Wiltshire Council
Where everybody matters

INFORMATION GOVERNANCE
SENIOR INFORMATION RISK OWNER ANNUAL REPORT
APRIL 2018 – MARCH 2019

1. Purpose

This report provides an overview of the current Information Governance status including compliance with key standards and a report on data incidents. It ensures that CLT and Cabinet are advised of the most significant current and emerging Information Governance issues and the measures being taken by the Authority to ensure it meets the national and mandatory standards.

Specifically, this report will:

- Provide an update relating to the responsibilities of the Council's Senior Information Risk Owner (SIRO).
- Outlines activity and performance related to information governance during the 2018/2019 financial year
- Documents organisational compliance with the legislative and regulatory requirements relating to the handling of information and provide assurance of ongoing improvement in relation to managing risks to information. This includes:
    - the General Data Protection Regulation 2016 (EU Regulation 2016/679)
    - Data Protection Act 2018
    - the Freedom of Information Act 2000
    - the Information Security Standard ISO/IEC 27002:2007
    - Data Security and Protection Toolkit
- Detail any Serious Incidents Requiring Investigation (SIRI) within the preceding twelve months, relating to any losses of personal data or breaches of confidentiality.

It also asks the reader to reflect and consider the real risks and challenges being presented to this organisation daily. Good information governance must be embedded as part of the Council's culture and only the understanding and engagement from managers, staff and elected members will achieve this.

ICT security and cyber risks present a real and increasing threat to all organisations and is not something that can drop down the priority list. The ability to deliver services depends on the ability to have safe systems and reliable information.

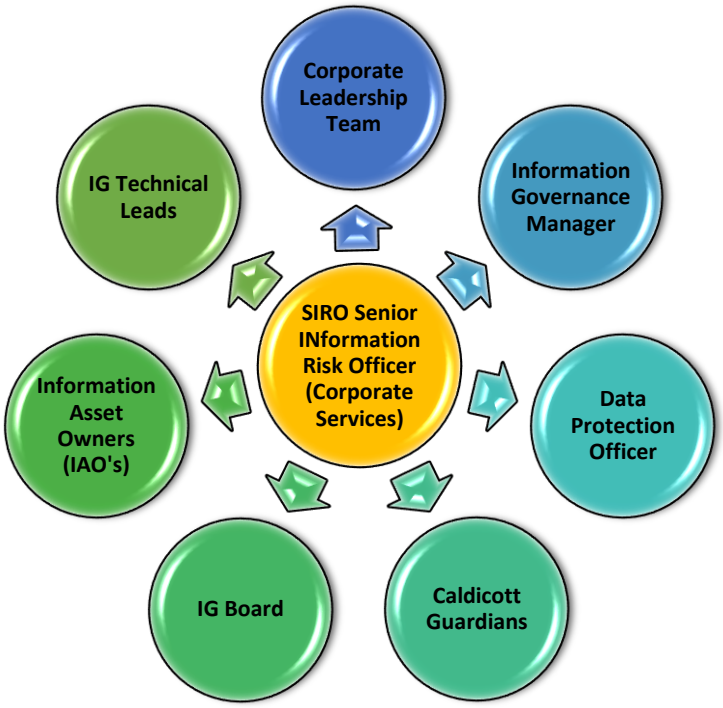
2. Introduction

It is the role of the SIRO to be responsible for and take ownership of, the Council's information risk processes together with advocating at the appropriate Board level, for the reduction of information risk by ensuring effective use of resource, commitment and appropriate communication to all staff, managers and elected members.

By working alongside the Cabinet, Corporate Leadership Team, the Information Governance Team, ICT and other key stakeholders, the SIRO aims to create a culture in which information is valued as an asset and information risk is managed in a realistic and effective manner.

Information Governance relates to all information in whatever medium it is held. However, as the Council embraces digital ways of collecting and managing information, it is important to ensure that there is robust governance in place so that the Council remains compliant, legal and that progress and achievements are not undermined or damaged by poor IG practices.

Diagram of SIRO Relationships with officers across the Council



It is vital that the SIRO engages with the above stakeholders across the Council, to ensure a "golden thread" of good Information Governance combined with the corporate oversight.

3. Physical Records Storage

The contract with Iron Mountain has now been running since 2017 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 33,612 boxes in storage which equates to 38,901.49 cubic feet. We are charged £0.15 per cubic foot. There has been no significant change in storage capacity from last year when the figure was 38,918.15.

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 not 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 both their ongoing storage requirements and the need to continue to produce paper. The less the council can do of both supports the drive to migrate paper-based processes on line set out in the council's digital strategy and will contribute to cost savings over time.

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 2018/2019. In comparison to last year, the total has increased by 21% from 1,495 in 2017/2018**.**

FOI and EIR requests 2018/19	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	155	99%	117	43	0	0
May	161	95%	120	33	5	0
Jun	148	99%	126	26	0	0
Jul	165	98%	119	19	1	1
Aug	153	98%	108	10	5	0
Sep	143	98%	95	20	3	0
Oct	148	99%	101	36	8	1
Nov	154	98%	108	40	1	1
Dec	80	95%	59	16	2	2
Jan	188	99%	125	48	0	0
Feb	145	99%	110	44	5	0
Mar	178	99%	121	57	3	0
Total	**1818**	**98%**	**1309**	**392**	**33**	**5**

Of the total 1,818 requests received, 98% were responded to within the legal compliance time of 20 working days compared to 97% in the previous reporting period.

The data shown in Table 1 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.

