Regulatory Committee:	Audit & Governance Committee
Date:	29 September 2023
Chair:	Cllr John Bloxsom
Presenting Officer:	Jenny Grodzicka, Head of IMS (DPO)
Item Type:	Annual Report: For information
Purpose of Report:	To update committee members on data protection compliance across the council. To provide assurances on work completed or planned to ensure compliance with key elements of data protection legislation.
Recommendations or Actions Sought:	To note the report
Background Documents:	n/a
Forthcoming Cabinet Decisions:	The report does not relate to any Cabinet or Cabinet Member Decision.
Appendices:	n/a
Contact Information (For information on the report)	01452 324000 dpo@gloucestershire.gov.uk

Data Protection Officer (DPO)
Annual Report 2021/22 and 2022/23

1. Foreword

Whilst the worst of COVID-19 may be behind us, for many it has still been as real and at the front of our minds as previous years, with a continued impact on the ways we work together. Agile ways of working are more firmly embedded and seen by many more as THE way to work. As a result, swathes of people moved roles across the country. With geographical boundaries no longer a barrier to getting that dream job it made the task of retaining and attracting the right people harder than ever.

With regards information management, it has been a period of consolidation and catching up, with the council taking big steps forward in reducing backlogs, both in requests for information and records management processes. The work on improving and consolidating privacy notices was completed, alongside a revamp of both information management's (IMS) Staffnet and website content, improving accessibility, relevance to the audience and reducing the impact of maintaining the content.

We continue to make progress with the actions from the ICO audit, sufficiently so that in December 2021 the ICO was satisfied with the improvements and direction of travel and concluded that they did not need to continue to monitor progress, for now. However, some actions remain outstanding, notably those relating to disaster recovery testing, the requirement to proactively monitor compliance across the organisation and the improvements to the Information Asset Register.

FOI and SAR performance is not yet consistently where we want it to be but continues to improve, with the national targets becoming ever more within our sights. The council attracted further attention from the ICO in 2022 due to several complaints about subject access responses. This supported a more in-depth review of SAR backlogs, and as a result some longstanding cases were resolved. Furthermore, monitoring has been enhanced, resulting in earlier escalation of arising issues.

The implementation of Microsoft 365 (M365), ensuring both a secure and future thinking approach, has proven challenging. The implementation has highlighted that whilst technical security is increasingly considered, governance reviews are yet to become an integral part of the implementation and release of new software.

The foundations are getting stronger by the year, which will allow the council to look at how it can safely exploit and use its information in ways to support effective working and meet the needs of our communities.

Jenny Grodzicka, Data Protection Officer, Gloucestershire County Council

2. Context

The Data Protection Officer (DPO) is a statutory role that the council is required to have in place. Under data protection law, the DPO must undertake the following statutory tasks:

- inform and advise the council and the employees who carry out processing of their Data Protection obligations;
- monitor compliance with Data Protection legislation and Data Protection Policy, including the assignment of responsibilities, awareness-raising and training, and related audits;
- provide advice regarding, and monitoring of, Data Protection Impact Assessments;
- co-operate with the Information Commissioner's Office (ICO); and
- act as the contact point for the ICO on issues relating to processing and to consult where appropriate on any other matter.[1]

The council must:

- involve the DPO, properly and in a timely manner, in all issues which relate to the protection of personal data;
- support the DPO in performing their tasks by providing resources necessary to carry out those tasks, by providing access to personal data and processing operations, and by supporting the DPO to maintain their expert knowledge;
- not instruct the DPO in the exercise of their tasks, and to ensure the DPO reports directly to the highest management level of the council; and
- ensure any other tasks and duties assigned to the DPO do not result in a conflict of interests.[2]

3. Governance and Accountability

The council has an established Information Board, reporting into the Corporate Leadership Team, with representation across the council. It is important for this to be maintained to ensure that it works effectively to direct, prioritise, and monitor compliance.

A network of Information Asset Owners (IAOs) and Information Asset Managers (IAMs), who have responsibility for their specific information assets, is well established. However, formal internal information governance operational groups and champions are yet to be fully established within the council.

The council is an originating member of the Gloucestershire Information Governance Group (GIGG). This is an extremely useful working group which discusses matters of shared concern, and to share effort such to prevent re-inventing the same wheel. The council is also a member of the West Midlands Governance Forum, which enables informal learning and further sharing of good practice.

