and media, but they have focused the thinking and planning that organisations must now give to the threat of a cyber security attack.

During 2019, the Head of Service and Information Assurance and Monitoring Lead worked with colleagues from the Cabinet Office, NHS, and other local authorities to assist MHCLG in developing the course content for the Pathfinder series of Cyber-Security training which has been provided nationally.

Prior to the Covid-19 lockdown, the Government had agreed to provide a further year of training, and it is recommended that relevant colleagues from across the council attend to broaden the scope of this new approach across the Council. This will build on the very successful cyber training event that was held on 16th January 2020.

This training delivers several key messages, which are in line with National Cyber Security Centre (NCSC) guidance. These messages underpin the Council's approach to Cyber Security and helped to inform the planned publicity and awareness campaigns which were due to start in March.

Key points include:

- Have strong defences – wherever possible, prevent attacks reaching our information or employees. Nowadays many attacks are literally impossible for a person to detect, so ease the burden on staff and provide as much automatic protection as possible.

- Empower employees by creating a no blame culture of reporting. Colleagues should be encouraged to share their concerns and seek advice.

- Good information governance equals good cyber security – each element reduces the overall risk to information security. The information asset register identifies what information processing is critical for the Council to function. Good disposal means you only retain what you need; good information security means you know who should have access, and when.

- Ensure Business Continuity Plans consider cyber incidents, not just fire and flood – know how to work differently with limited resources and tools and ensure a cohesive approach across the Council.

- Cyber Security is not just ICT's responsibility – good recovery is about Heads of Service using their knowledge of their information and systems and working with ICT, IG and Emergency Planning to be as well-prepared as is realistically possible.

IG has collaborated with other teams on a broad range of projects and programmes across the Council, working to ensure that information security and regulatory compliance is maintained as new and more efficient ways of working are introduced.

This has included:

- Working with the procurement team on a new approach to the tendering process;

- Attendance at the Technology Authority Board to provide advice on information governance issues and risks before new assets are purchased;

- Working with colleagues in ICT and the Programme Office to ensure that information security and cyber security considerations are addressed in the early stages of a project, in line with legislation and ICO expectations. Whilst this approach has ensured proper mitigation and management of information governance risks on many projects, it has also led to an increase in demand on IG resources.

We must strive to meet the changing cyber-security requirements as they appear on the horizon to protect the Council and its residents from cyber attacks and data incidents.

11. Information sharing requests

Wiltshire Council manages a variety of information assets which are essential for service delivery. The council has a statutory requirement to ensure that its information systems and supporting processes meet security, confidentiality, data protection and data quality needs.

The Council has established and embedded a formal mechanism via its Information Asset Change Policy and its Information Sharing Policy, which provides assurance that all the above requirements have been considered for any new or re-configured asset system or business process.

In this reporting period the IG team has received 33 change requests from teams who are purchasing or developing new systems. There were 31 received in 2018/2019.

The team have also received 35 SharePoint Online Collaboration site requests. These are requests by Services who have a requirement to share information with internal colleagues and/or external third parties. There were 5 received in the 2018/2019.

12. Data Incidents

There is a very small increase in the number of incidents reported, with a total of 331 reports this year, compared to 314 in the previous period.