Table 1 - Number of FOI requests

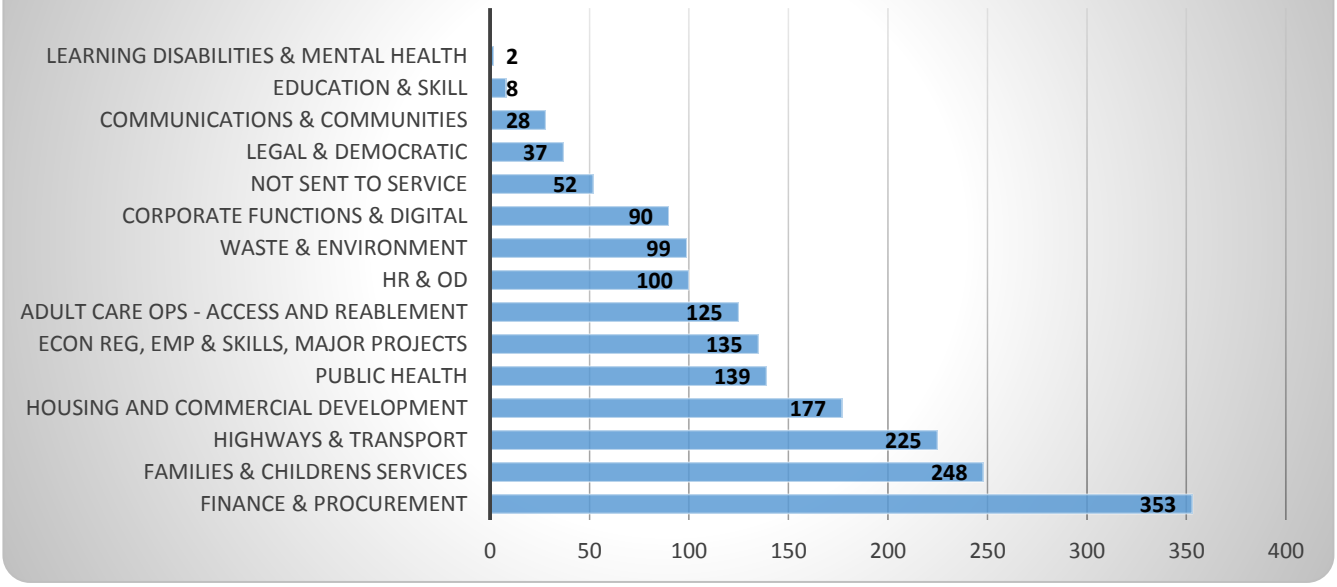
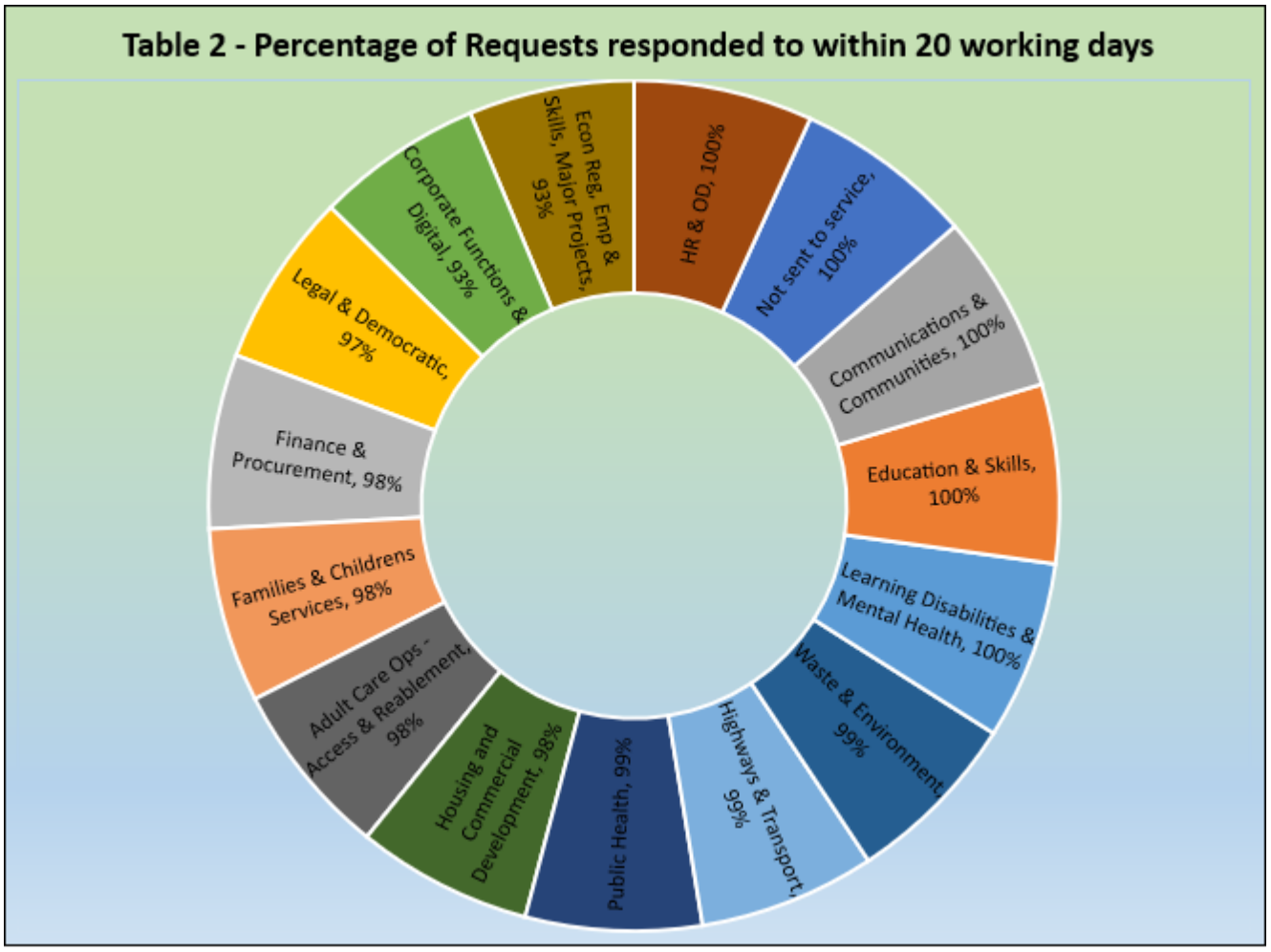


Table 2 - Percentage of Requests responded to within 20 working days



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.

5. Publication of Information

Following on from the work undertaken during the previous reporting period, information over and above that defined by the publication scheme and the Local Government Transparency Code, has been progressively added to the council website.