Demonstrating compliance is a key part of the data protection regime, requiring ongoing maintenance of appropriate evidence, such as registers of data sharing agreements, privacy notices and information assets. With largely devolved processes this continues to present challenges, as full and timely engagement is needed from already stretched services.

---

[1] UK General Data Protection Regulation, Article 39 – Tasks of the data protection officer
[2] UK General Data Protection Regulation, Article 38 - Position of the data protection officer

Key achievements in this area include:

2021/22

- Revised terms of reference for the Information Board.
- Formal acknowledgement of IAO/IAM responsibilities by relevant staff, through a targeted sign-up process.

2022/23

- Compulsory training for IAOs provided by an external training provider was commissioned and delivered.
- Registers for Data Protection Impact Assessments and Sharing Agreements have been developed.
- A clean up and simplification of the council's Privacy Notices was carried out to improve the user experience. See section 7 for more information.

Areas for further improvement

- Continue with the work to implement improved compliance monitoring and establish Directorate Operational Groups
- Regular and relevant refresher training for IAOs/IAMs, appropriate to the information risks of their assets.
- The creation of a collaborative space for the IAO network, potentially utilising Microsoft Yammer / Viva Engage.
- Further consolidate and improve IAR entries, to make this a more useful business tool.
- Implement a GDPR classification label within M365 to support improved identification of personal data within the council.

4. Policy, Training and Awareness

Together, policies and procedures provide a roadmap for day-to-day operations. They provide a framework for compliance with laws and regulations, give guidance for decision-making, and provide clarity over governance structures and roles and responsibilities.

The council continues to have a strong generic data protection training presence, using a variety of methods to raise awareness and educate staff, supported by an annual communications plan, including videos, TalkSmart articles, Managers' briefs, and tailored training sessions.

Data Protection awareness training for all staff is largely focussed on cyber security, as the highest risk area, and is made available to staff via MetaCompliance. Training consists of 12 short videos and a multiple-choice assessment, each taking no longer than 15 minutes.

A move to a less mandated approach, relying on staff to opt-in to the training, resulted in an unacceptable drop in take up of policies and training. Consequently, various short-term measures to improve staff take-up have been taken, with uptake increasing slightly, but still not sufficiently.