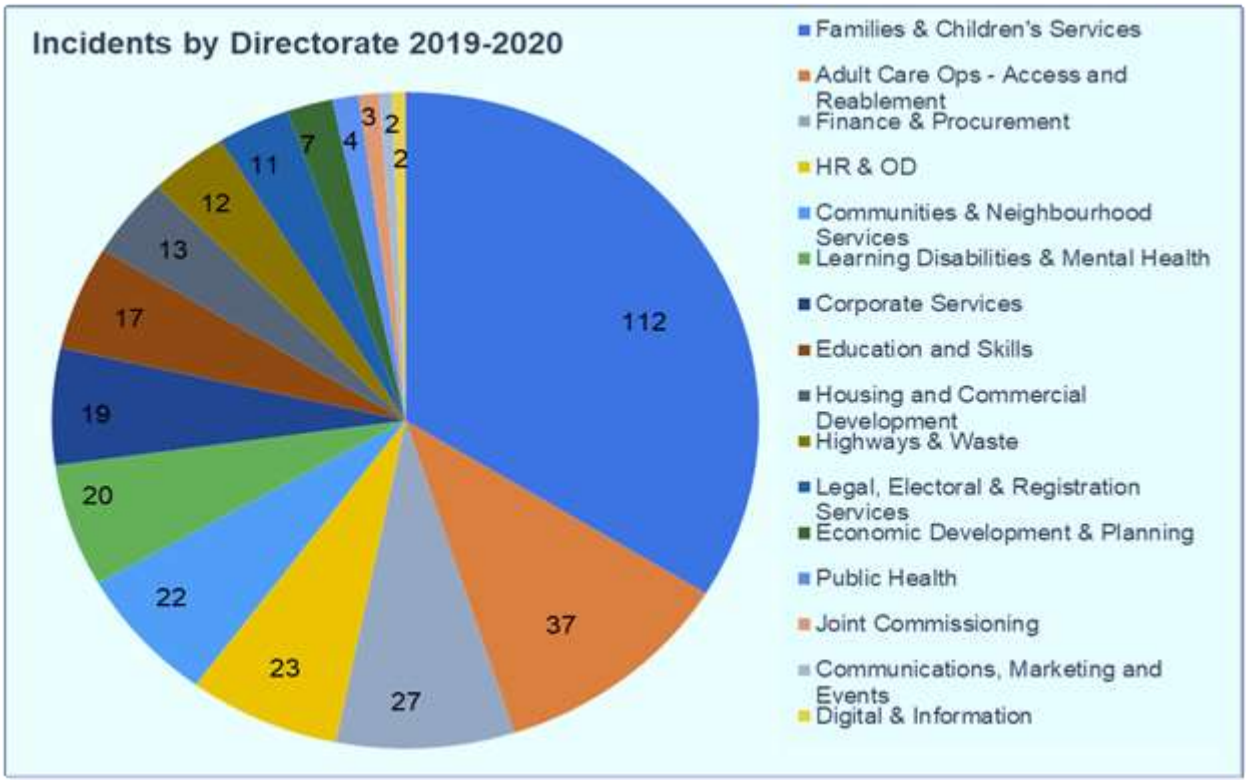
Despite the similarity in the overall figure, we believe this would have been higher if it were not for the implementation of a number of tools and measures which improve our overall cyber-security and ease some of the burden on colleagues.

IG have worked with the organisation to create a supportive culture around incident management, to ensure colleagues are not afraid to report incidents, and this is reflected in the figures we see reported each year.

Incidents by Directorate area shows little change to the areas which report the highest number of incidents (FACT, Adult Care, Finance and Procurement, and HR&OD) and this reflects the nature of the work undertaken by these areas.