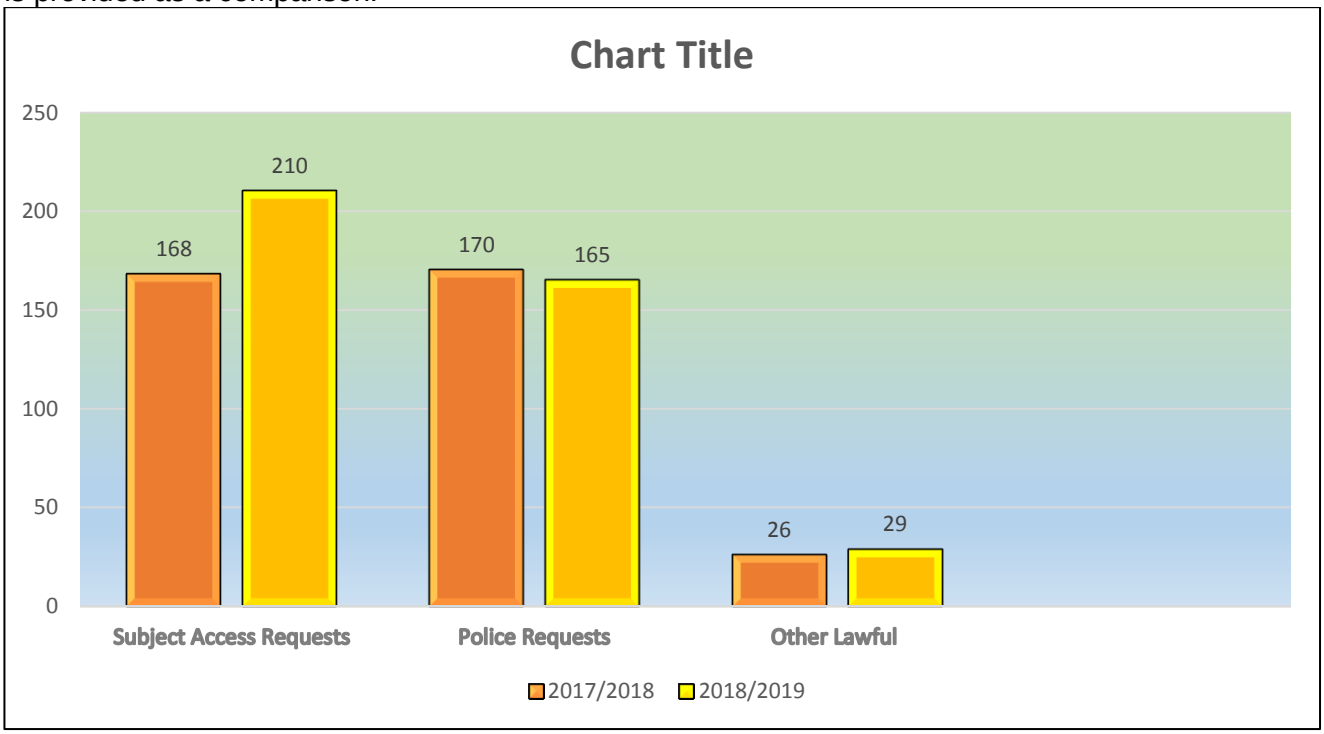
The FoI pages contain a list of standard responses to some of the most frequently submitted requests meaning that Service Areas no longer need to deal with a proportion of requests as the IG team can signpost requestors to the FAQ's which satisfies the legislation.

Work is underway 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.

A disclosure log has also been added to the website which lists all FOI requests received during the preceding two years. Copies of previous responses can be provided with no recourse to Service Areas and minimal redaction work on the part of the IG team further reducing the resource demands placed on Services.

6. Data Protection / Subject Access Requests

The following table shows the number of Subject Access Requests made under Data Protection legislation, which were received by the Council for the reporting year. The previous year of 2017/2018 is provided as a comparison.



In respect to the numbers of data subjects making access requests for personal data held about them, there is a slight upward trend. This might have been affected by wider public awareness caused by the saturation publicity around April-May 2018 to provide information about the implementation of GDPR on 25th May.

There is no significant change in the numbers of police requests or those from organisations such as regulatory professional bodies or the DBS.

7. Internal Reviews, Self-referrals & complaints raised to the Information Commissioners Office

In the reporting period 5 self-referrals have been made to the Information Commissioner's Office (ICO) of suspected serious breaches of personal data. One referral was withdrawn once the ICO was satisfied there was no evidence of privacy being compromised.

Of the 4 remaining, three have been closed by the ICO with no further action as we were able to demonstrate the mitigating actions we put in place and that the root cause was human error and one remains open at the time of writing this report.

In the reporting period, the Council's Data Protection Officer has received four 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 our compliance in each case.

The IG team has redesigned the reporting process and recording methodology. The team also amended the triage process to consider and assess the severity of reported incidents at the earliest stage and is working with the SIRO and the Corporate Leadership to refine the referral process and ensure the approach is consistent.