Chart 1: Information governance e-learning staff take-up 2021/22 – 2022/23

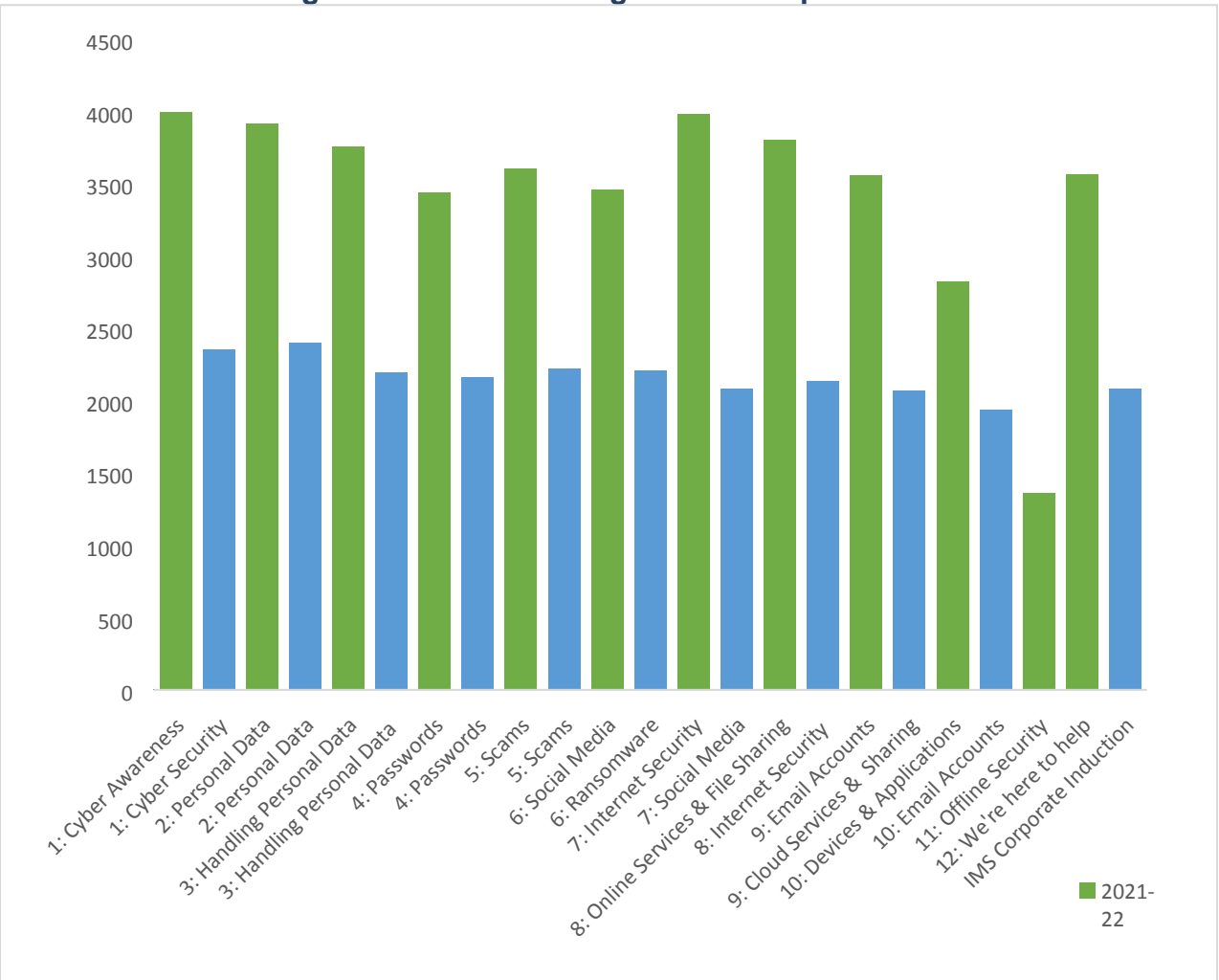
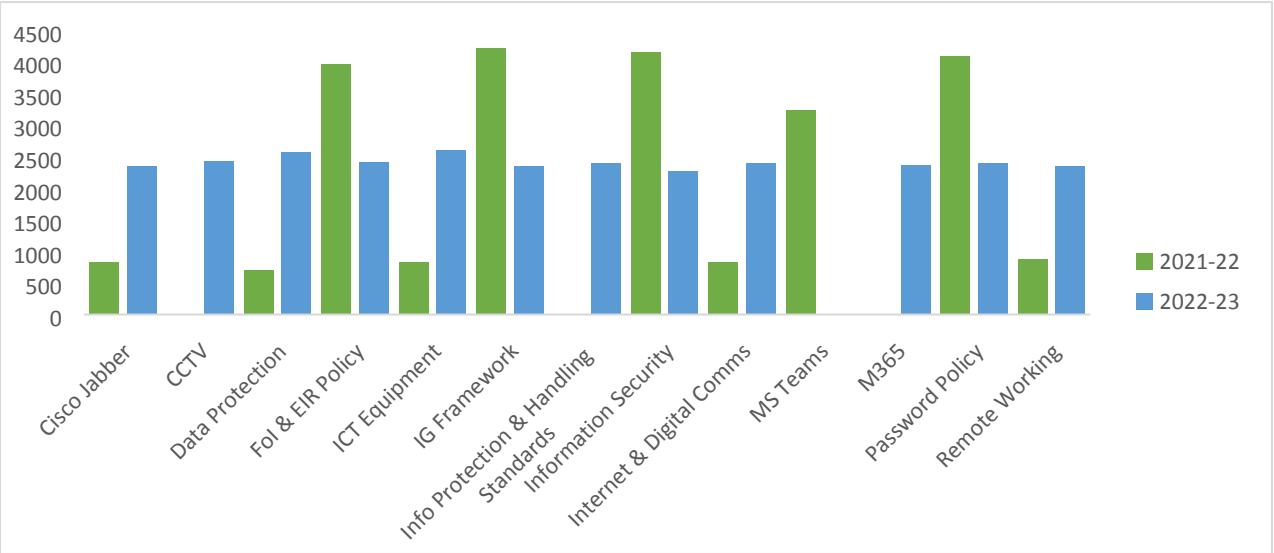


Chart 2: Information governance policy staff take-up 2021/22 – 2022/23



Key achievements in this area include:

2021/2022

- The information management corporate induction training was launched.