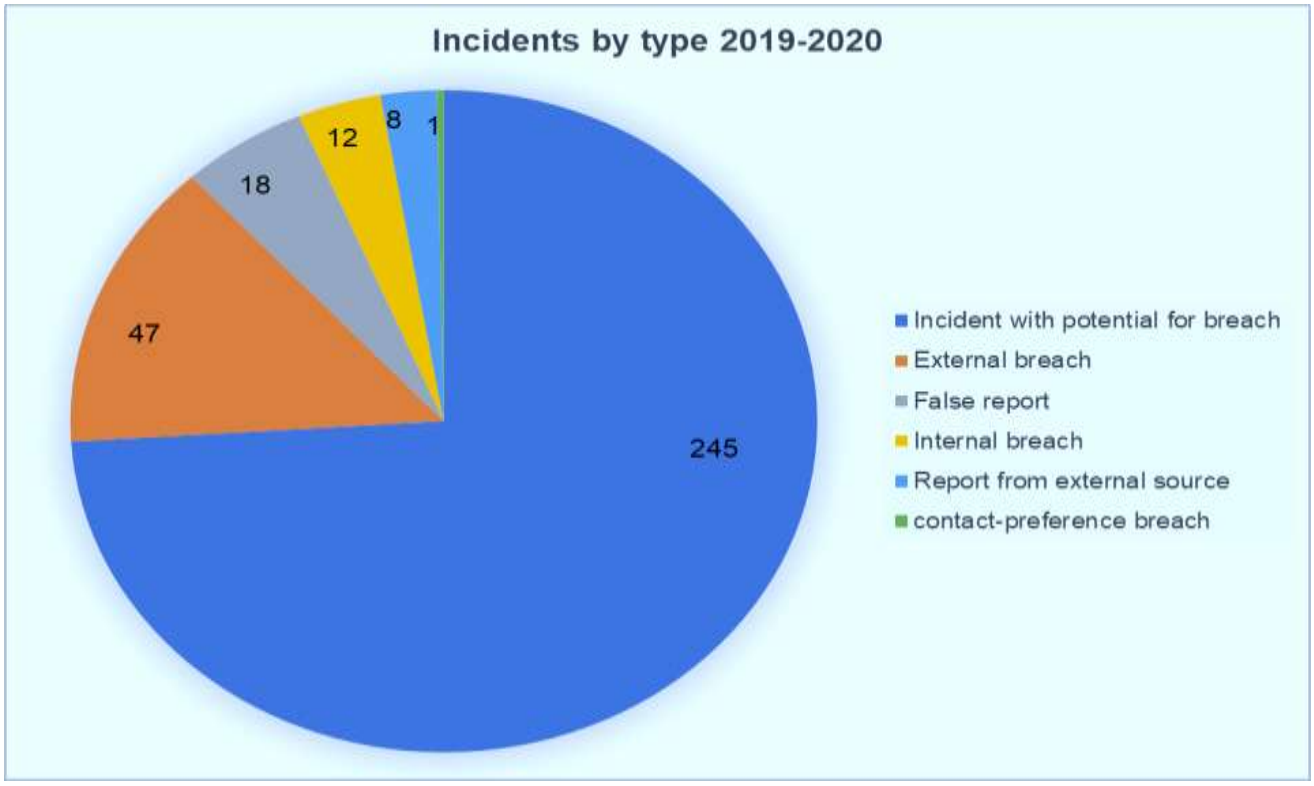
Following a number of incidents over the reporting period, the Council was subject to a reprimand from the ICO. IG worked with Directors and Service Areas to implement a variety of changes. This includes managers carrying out formal investigations with their staff if a data incident occurs. IG have developed a training package which can be delivered ad-hoc to services. This is now being rolled out as part of the standard induction package for new Council employees.