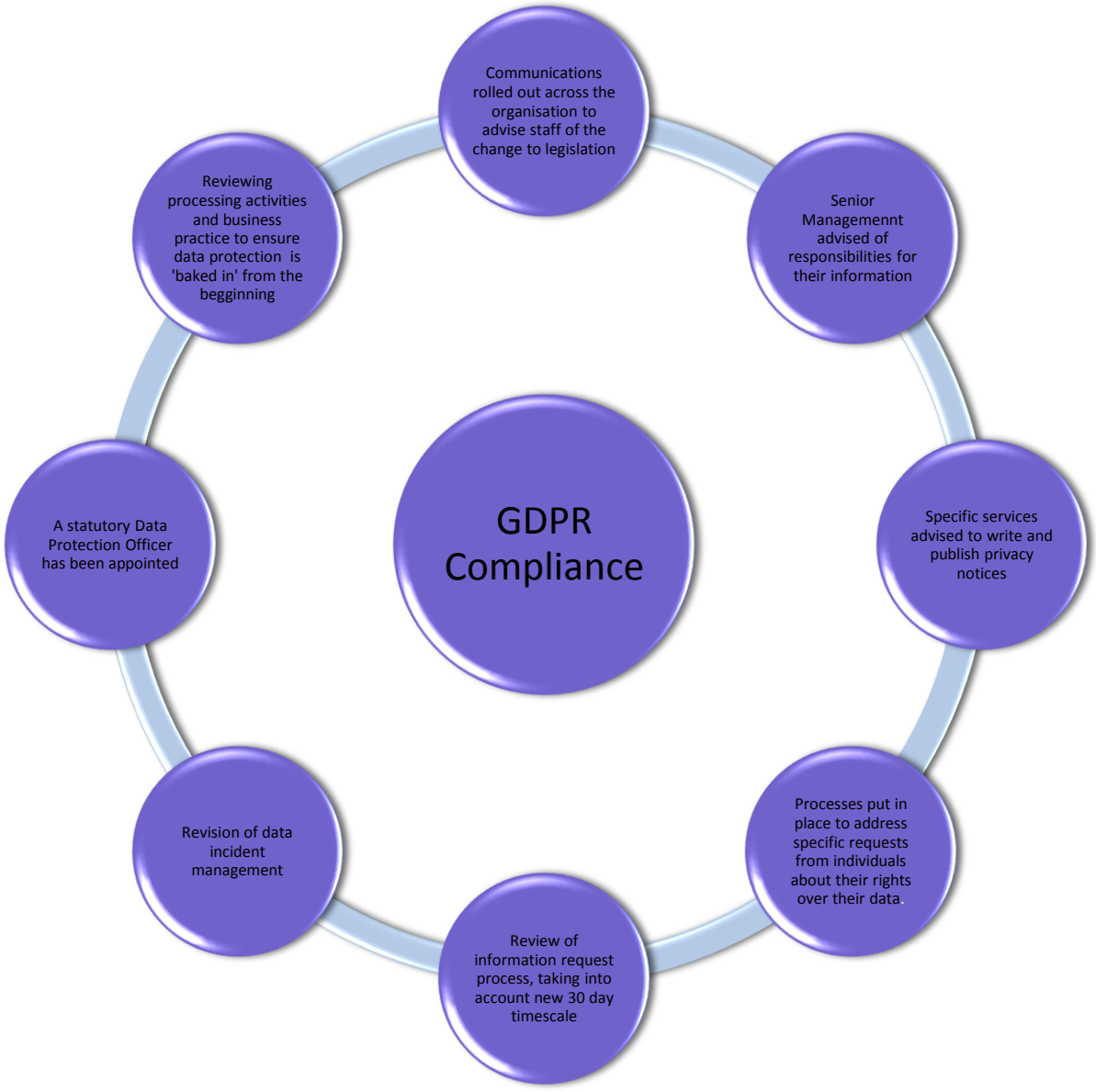
8. Changes to legislation during reporting period

Since the last report was published, the full implementation of the General Data Protection Regulation (EU)2016 and the UK Data Protection Act 2018 has taken place. The IG team has invested a significant amount of time and effort implementing the new regulations and although there are areas that still require attention to meet full compliance which may be seen as 'risks' we are aware of them and have the structure and resource to address them in this current year.

A recent audit undertaken by SWAP concluded that significant work appears to have been undertaken by the Information Governance Team and individual service areas in relation to General Data Protection Regulation (GDPR) compliance. This is contributing, actively working towards ensuring compliance and raising the awareness of staff across the Council. It is however recognised that the work required for compliance is a constantly evolving target and services will need to adapt as the interpretation of the legislation continues to develop.

The audit has made two recommendations for improvement, the first addressing inconsistency in the availability and the second about staff having access difficulties to enable completion of the compulsory e-learning training modules. The later has been rectified since the audit was completed.

Below are some of the areas of GDPR compliance we have worked on and will continue to review going forward.



9. Data Security and Protection Toolkit

In this reporting period, the Information Governance Toolkit changed into the 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 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 10 data security standards are: -

Standard	Description
Personal Confidential Data	All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.
Staff Responsibilities	All staff understand their responsibilities, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
Training	All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised IG toolkit.
Managing Data Access	Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
Process Reviews	Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
Reporting to Incidents	Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
Continuity Planning	A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
Unsupported Systems	No unsupported operating systems, software or internet browsers are used within the IT estate.
IT Protection	A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
Accountable Suppliers	IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

The evidence requirements are much more robust and are aimed at demonstrating that the organisation is taking its responsibility seriously and holding itself accountable.

The Council completed and submitted its annual return for 2018/2019 in March. Notification regarding the successful completion of all standards had not been received at the time of this report being written.

10. Information Security

Awareness of the subject of Information Security has significantly increased over the last year, with the topics of GDPR and cyber security threats receiving intense media coverage. This, and the e-learning rolled out in 2018 has had a positive impact on the desire for good information security knowledge of our colleagues.

The IG Team has used the engagement opportunities this has created to work more closely with areas where information security risks are high, to understand more about how they work and how they can be supported to achieve a good, and consistent level of information security. In those areas especially, but also across the council, Information Security is starting to be something we all do every day, rather than something IG do.

Working more closely with individual teams has allowed the IG team to identify and resolve issues such as unwieldy processes being introduced in the name of information security. Undoubtedly this will be happening across the organisation, so we need to carry on building on those basic foundations, addressing some of the barriers to good information security – such as not having the right software, or being unclear about what information you can share.

The next step is to raise awareness and empower staff about how to spot potential cyber security threats, and how to respond. At the same time, there is a need to keep staff up to date on subjects covered previously – information security is a continuously evolving subject.

It's vital that IG is part of council-wide initiatives like the Digital Programme, not only from an overall governance perspective, but also to feed into how apps are used, and to ensure good information security is embedded into the culture being developed. We need to ensure that new ways of working do not compromise our information security, and to ensure that we also use new ways of working to provide useful and relevant information to our colleagues.

11. Public Services Network (PSN)

PSN testing is carried out every year across the Authority and provides a benchmark of how secure the Council's IT systems are to external interference.

The last tests took place in 2018. Initially, 9 critical issues and 47 high issues were identified, along with several medium and low risks. Work has taken place over the last 12 months and **all** the critical issues have been resolved, as have 45 of the identified highs. Medium issues are down to 15 outstanding.

Work will continue to resolve these remaining 15 and also to address any low issues that were identified.