- Policies developed for working in the new M365 environment and agile working.
- A new CCTV and Surveillance Policy and accompanying process was developed.
- The council's intranet (Staffnet) pages were comprehensively redesigned to improve staff's access to guidance and advice.
- To re-enforce and validate cyber awareness, two phishing simulation campaigns were completed.
- IAO and IAM refresher training was developed.

2022/2023

- Policy created governing the use of Bring Your Own Device (BYOD).
- The council's information management web pages were redesigned to improve accessibility and relevance to the audience.
- Delivery of training for IAOs.
- A new policy template was created to standardise the look and feel.

Areas for further improvement

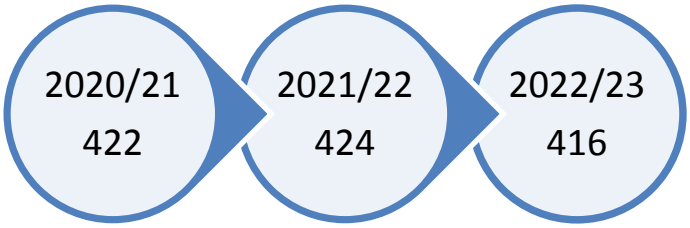
- Improve the uptake of the e-learning, such as through working with Heads of Service and the technical implementation of MetaEngage.
- Ensure that data protection is considered in the development of wider council policies.
- Streamline the policy review process and ensure it is aligned with the dissemination process.
- Integrate information governance training into the corporate offer.

5. Transparency and Individuals' Rights

In response to the ICO audit, and in recognition of the complexity around privacy notices that had developed over time, the council's privacy notices have been overhauled and presented in a new style, helping to simplify and streamline the approach. The council's layered approach to privacy notices was completed, reducing the service specific ones from 65 to 8; improving the experience for both staff and customers.

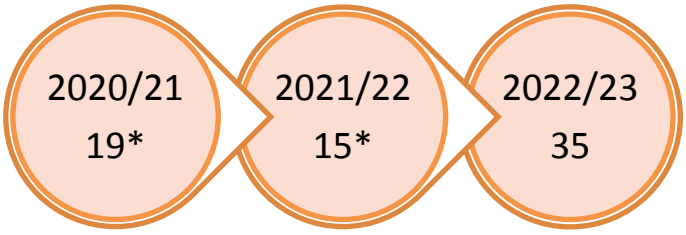
The number of subject access requests received now remains relatively consistent, although even a small increase has a disproportionate impact on capacity.

In August 2022 the Information Commissioner's Office (ICO) contacted the council, raising concerns about the number of subject access requests (SARs) going out of time. Due to the work the council had previously implemented, we were able to provide a timely response about the 22 cases overdue at the time. This response was sufficient to assure the ICO that the council was effectively managing and improving the situation and substantial progress has been made on reducing this backlog; only 1 of these cases remains open (in agreement with the requestor, due to the size of the request, information is provided regularly).



Number of subject access requests received:

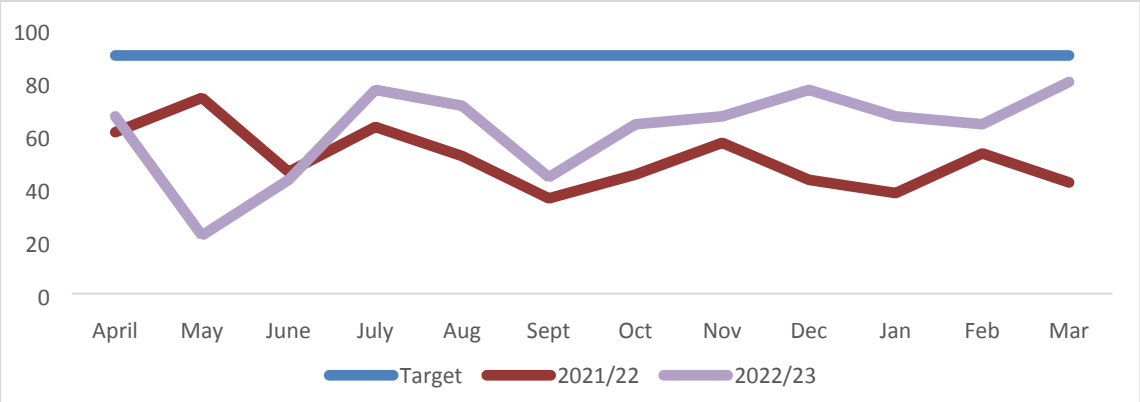
Number of other types of rights requests received[3]:



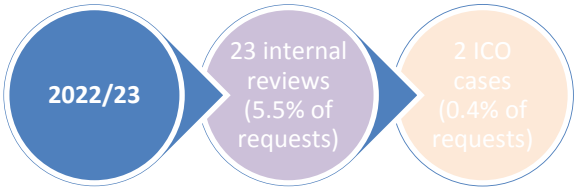
* Please note the above figures relating to other types of rights requests may not be 100% accurate due to the way they were historically able to be categorised in the IT system. Improvements were made in 2022 to rectify this.

Most requests from individuals relate to complex social care situations, that have resulted in a large number of files covering many years. A combination of a backlog that had developed, complexity and volume of cases, and capacity issues across the process, meant the council has not been meeting the 90% on time target. However, over time this picture is improving, with new processes developed, and increased oversight contributing to the improvements.

Chart 3: Percentage of subject access requests responded on time 2021/22 - 2022/23



Request Escalation



3 These include requests such as objections to processing and requests to erase or correct personal data.

Despite the increase in numbers and challenges in responding in a timely manner the number of subject access requests escalated to internal review and the ICO remains exceptionally low.

Two cases resulted in a complaint to the ICO by the requester in 2021/22. Out of the 439 total cases received, this represents 0.5%.

- One was in connection with a SAR; and
- One was about a request for rectification.

The ICO upheld the council's original position in in both cases.

Two cases resulted in a complaint to the ICO by the requester in 2022/23. Out of the 451 total cases received, this represents 0.4%.

- Both cases were in relation to the response missing the statutory deadline.

The low number of escalations is believed to result from the improvements that have been made to the process, in particular the positive engagement from Children's Services, and the adoption of a more customer-focussed approach.

Key achievements in this area include:

2021/2022

- A revised Privacy Notice template was designed, to better enable service areas to develop their own privacy information.
- Children's SAR process introduced to ensure the timely receipt of Children's Social Care data to the Request Management Team.
- Introduction of the Children's Directorate Information Governance Group, with the aim to produce solutions to information issues.
- Clarifying the approach to extending the deadline for Subject Access Requests.

2022/2023

- Completion of the layered approach to privacy notices, reducing the service specific ones from 65 to 8.
- Developed QR codes that can be added to documents to allow people another method of digitally accessing the privacy notices.
- Introduced a template privacy notice for consultations.
- Improved monitoring and oversight of overdue requests.
- Guidance reviewed for all types of individual rights requests.
- Internal guidance on the SAR internal review process developed.

Areas for further improvement

- Explore how privacy information can be made more accessible for children, young people, and people with disabilities.
- Quality audit reviews ensuring that processes are fit for purpose and to improve our governance on requests.
- Request coordinator re-engagement including regular communications and training.
- Review of current processes to consider where further efficiencies can be made.

6. Information Asset Register (IAR) and Register of Processing Activity (ROPA)

GDPR requires the council to maintain a record of processing activities, specifying what details about the use of personal data need to be included. The council achieves this through its Information Asset Register.

We recognise that further work is still needed on this to develop a proportionate approach, supporting the business in completing and maintaining it and making it a more useful business document. Consultation has been taking place to ensure that the direction of travel for the IAR and ROPA is clear and understood. To continue to take this forward a delivery plan for the revised IAR has been developed.

Key achievements in this area include:

2021/2022

- An exercise was completed to improve the quality of data in the IAR and to meet the Register of Processing Activity requirements.

2022/2023

- The definition of an Information Asset has been clarified to enable cleansing of register entries.
- A new approach for the structure of the IAR has been approved by the Information Board.

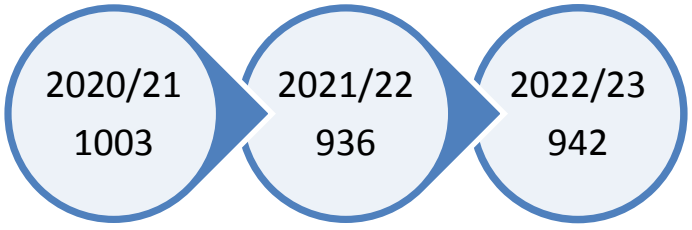
Areas for further improvement

- Design and creation of a new IAR format to meet the approach agreed by Information Board.
- Development of a system for hosting the IAR that is accessible and integrates with the council's M365 functionality.