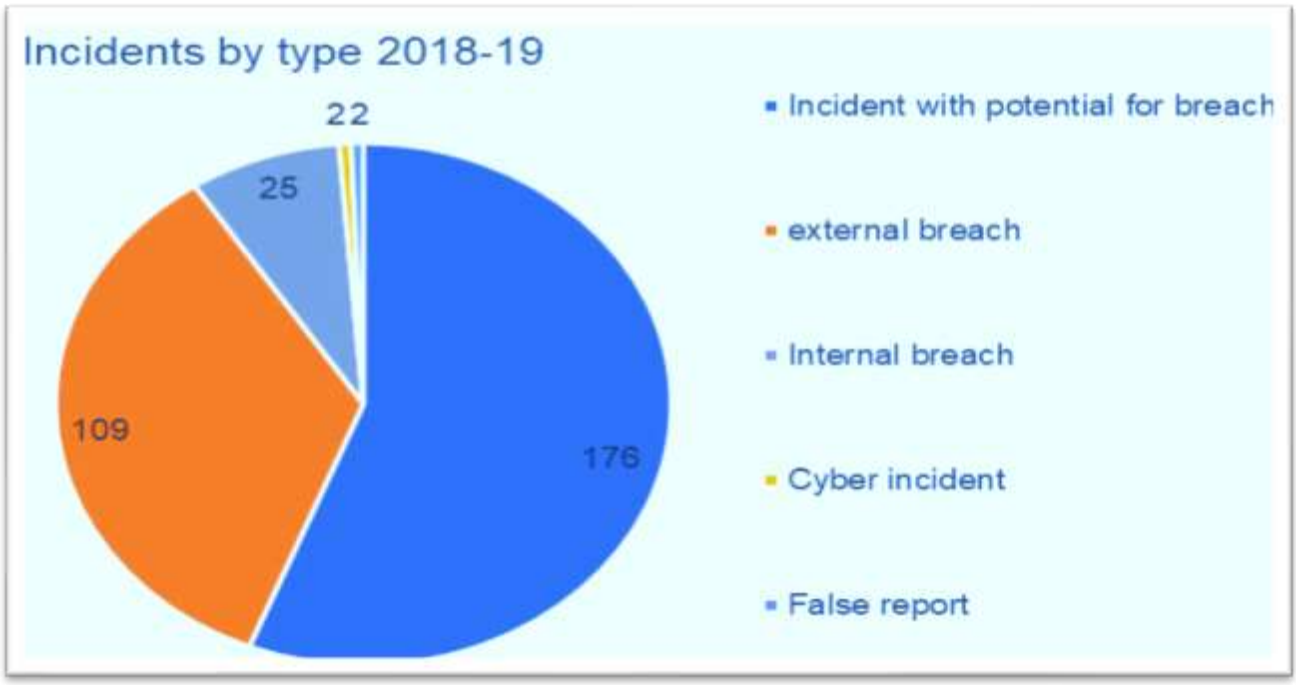
It is imperative that services continue to develop and improve their processes around managing information and work with IG to continue to embed the practices and protocols required.

