General Dental Council | protecting patients, regulating the dental team

Item 11
Council
31 January 2019

Annual 2018 Information Governance Update

Purpose of paper	This paper provides the annual 2018 information governance update
Action	For information
Corporate Strategy 2016-19	Performance - Objective 2: To improve our management of resources so that we become a more efficient regulator.
Business Plan 2016	Manage the GDC's finances effectively, maintaining sufficient reserves to ensure resources are available to manage our statutory functions.
Decision Trail	SLT and the Audit and Risk Committee receive quarterly reports on performance. Council receives an annual report on performance.
Next step	As above.
Recommendations	Council is asked to **note** the annual 2018 information update.
Authorship of paper and further information	Luke Whiting – Information Governance Manager Telephone: 0207 167 6309 Email: lwhiting@gdc-org.uk Lisa Marie Williams – Principal Legal Adviser Telephone 020 7167 6266 Email: LMarieWilliams@gdc-uk.org
Appendices	Appendix 1 2018 DSI report. Appendix 2 2018 FOI/DPA report.

Executive summary

1. This paper reports on the annual 2018 information update including:
    - the Information Governance Team and its work;
    - Data security incidents (DSI);
    - Freedom of Information (FOI) and Subject Access Requests (SARs); and
    - Information Commissioner's Office (ICO) decisions and correspondence.
2. Throughout 2018, and going into 2019, there remains a strategic risk on the GDC's register in relation to data breaches, Risk CP1 - *"Failure to comply with the requirements of the GDPR and Data Protection Act 2018 leading to enforcement action".* The residual risk score for CP1 is currently 12, which is on the risk appetite limit.
3. During 2018, the Information Team has managed a complex caseload of information requests, the GDC's DSI reporting process, and the GDC's relationship with the Information Commissioner. Alongside this core work, the team have continued to train and support staff, and develop the GDC's information governance framework.
4. Other significant work completed during the year included leading on the delivery of the programme of work to implement the requirements of the General Data Protection Regulation (GDPR).
5. The team's performance against KPIs remains extremely high. During the year **99% of FOI requests** completed (218 requests) and **97% of SAR requests** completed (94 requests) were responded to within the statutory deadline. This translates to missing three FOI and three SAR deadlines. This is a significant achievement given the additional work the team completed during the year.
6. Another critical measure of performance across the organisation and reported on by the team is in relation to Data Security Incidents (DSIs). **142** incidents occurred and **five** of these were reported to the ICO in 2018, although no enforcement action was taken.
7. Please see Annex A for a summary of the core work of the team.
8. Council is asked to:
    - Note the 2018 annual information update.

The Information Team

9. During 2018, the GDC continued to develop and improve its information governance framework, the way it manages and disposes of information, identifies and responds to data security incidents, and ensures compliance with the Freedom of Information Act 2000 (the FOI Act) and the Data Protection Act 2018 (the DPA).

10. The team expanded in the year to include a Deputy Information Governance Manager and a Records Manager. These posts provided much needed extra capacity and expertise for both BAU, GDPR and improvement activities.

11. A summary of the work of the team is set out below:

Area	**Work Undertaken**	**To note**
Training	The team have run **monthly** induction training sessions (twice monthly for the past four months for new staff in Birmingham) for new staff, **quarterly** training and update sessions for the GDC's 'FOI Reps' and ensured all GDC staff completed **annual** data protection training on the GDPR.	The content of the training for new staff was reviewed and updated, making it more GDC specific and more relevant and digestible. Feedback on the updated content has been positive.
Disclosure log	FOI responses are reviewed and appropriate data is published.	The GDC's publication scheme and the team's web pages were also reviewed and updated.
Legal Advice	The GDC's information law solicitor, provided more than **200** pieces of formal legal advice (in addition to advice provided informally and supporting the team more widely) to internal clients on matters relating to the disclosure of information under the FOI, DPA and our own legislation (mainly in relation to FTP).	Disclosure requests for clinical advice reports have been particularly challenging to manage following a change in the case law. Advice on complying with DPA/GDPR requirements was also provided on several research projects involving the collection of personal information and some process changes under the FtP end-to-end review. The volume and complexity of issues advice requests related to increased post GDPR.
Objections to processing	The Data Protection Officer has responded to six formal complaint and objections to the way in which the GDC has processed personal data.	