7. Data Security and Breaches

Key to the protection of personal data is the security measures the council is required to have in place. These fall into 3 categories: physical, organisational, and technological. As well as being necessary for compliance with the law, these often form essential controls to reduce the risk of cyber-attack, both protecting data and ensuring continued service provision.

Number of internally reported potential incidents:

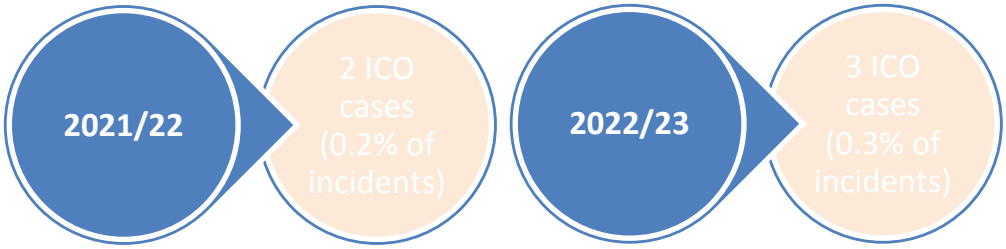


The number of suspected data breaches reported and managed has remained consistent. Whilst the numbers remain relatively high this is considered a positive position for the council, as it is believed there is a good level of staff awareness and understanding of the importance placed on security.

A significant proportion of mistakes arise due to human error i.e., lack of due care when handling personal data, for example:

- Unauthorised disclosure of personal information accounted for 240 of reported incidents in 21/22 and 302 in 22/23
- Incorrect information uploaded to internal systems accounted for 270 reported incidents in 21/22 and 191 incidents in 22/23

Incident Escalation:



Two data breaches were considered to reach the threshold for reporting to the ICO in 2021/22 and three in 2022/23. Whilst for each of these cases only a small number of individuals were affected, the circumstances for each case are briefly summarised below:

- Case 1 - A confidential address of a service user was disclosed in error.
- Case 2 – Information deemed to be either misleading or inaccurate was shared in error.
- Case 3 – Loss of a work bag containing sensitive information relating to children's cases.
- Case 4 – An incorrectly addressed referral led to the wrong family being contacted.
- Case 5 – Sensitive information was shared with 3rd party connected to the case.

Whilst the impact on those affected should not be underestimated, in each case the ICO did not consider that either formal or informal enforcement was necessary. However, recommendations made by the ICO were actioned accordingly with internal business units.