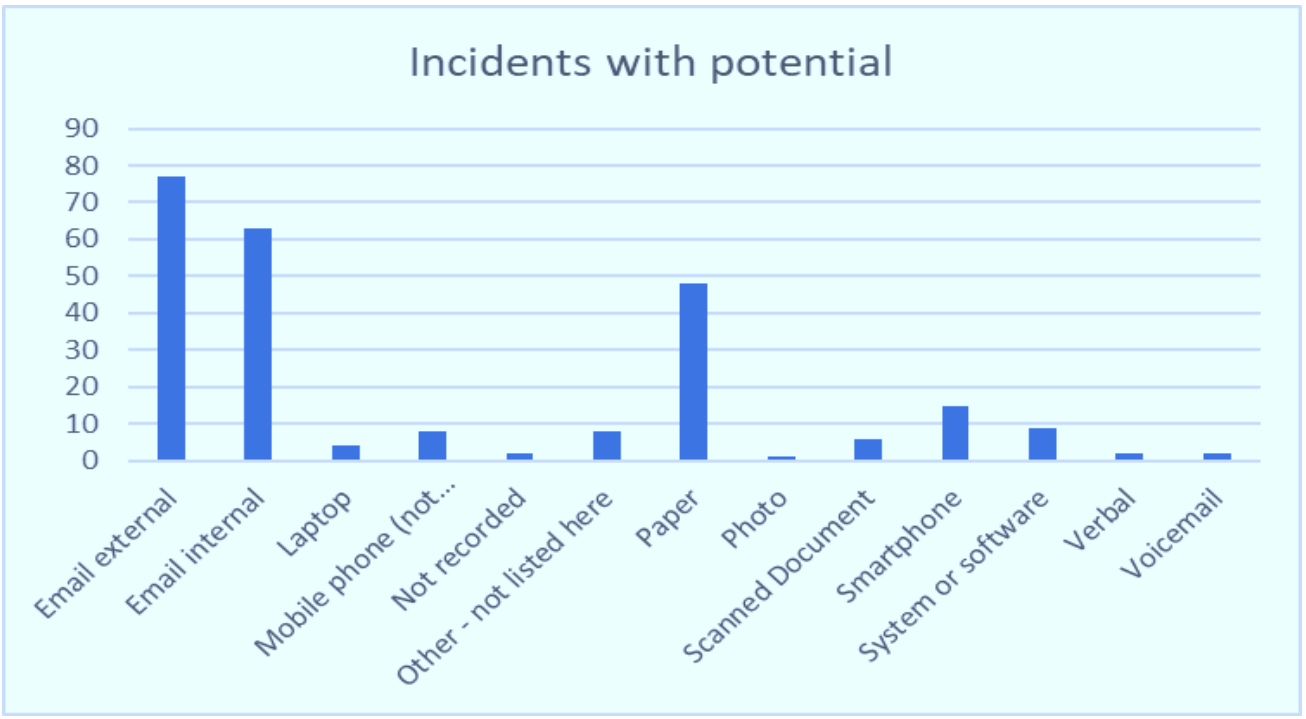


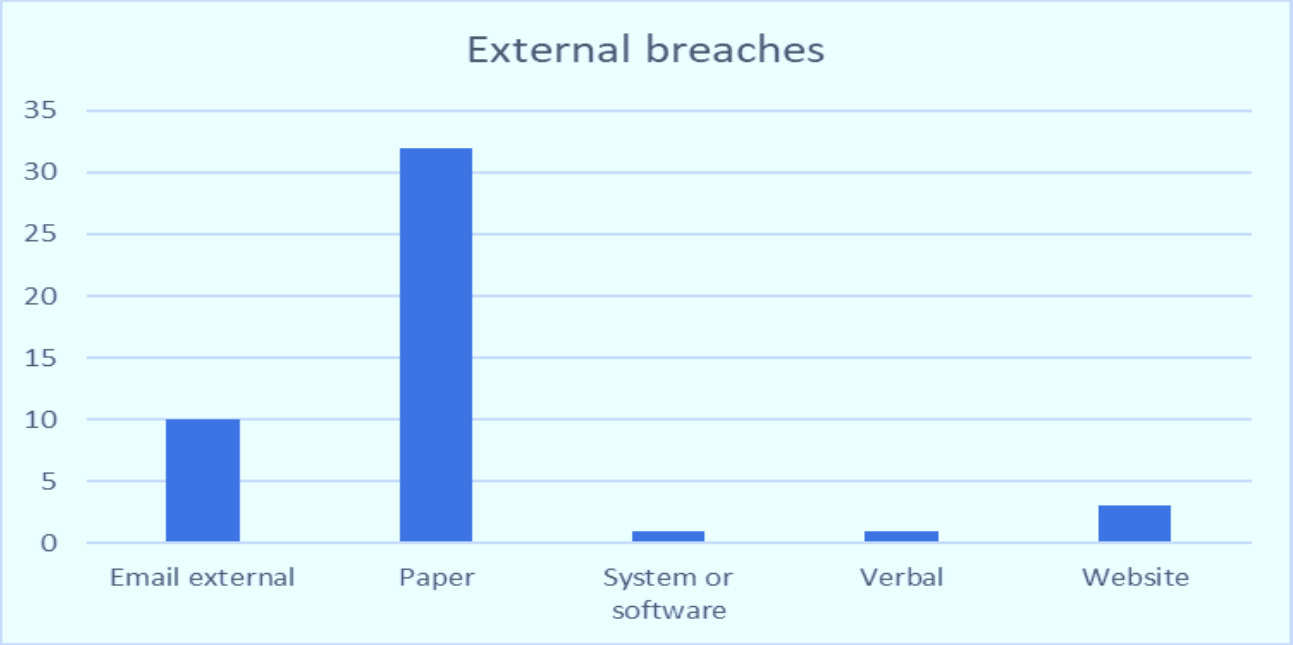
Figures for the previous year are included as a comparison, although there are some changes in directorates because of restructures that have taken place.

Please see Incidents by Type for the periods 2019-2020, with 2018-2019 included for comparison, below. Although most of our reports again relate to “incidents with potential for breach” we have seen some differences in incident details.