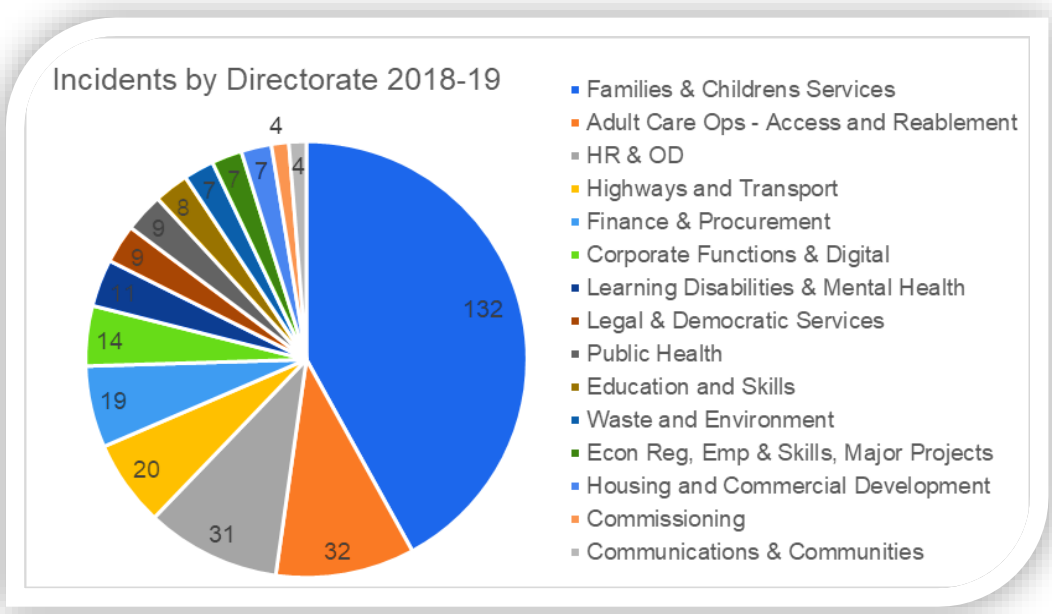
As incidents in South Wiltshire at the start of last year unfolded, Wiltshire become a centre of worldwide attention. This interest was not restricted to the media, but also manifested itself as a

significant increase in activity to break into our systems, causing significant additional work to ensure they remained secure. The National Cyber Security Council and MHCLG supported us to help scan our activities in terms of Cyber security and provide an overview of cyber security arrangements in both the council and Wiltshire police. Reassuringly they stated they were happy with how the incident has been managed.

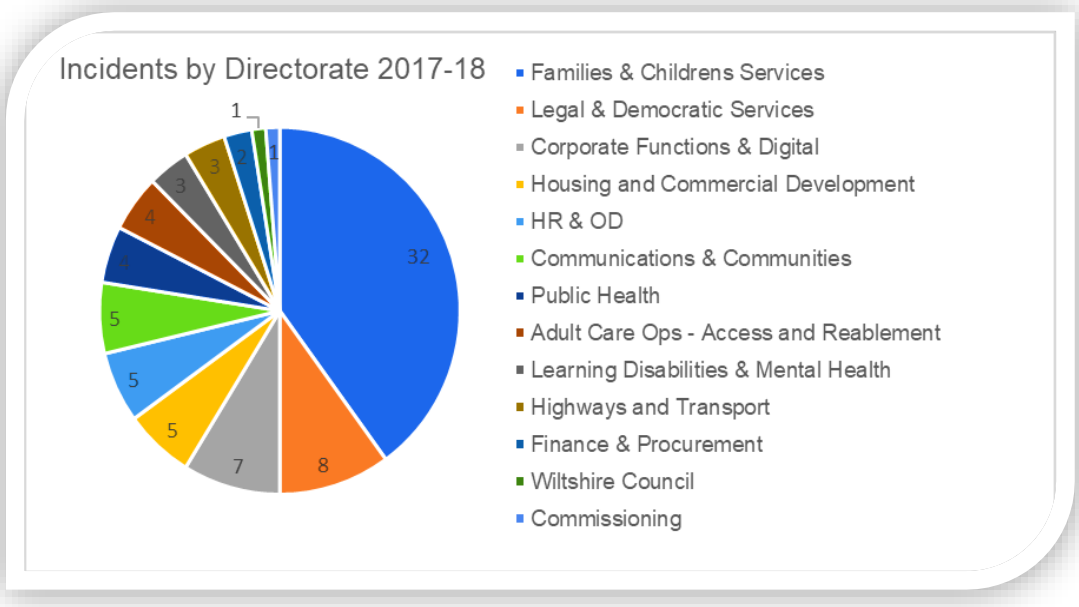
12. Data Incidents

Reported data incidents have significantly increased in the last year, climbing from 83 reports in 2017/2018, to 314 for 2018-19. An increase of 378% might appear as a negative, but in fact this reflects the greater awareness of the need to report which we have achieved this year with the e-learning and other engagement sessions.

This table shows the number of reported Incidents by Directorate area. Figures can be broken down to report on individual teams or service areas, which allows the IG Team to work closely with our people to help identify areas where information security needs to be improved – whether it's a need for further training, or a process which needs to be revised.