Chart 4: Security incidents logged 2021/22-2022/23

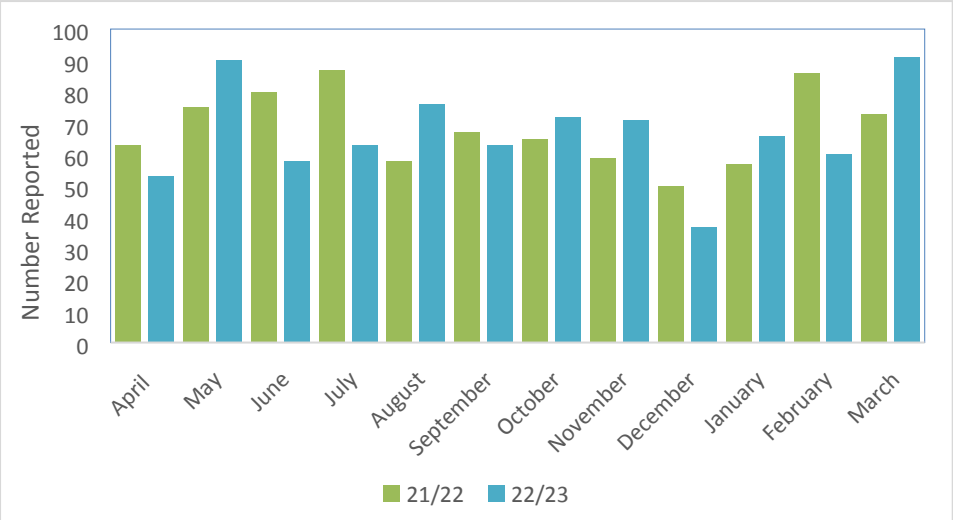
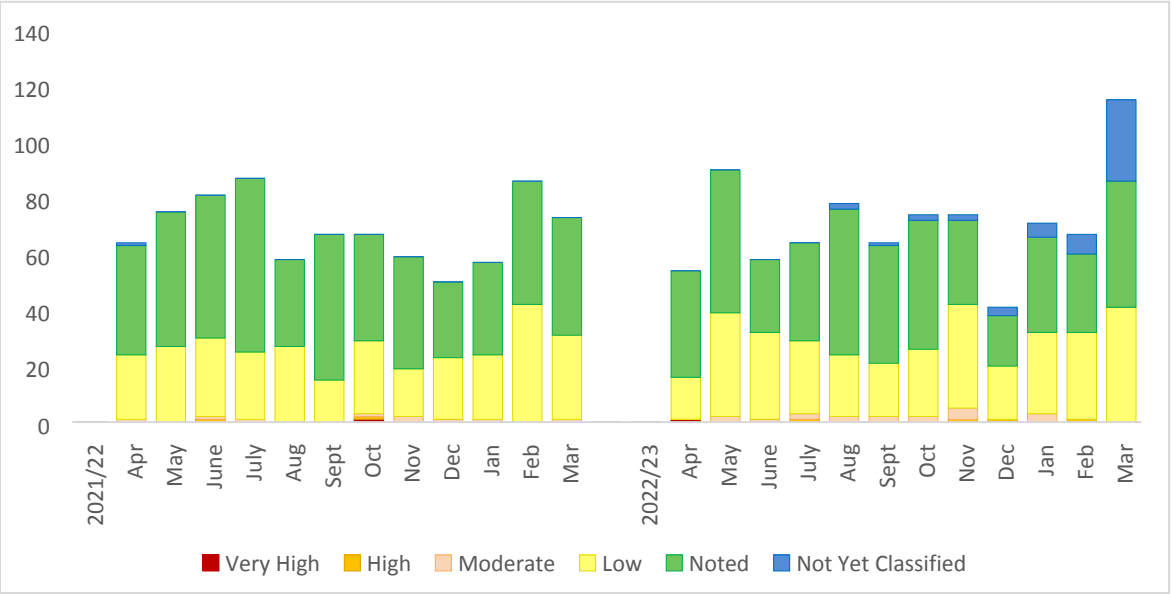


Chart 5: Severity of security breaches 2021/22-2022/23



Key achievements in this area include:

2021/2022

- Continued to satisfy the requirements for the NHS Data Security and Protection (DSP) Toolkit.
- Revised information security requirements for suppliers to simplify the process whilst maintaining assurance levels.
- Improved Cyber Resilience Plan to better assist officers in understanding their responsibilities and the processes to follow.
- A framework for implementing and maintaining surveillance camera systems.
- Integration with the wider Business Continuity Management Board.
- Two Phishing simulation campaigns to help increase staff awareness.
- Improved guidance for staff on how and when stakeholders will be informed about the progress of an incident investigation and its conclusion.

2022/2023

- PSN accreditation regained.
- Continued to satisfy the requirements for the NHS Data Security and Protection (DSP) Toolkit.
- Established a corporate cyber risk register and review regime.
- Procured a Security Information Event Management (SIEM) system.
- Cyber plan exercises held for ICT/IMS and GOLD.
- Upgraded our backup solution.
- Implemented a vulnerability management solution.
- Implemented M365 security controls, including encryption for Exchange Online emails.
- Completed a phishing simulation campaign to help increase staff awareness.

Areas for further improvement

- Introduction of new Phishing simulation functionality through the exploitation of M365 license.
- Review of the severity rating criteria for security incidents.
- Development of escalation processes to expediate the business response to breaches.

- Support further cyber resilience exercises & business continuity testing.
- Rollout of Data Loss Prevention (DLP) policies in M365.
- Review M365 system policies and governance to ensure they are fit for purpose and risks are understood and managed.
- Plan and implement appropriate solutions to reduce technical risks, as identified in assessments such as the ICT Health Check.