Incidents by type 2018-19
22
25
109
176
Incident with potential for breach
external breach
Internal breach
Cyber incident
False report


Incidents with potential
90
80
70
60
50
40
30
20
10
0
Email external
Email internal
Laptop
Mobile phone (not...
Not recorded
Other - not listed here
Paper
Photo
Scanned Document
Smartphone
System or software
Verbal
Voicemail



13. Data Incident Analysis

Incidents with potential are breaches where no information was sent that personally identified individuals or consisted of special category details but was still incorrectly processed or shared.

Incidents with potential for breach have increased whilst external breaches have decreased. We are now seeing the result of changes like secure email which were predicted in the previous report. So, although we may be sending wrong information, or sending information to the wrong people, the likelihood of that information being sent securely has increased (as more organisations like schools improve their email security) – and that is a factor in how we mitigate the potential severity of an incident.

Incidents where we sent information to the wrong person, or indeed sent out the wrong information, account for 67% of all incidents with potential. They also make up almost 90% of our more serious external breaches, including those referred to the ICO.

The biggest factor for external breaches was information being shared inappropriately, where 30 out of 32 incidents relate to paper copies of information being posted.

Incorrect addresses are a factor in many incidents. This is due to a mix of service users changing address without advising us, as well as processes not working correctly, and relevant records not being updated appropriately. This has resulted in two complaints to the ICO.

We continue to use tools like Data Leak Protection (DLP) and e-discovery to audit our use of tools like email, SharePoint Online and – very soon – Teams to identify areas for improvement, or in line with disciplinary concerns.

14. E-Learning Programme and Raising Awareness

IG training compliance was made a priority in this reporting period, and a target of 95% was set in accordance with the requirements of the Data Security and Protection Toolkit.

At the end of the reporting year (31st March) the completion stats were that 67.3% of staff had completed all 4 e-learning modules. A further 10.8% had completed one or more of the e-learning modules, which left 21.9% of staff who had not been able to complete any of the e-learning modules.

Although completion targets have not been achieved, significant efforts have been made to promote and encourage engagement with the training and this will continue.

As well as the e-learning modules, the IG team delivered training sessions to over 200 Children's Service staff on information security and information sharing specifically around their service area. This was done in collaboration with the Head of Service for Support and Safeguarding, to ensure a consistent message and that staff understood the importance of attending the sessions. For the most part these sessions were received positively and raised a number of points for further consideration and reflection.

Members of the IG team also attended several team meetings to speak on a range of subjects. This engagement with different service teams reinforced the messages both within the e-learning and the advice and support IG are able to provide.

The IG team continues to work with the organisation to highlight the importance of all staff, managers and elected members being aware of their responsibilities when it comes to managing information.

15. Information Governance response to the Covid-19 crisis

Towards the end of this reporting period, the country was placed in lockdown due to the Covid-19 pandemic.

The ICO provided clear updates about the ways we might need to work differently under lockdown conditions. NHS has also provided updated information to employees. Within the Council guidance was provided on the most appropriate communication channels to use during this period. For example, it was decided that 'Zoom' should not be used to conduct Council business.

A SharePoint Online Collaboration site is being used to manage Covid-19 response information.