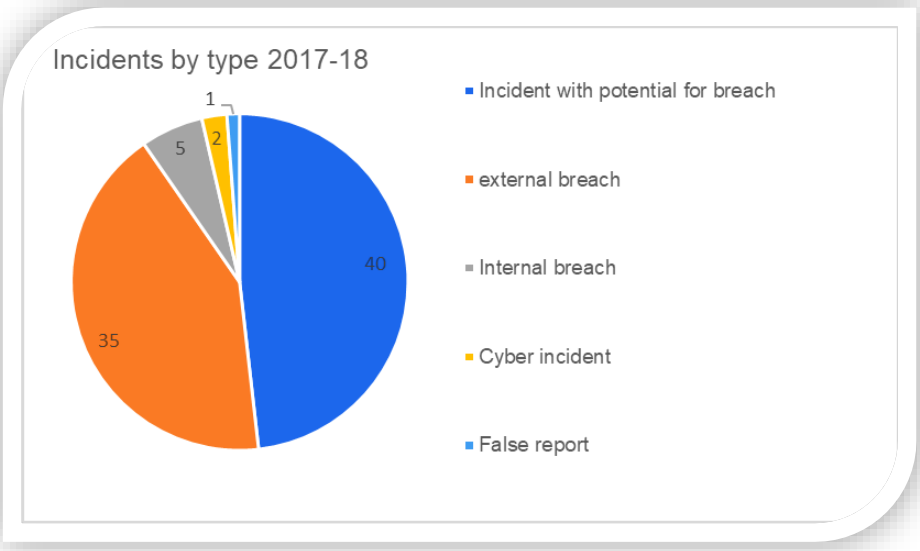


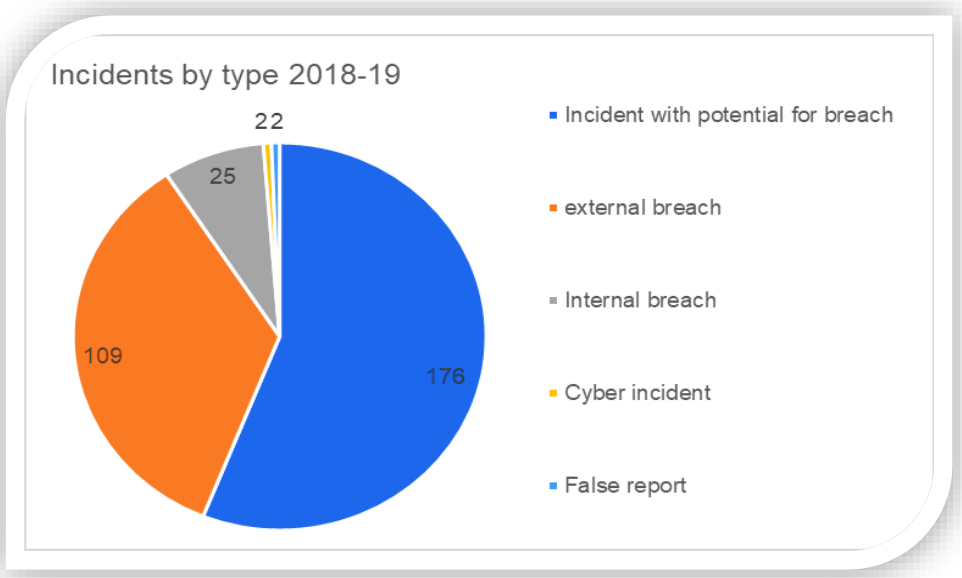
As a comparison, the previous year is included below.



During this reporting period, the way incidents are reviewed and classified, making it much easier to provide detailed information, including details like data sensitivity, and number of data subjects. The revised outcomes mean we can now identify how many incidents were “incidents with potential for inappropriate disclosure”, where no personally identifiable data was affected, as opposed to internal or external breaches where information has been shared inappropriately. We have revised our figures for 2017-18 to allow for meaningful comparison.

The following tables for Incidents by type for 2017-18 and 2018-19 show that, despite the increase in reported incidents, the split of incident types across the total is very similar. Most of the reports are for incidents with a potential for inappropriate disclosure – for this year these are made up of “information being shared to the wrong person” and “information being sent non-securely”.





The email address book including police staff and council staff in one list is a factor in information being shared to the wrong person, and we are considering whether it is feasible for the two organisations to have separate address books. The removal of GCSX and changes to secure email mean there is much less requirement for colleagues to apply additional protection to our information when they share it, and so we should see a reduction in information being shared non-securely in the next reporting period.

Liaising with colleagues about hundreds of incidents has given us a great opportunity to understand what the root cause of an incident is. We can move away from the “human error” and start to address the behaviours and root causes to improve our information security. Our incidents often happen when people work on more than one thing at a time; another factor which is on the increase is colleagues not always having the right tools for the job they are doing. Whilst it is simple to supply the software, changing colleagues’ perception that everything is time-pressured is a bigger challenge, and one that will require buy-in from all levels of management.

The breakdown of incidents by directorate for 2018-19 provides an overview of the volume and level of incident reported by each area. The improved reporting will be used to work with Families and Children’s Services to reduce the volume, especially of external breaches. The following table provides a full list of reported incidents, broken down by directorate and outcome. The monitoring and reporting of cyber security incidents (where we are targeted) is being reviewed as whilst the number and might look like a positive, by their very nature, incredibly hard, to identify. In our collaboration with Microsoft via our Digital Transformation programme and the adoption of the ICT Strategy, there is significant work being undertaken to mitigate and where reasonable to eliminate risks. It should also be noted that teams like Payroll are very proactive in spotting and reporting phishing emails.

Incidents by Directorate 2018-2019	Total	% of Total
Adult Care Ops - Access and Reablement	**32**	**10%**
external breach	6	
False report	1	
Incident with potential for breach	23	

Internal breach	1	
Not recorded	1	
Commissioning	**4**	**1%**
Incident with potential for breach	3	
Internal breach	1	
Communications & Communities	**4**	**1%**
Incident with potential for breach	4	
Corporate Functions & Digital	**14**	**4%**
Cyber incident	1	
external breach	2	
Incident with potential for breach	8	
Internal breach	3	
Econ Reg, Emp & Skills, Major Projects	**7**	**2%**
external breach	4	
Incident with potential for breach	2	
Internal breach	1	
Education and Skills	**8**	**3%**
external breach	2	
Incident with potential for breach	6	
Families & Children Services	**132**	**42%**
Cyber incident	1	
external breach	50	
Incident with potential for breach	75	
Internal breach	3	
Not recorded	3	
Finance & Procurement	**19**	**6%**
external breach	12	
Incident with potential for breach	6	
Not recorded	1	
Highways and Transport	**20**	**6%**
external breach	8	
False report	1	
Incident with potential for breach	7	
Internal breach	4	
Housing and Commercial Development	**7**	**2%**
external breach	4	
Incident with potential for breach	2	
Internal breach	1	
HR & OD	**31**	**10%**
external breach	9	
Incident with potential for breach	14	
Internal breach	8	
Learning Disabilities & Mental Health	**11**	**4%**
external breach	2	
Incident with potential for breach	8	

Internal breach	1	
Legal & Democratic Services	**9**	**3%**
external breach	4	
Incident with potential for breach	5	
Public Health	**9**	**3%**
external breach	3	
Incident with potential for breach	6	
Waste and Environment	**7**	**2%**
external breach	3	
Incident with potential for breach	2	
Internal breach	1	
Not recorded	1	
Grand Total	**314**	

The 83 incidents reported in 2017-18 are broken down as follows:

Reported incidents 2017-18	Total	% of Total
Cyber incident	2	2%
external breach	35	42%
False report	1	1%
Incident with potential for breach	40	48%
Internal breach	5	6%
Grand Total	**83**	

A recent audit undertaken by SWAP provided reasonable assurance and concluded that most of the areas reviewed were found to be adequately controlled. The report only contained one priority three recommendation for improvement, relating to the review and upgrading of policy documentation

13. E-Learning Programme and Raising Awareness

In the last reporting period, the IG team in collaboration with the HR and Organisational Development Directorate developed and rolled out a set of 4 e-learning modules: Data Protection, Information Security, Freedom of Information and Records Management.