Information Governance Group	The IGG is part of the GDC's information governance framework and in the first half of the year played an important role in helping to ensure the business engaged with the requirements of the GDPR and related implementation work. In the second half of the year, workshop sessions with the IGG have helped shape the development and roll out of the GDC's Email Deletion Policy and the development of the data security incident reporting, policy, and support framework.	
Records	Work this year has included leading and supporting work on the scanning of records in FTP casework and on the implementation of the GDC's email deletion policy (GDC wide workshops were run to support staff when the policy was implemented). In addition a significant amount of work has been undertaken to create a detailed inventory of the records held by the GDC in offsite storage.	Proposals for the review and disposal of these records in line with the GDC's retention schedule are being drawn up and will be considered by SLT at the start of 2019.
GDPR	More detail about this work can be found in Annex B. To summarise, this work included: • A GDC wide information asset audit • A GDC wide audit and review of conditions of processing • Completion of the GDC's records retention and disposal schedule • Creation of a data processing activities record • Review and update of contracts with data processors • All GDC staff completed GDPR training • Review and update of the GDC's Privacy Policy • The creation of a Data Subject Rights Policy • The creation of an Information Access Fees Policy • The creation of an 'appropriate policy' for the DPA 2018 • GDC wide review and update of consent processes, template letters, web forms, application forms, and policies.	

Review and analysis of Data Security Incidents

2018

12. There was an increase in the number of DSIs reported during 2018, compared with 2017 and 2016. The number of incidents reported last year was considered to be low though because of the backlog of work awaiting assessment in FTP casework at the time. The annual figures are attached at **Appendix 1.**

13. As in previous years the majority of incidents reported occurred in FTP Casework, and in areas of the office that handle large volumes of personal data. Although all areas of the organisation reported incidents, indicating that awareness and use of the reporting system is good. The main cause of incidents continued to be human error. This was often where checks failed to prevent

an DSI occurring. Causes of these lapses are being reviewed and include where people were working under pressure or too quickly and across multiple cases at once.

Data Security Incidents referred to the ICO

14. In 2018, **five incidents** (one involving mental health records, one relating to information in a newspaper article, one where information was disclosed to someone's ex-partner, one involving the loss of study models by Royal Mail, and one relating to a letter appearing to be sent to the wrong registrant) were considered serious enough that we self-reported them to the Information Commissioner.

15. Although the number of serious incidents referred to the ICO has increased in 2018 this should be set in context. Early indications are that all organisations, not just the GDC, will be self-referring more incidents to the ICO following the implementation of GDPR. This is because the threshold for reporting under GDPR is reduced to include any incident where there is a risk to the data subject.

16. In the five incidents the Information Commissioner concluded that the GDC's response and the changes it had implemented as a result were appropriate. On that basis, the Commissioner decided that they should not take any enforcement action.

Information requests

17. During the year 312 requests were also completed. Although down slightly from 2017 (94 2018 113 2017), the SAR requests processed, in particular, were more complex and several were from members of staff involved in the grievance process or from registrants with a long and/or challenging history with the GDC. The annual figures for 2018 (**attached** at **Appendix 2**).

18. 99% (215) of the 218 FOI requests responded to in 2018 were responded to within the statutory timeframes (20 working days) or an extension was appropriately claimed to carry out a public interest test. 97% (91) of the 94 subject access requests responded to in 2018 were responded to within the statutory timeframes (40 calendar days or 30 following GDPR) or an extension was appropriately claimed. This maintains the high standards of 2017 (itself the highest compliance rate for five years) and is a considerable achievement given the volume and complexity of the project work the team also undertook in 2018.

19. FOI requests of note received during 2018, included requests for information about represented and non-represented registrants in FTP proceedings, information about EU and Non-EU registrants, hearing transcripts, costs associated with medical testing, under guise visits in FTP, and FTP throughput times.

20. Requests for information under the DPA in 2018 most often related to a single FTP complaint, for example a copy of the case file usually from the patient (informant) but also from the registrant. We have though received a volume of requests for 'all information held', expert reports, including clinical advice, and individual medical records. We also received several requests from members of GDC staff going through the disciplinary and/or grievance process.

Internal Reviews of our decisions

21. Under the FOI Act organisations are required to carry out an internal review of an initial decision where someone expresses dissatisfaction. In Q4 2018, the GDC received two requests for an internal review. 12 reviews were received and completed in total for 2018 (seven in relation to FOI and five in relation to a SAR). This compares to 19 reviews in 2017.

ICO FOI Complaints and Decisions

22. Of the 312 information requests the GDC responded to in 2018, **zero** FOI responses were appealed to the Information Commissioner (two in 2017 and seven in 2016). This is unusual and speaks to the quality of the team's initial responses and the effectiveness of the internal review process.

23. One subject access case was referred to the Information Commissioner. One complaint was also made to the ICO about the information team's web form requiring requestors to identify whether or not they were a registrant.