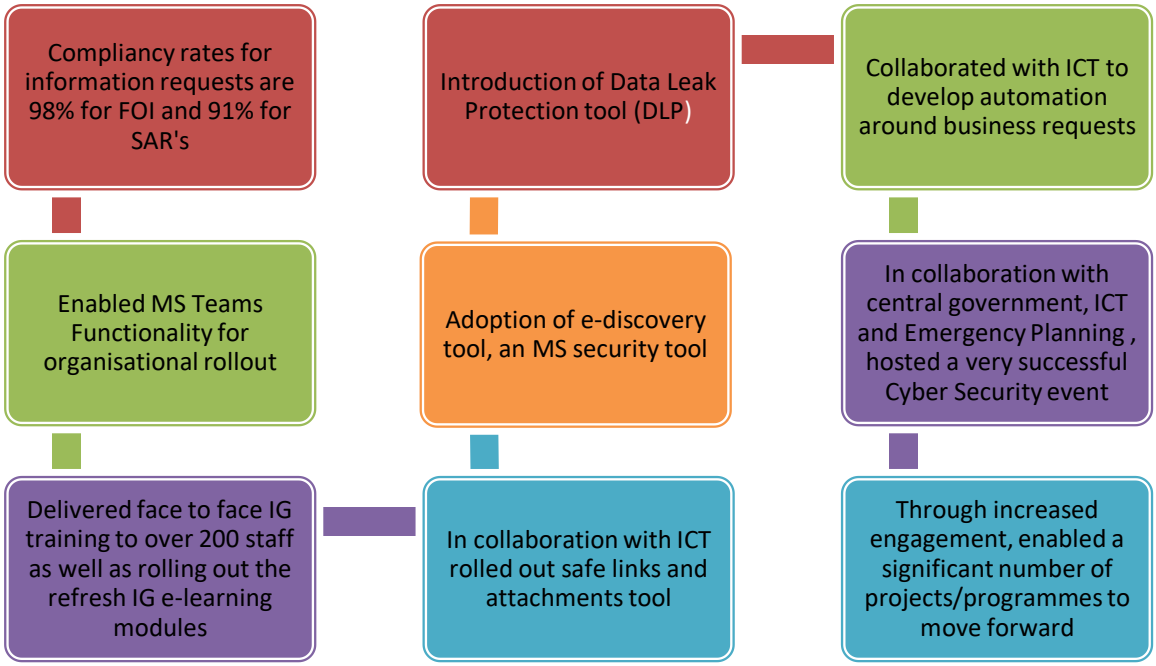
MS Teams has been introduced successfully with most staff being able to use Teams instead of Skype, which reduces our bandwidth usage. We are currently working with HR&OD to understand and respond to all usage scenarios.

Live Events in Teams was enabled for Democratic Services to deliver council meetings virtually putting us in a good place to be able to use that solution in a variety of scenarios to enable "face to face" events to take place. This will be rolled out further for other committee meetings and Area Boards in September.

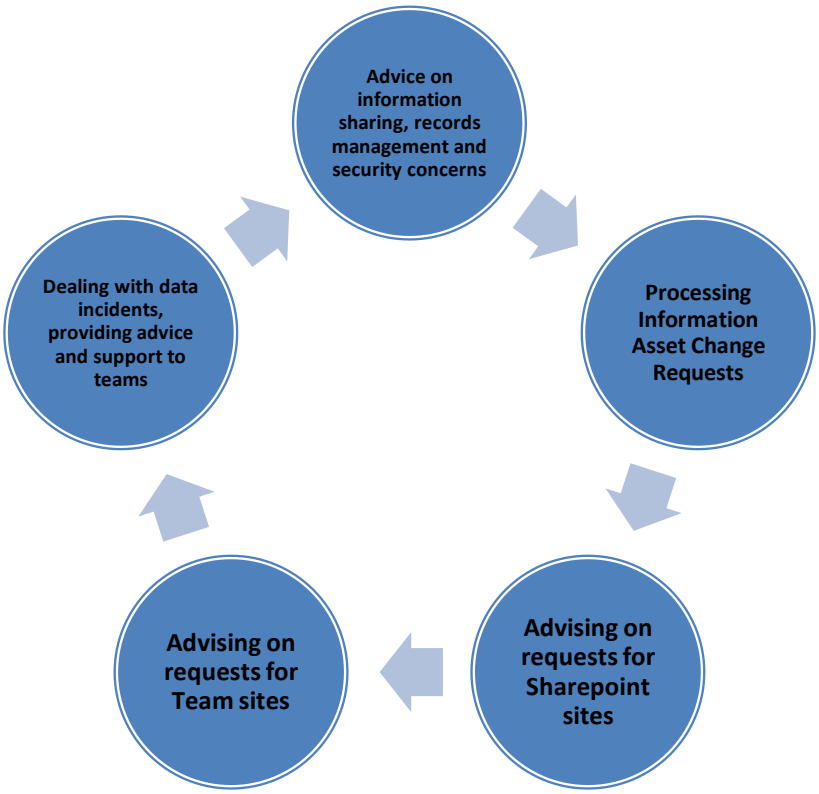
We continue to receive a higher than usual number of queries and concerns around information security and data protection. On average, this Council receives 595,000 spam emails per month. Within those emails is a variety of content, some of which would have a significant impact if not blocked. We receive a high number of cyber-attack attempts throughout the year and, as has been well documented in the media, this threat increases during an event like a pandemic. With this increase in threat level, and the likelihood that we will roll out new tools and ways of working at pace, it is even more vital that the council remains vigilant and meets cyber-security requirements by early engagement with IG.