Not only is there a need to raise awareness across the organisation for the purposes of improving understanding in staff., but there is also a requirement from the Information Commissioner's office (ICO) and the Data Security and Protection toolkit, to evidence an education program for staff.

Our most recent IS e-learning module in 2018 has been our biggest vehicle for promoting good information security so far. The topics covered were those identified as most relevant to the bigger picture, and those required for NHS IG toolkit compliance. Guidance was limited to bite-size chunks, but covered subjects from ID badges and door security, to email and acceptable use of systems, which resulted in a lot of information for our end-users to consume in one go. The second iteration of the e-learning will have a stronger emphasis on cyber security. It will also be presented along with face to face offerings and team sessions to meet a variety of learning styles.

This format was duplicated across the other modules and following feedback regarding the content and structure of those modules, we have reviewed and refreshed all 4 modules to consider the comments from staff.

In the next reporting period 2019/2020, we will be rolling the modules out in one go rather spaced over 4 months. We believe this is a more controlled way of monitoring the completion of the modules and we hope will provide staff the opportunity of putting some dedicated time aside, if they can see each of the modules.

This new IG education program will also feature introduction videos explain to staff why the completion of these modules is important. Staff will be encouraged to take responsibility for the way they work with and manage information. It is not a single team responsibility to manage the information of the Council. It is a combined approach that involves direction from the IG team, Corporate Leadership, Senior Management and accountability from the staff, managers and elected members.

Because of the importance of this training, a decision was taken to make the training mandatory with a failure to undertake any of the modules, resulting in laptop access being suspended. This decision was not taken lightly, and it is acknowledged that there is the potential for this to cause problems if members or officers do not comply and undertake the training in a reasonable timeframe, acknowledging that there will always be accepted caveats regarding justifiable reasons that may impact on staff completing the training within the prescribed time period. Whilst this was a decision made in the last reporting period, the reality of trying to apply this in the middle of a major national security incident was not feasible or realistic. There will be a much more focused and transparent approach in the next reporting period.

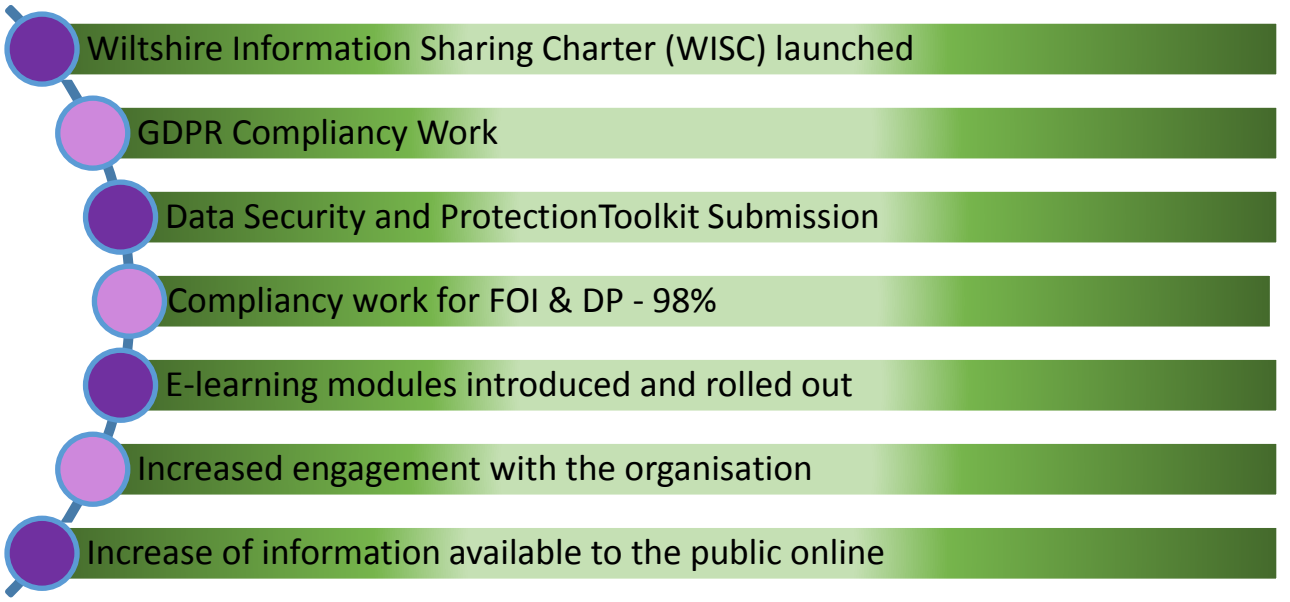
We are also aware that E-learning on its own may not be having the required impact, so we will also be considering other training and information outlets to get the message across on a regular basis. Options such as whether there is a benefit of the subject being incorporated into the induction programme and / or a feature of the leadership and management development programmes so aspiring and developing managers can be made clear about their responsibilities, as well as whether there may be the opportunity to link into appraisals and management meetings will be considered the subject is always on the agenda and not just something everyone has to do once a year.

As already mentioned, the Information Commissioner's office also asks for evidence of staff training, when complaints or investigations are undertaken. They are particularly interested that this has taken place when a data incident has taken place resulted in the breach of information.

Raising awareness levels is a constant process and aims at keeping Information Governance on people's radar. Regular notices are put in the Electric Wire and the Managers Wire. We acknowledge it is not the most 'interesting' of subjects, however understanding information, how it is stored, shared it and knowing when and how to dispose it, is important and is the key asset within this organisation.

14. Key achievements

The work undertaken in the last reporting period has been encouraging and has been achieved with a collaborative and engaging approach. Here are just a few of the key achievements.



It has been a busy but successful year for Information Governance. With the restructure of the Information Governance team now complete, it has provided an opportunity within the team to take stock of where it is and where it wants to get to going forward.

The Digital transformation programme is a key cultural change within the organisation and Information Governance is already part of the conversation and projects that are taking place. Over the next twelve months we will be looking to the Information Governance workstream to support the OD and Change workstream to help ensure staff understand the importance of IG. This will also support the development of the recently restructured IG team with the development of the new service model and how we provide a supportive approach to the organisation in how it governs its information.

Together with the organisational vision, business as usual within the Information Governance arena will include continuing with the compliancy work associated with GDPR, working towards reducing the number of requests for information coming directly into the team through improved availability of information on the Council's website and filtering back to services what can be easily addressed by better understanding of what can be shared with members of the public.