8. Data Protection Impact Assessments (DPIA)

The awareness for the need of a DPIA has risen, largely thanks to its inclusion in the Cabinet Report and procurement processes. Those engaged with the process have also provided feedback about its usefulness in helping them better understand the use of data in service delivery.

A DPIA review process was developed and published in response to the ICO Audit. The process sets out the responsibility of IAOs or DPIA owners to ensure their DPIAs are reviewed on an annual basis, or when changes to processing take place.

Work on a DPIA register within Microsoft 365 has begun. The new register will allow the Information Management Service (IMS) and stakeholders to review the status of a DPIA, high risks and when an DPIA needs to be reviewed by the relevant IAO. The register will also send automated reminders to the IAO when that DPIA needs to be reviewed. Improved reporting will also be available. Work needs to be completed to bring in all existing DPIAs, and then communicate the register and new process to the wider council.

Key achievements in this area include:

2021/22

- Creation and publication of a DPIA review process.
- 45 enquiries relating to DPIAs were managed.

2022/23

- A review of the DPIA template was carried out, with a new version created and published on Staffnet.
- The significant DPIA for the M365 programme was completed.
- 42 enquiries relating to DPIAs were managed.

Areas for further improvement

- Integrate an information risk appetite matrix into the DPIA to enable IAOs to better understand and manage their risks.
- Completion of the DPIA register work.
- Improved reporting on DPIAs, how many have been reviewed by the DPO, DPIAs that are overdue a review by the IAO, and the number and status of DPIAs with high risks.

9. Data Sharing

The council has longstanding data sharing arrangements with key partners such as the NHS and Police, or contractual terms with suppliers and providers of services. Much of IMS's work relating to data sharing is directed at supporting new processing, as service

areas engage in new commissioned work. The data protection relationships with third parties are becoming increasingly more complex as the council allows greater decision making to be made by third parties in how services may be provided. This additional complexity impacts on the review and revision of existing arrangements.

In future, the development of the Information Sharing Register will allow for automated processes to be run that inform an IAO or agreement owner of when they need to review an agreement and allow improve support for existing agreements that require our attention.

A complete review of the Gloucestershire Information Sharing Partnership Agreement (GISPA) was led by the council with input from the partner organisations who make up the Gloucestershire Information Governance Group (GIGG). This work has helped to update the council's data sharing agreements, bringing them in line with the industry good practice and regulatory requirements. This new data sharing protocol has been signed off by GIGG and launched in 2021/22.

Key achievements in this area include:

2021/2022

- IMS received 88 enquiries relating to information sharing.
- The Gloucestershire Information Sharing Partnership Agreement (GISPA) was revised to bring it in line with best practice.

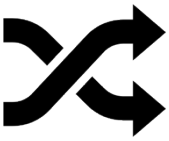
2022/2023

- IMS received 81 enquiries relating to information sharing.
- Currently 35 organisations working in Gloucestershire have signed up to the GISPA.
- A review of all known information sharing agreements has been completed.

Areas for further improvement

- Review of the information sharing agreements setup under S113 agreements between the council and local NHS partners.
- Revise Data Protection Terms and Conditions for contracts involving the disclosure of personal data to contractors.
- Complete the Information Sharing Register work in M365 in consultation with agreement owners.
- Improve reporting on information sharing agreements and automation of processes to support regular reviews.
- Continue to work with the DPO for GPs to establish sign up to a data sharing agreement for all GP practices across Gloucestershire.

10. Future Matters



Fully integrating data protection into the council's ethos is an ongoing ambition, future plans include:

- Consideration and implementation of the changes to the UK data protection legislation once they are finalised.
- Improving the uptake of training.

- Developing more tailored training, relevant to the information types and sensitivity, both for IAOs and staff.
- Establishing the organisation's information risk to better support IAOs in decision making, and ownership and management of their risks.
- Collaborating with Digital and ICT to ensure governance considerations become integrated with established practices.
- Ensuring that the development of M365 is done in a way that continues to ensure compliance, whilst supporting innovation.
- Building on the pilot for information governance champions and operational groups to further embed compliance.
- Continuing work to look at how we can safely use information to affect change that matters to our colleagues, our leaders and most importantly our communities.
- Better understanding how to engage our communities better in understanding their concerns about our use of their data.

11. Contact the DPO

If you would like to find out more about this annual report, or provide any feedback, please contact the Data Protection Officer.

01452 324000

dpo@gloucestershire.gov.uk