16. Key achievements

These include:



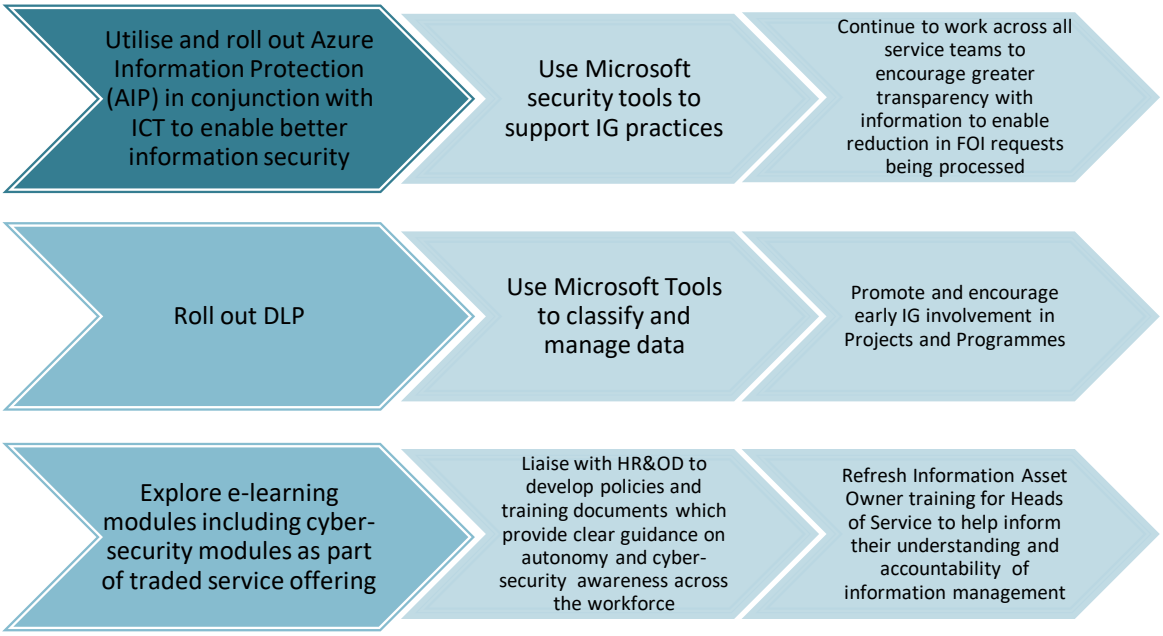
In addition the team's work includes:



Special thanks to the IG team for their work and commitment over the last year in this challenging area of the business.

17. Looking Forward

There is a large portfolio of work that Information Governance will be taking forward in the next reporting period. The IG team will be focusing on the following priorities:



IG will also have a significant role in the recovery phase of the COVID-19 pandemic, particularly in supporting the internal recovery theme.

18. Summary

Good information governance is essential for the efficient and effective delivery of the Council's business and open and transparent decision making. Everyone has an important part to play in achieving this and the IG team will continue to work with Members and officers internally and partners externally to this end.

Ian Gibbons, Director, Legal and Governance and SIRO

15 July 2020

Report Author: Sarah Butler, Information Governance Manager

Email**:** sarah.butler@wiltshire.gov.uk Tel: 01225 718446