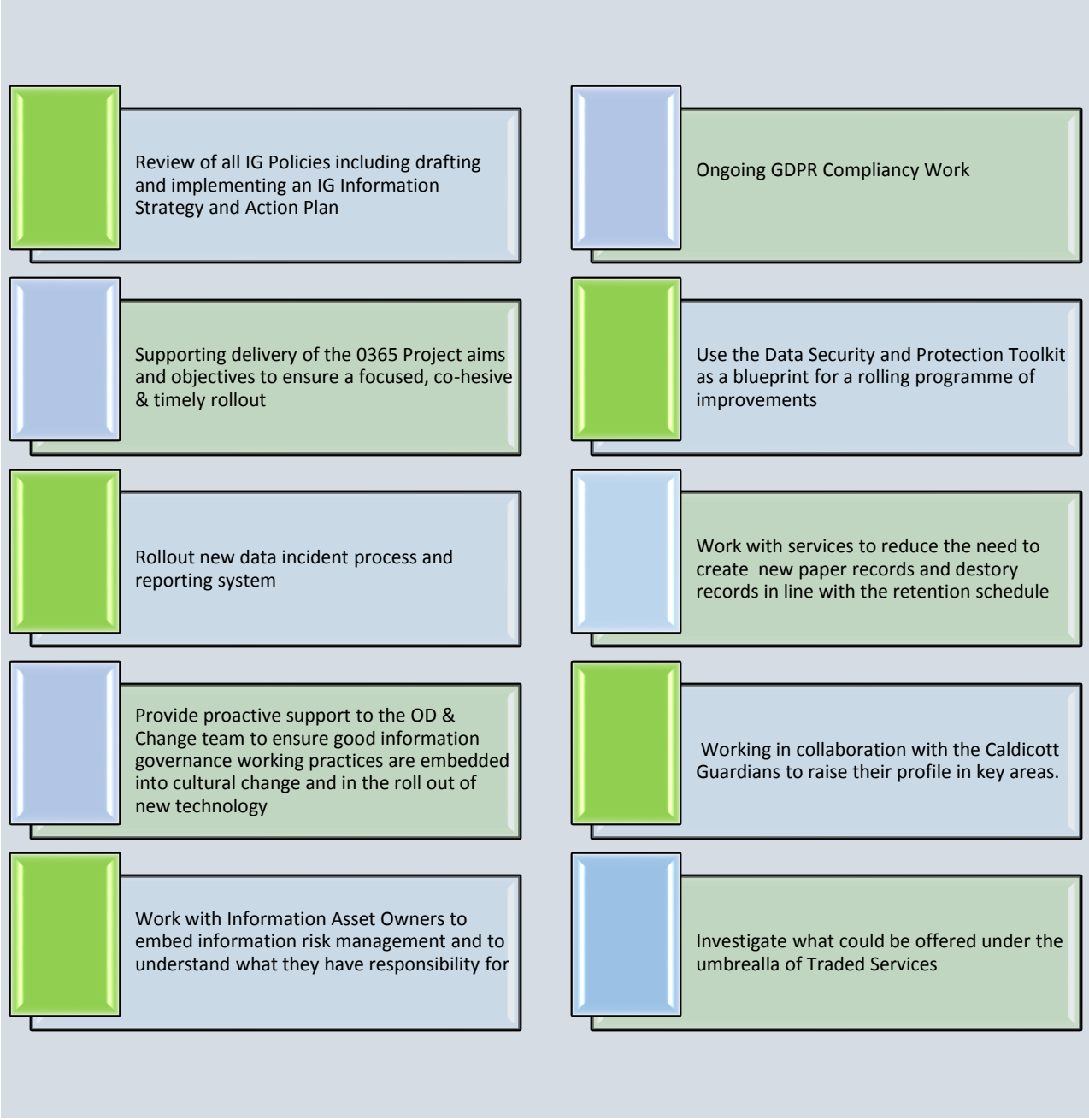
Improving engagement across the organisation and continuing to raise awareness about the importance of Information Governance will be front and centre going forward.

I would also like to thank the IG team in keeping positive in what has been a particularly challenging year. Their advice and guidance has been sought on a regular basis, on a number of subjects and they have done this whilst undergoing a team restructure themselves. They are a professional team and re seeking to engage with the organisation to get the IG message out.

There is much to be done still but I am reassured that the team will meet these demands and contribute to an ever-changing environment in their usual resilient way.

15. Looking Forward

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



16. Summary

The term Information Governance refers to a framework that supports legal compliance, transparency and risk management and balances that against the requirements of the organisation to deliver an effective service.

Good Information Governance is about enabling staff to perform their jobs in a way that supports them whilst ensuring they remain compliant, provide the necessary safeguards to protect personal

information, are proactive in storing, managing and eventually destroying information in line with the retention schedule and doing all of that in a secure way.

The key as always remains getting buy in from the organisation. Buy in from the Senior Management to ensure that Information Governance is embedded into the organisation's culture change and ensure that the message is constantly cascaded that information is our asset, is at the centre of all we do and is something entrusted to us by the public.

We also need buy in from the officers and elected members. It is the responsibility of all individuals regardless of role, to ensure they treat information within the boundaries of Wiltshire Council, with the same respect they would expect their own information to be treated. That means being aware when sharing information digitally or working from paper documentation. It is about being accountable for your own actions and seeking advice and guidance when appropriate.

As stated in last year's report, the ongoing cyber security threat to our systems and information remains high. In our collaboration with Microsoft via our Digital Transformation programme and the adoption of the ICT Strategy, there is significant work being undertaken to mitigate and where reasonable to eliminate risks.

This work along with adopting and being proactive with good Information Governance working practices will lead the organisation into effective cultural change.

The benefits of doing this will lead to staff being more confident and empowered in managing information. Doing that leads to the successful delivery of business goals because teams have the right information to focus on the most effective solution to service provision.

As I stated last year, the public trust that we are the guardians of their information and we must provide that reassurance, by having robust and resilient systems and processes in place. Information Governance therefore must be the voice of conscience. So, the IG team will continue to support, advise, challenge and question the working practices of services and will support the OD & Change team to deliver cultural change.

Robin Townsend, Director, Corporate Services and SIRO

Date: 6 June 2019

Report Author: **Sarah Butler, Information Governance Manager**

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