Recommendation

24. Council are asked to note the information update.

Annex A

	Q1	Q2	Q3	Q4	Annual Total 2018	Annual Total 2017	Annual Total 2016
DSIs	31	26	45	40	142	94	129
FOI Requests Received	74	54	41	38	207	234	369
FOI Requests Completed	64	61	44	49	218	228	391
SAR Requests Received	21	24	30	23	98	107	102
SAR Requests Completed	18	20	29	27	94	113	80
Internal Reviews	0	8	2	2	12	19	14
Complaints to the Information Commissioner (FOI and SAR)	1 (SAR)	0	0	0	1	3	7

Annex B

Process redesign and implementation

1.1. The final theme translated our findings from the 'Discovery' theme against the context of GDPR to enable the redesign and update of key business processes and implement changes to our customer facing communications and notices. The main deliverable and activities are detailed below:

High priority items updated by business areas to ensure compliance

- Privacy notices added to key letter templates
- Registration application forms
- Online application process
- Webforms – enquiry and complaint
- High priority contracts
- Updates to automated email and telephone line systems

Items updated	Quantity
Standard/template letters	28
Application forms/further information forms	34
Process changes – guidance and SOPs etc	33
Webpages/sites	25
Intranet pages	5
Webforms	6
Business contracts	18
Other (please add more as required)	7
Total	**156**

Figure 1 - Items updated to ensure GDPR compliance

Key items to update

- Standard template/letters: not GDPR time-dependent i.e. CPD audit and Dentist ARF letter templates
- Policies and procedures: part of wider review (i.e. IT and HR)
- 'Lower priority' contracts

Items to be updated	Quantity
Standard/template letters	45
Application forms/further information forms	1
Process changes – guidance and SOPs etc	28
Webpages/sites	0
Intranet pages	2
Webforms	0
Business contracts	10
Other (please add more as required)	0
Total	**86**

Figure 2 - Items to be updated post 25 May 2018

Retention and disposal policy published

- The GDC's retention and disposal policy, once agreed by EMT, was published on the GDC's website within the privacy policy.

Records management recruitment

- A new records manager post was created to support the business in key areas of the business including email retention, records retention and the implementation of the retention policy.

Updated cookie consent process

- Update of GDC's use of consent across its processes – ensuring our processes and basis on which we undertake our statutory duties is clear and informed to the registrants and public

Update of GDC's website cookies and privacy policy

- Each of the GDC's website were updated with more detailed cookie information including the public website, eGDC, Standards, DCS and the online register.

Lawful basis review – shift from consent to regulatory function

- Update of GDC processes and procedures including modification of the use of consent in key registration and FtP processes – addressing GDC's regulatory powers and expectations
- This included an in-depth review of FtP processes and agreed move from 'consent' as lawful basis for processing personal and sensitive personal data throughout FtP processes.
- Updates made to the FtP complaint webforms.
- Adjustments were made to DCS's engagement and information to registrants, clarifying that consent to engage with the complaint process was not voluntary, but actually required under the GDC's Standards.

Corporate contracts – developed and updated

- 20 high priority business contracts were reviewed and updated as required in line with external legal advice.
- Each contract was reviewed based on the service provided and personal information shared and the processing activities as controllers, joint controllers or processors.

Corporate privacy policy

- The GDC's privacy notice was developed following advice from external Counsel and each individual team to create the extensive privacy policy now available at gdc-uk.org/footer/privacy, with a dedicated URL redirection gdc-uk.org/privacy for GDC publications and references.

Fair processing notices - Update of SOPs/templates/implement CRM changes

- 156 items were updated throughout the business focusing on customer focus items were a change in consent, legal basis and sensitive personal data in collected or processed.
- A further 86 items, were identified as requiring further update post GDPR go-live. These have since been updated or will be amended in line with routine or scheduled updates as appropriate.

Subject Access Request and Data Security Incident process reviewed and updated

- The GDC's 'Subject Access Request' process was updated to accommodate the GDPR's change from 40 days to 30 days of processing time.
- A data subject rights policy has been developed to detail the rights individuals have under the new regulations and how the GDC will manage our commitment.
- Data Protection Act 2018 has changed the exemptions the GDC rely on in relation to SARs and the gateway for processing used in respect of enquiries from the police or other regulators. For example, the Information Governance team's standard templates and advice notes etc have been updated.
- A new Data Protection Policy has now been published.

Individual rights process implemented

- Guidance developed and published relating to the individual rights offered through GDPR and the GDC's required consideration of the rights.

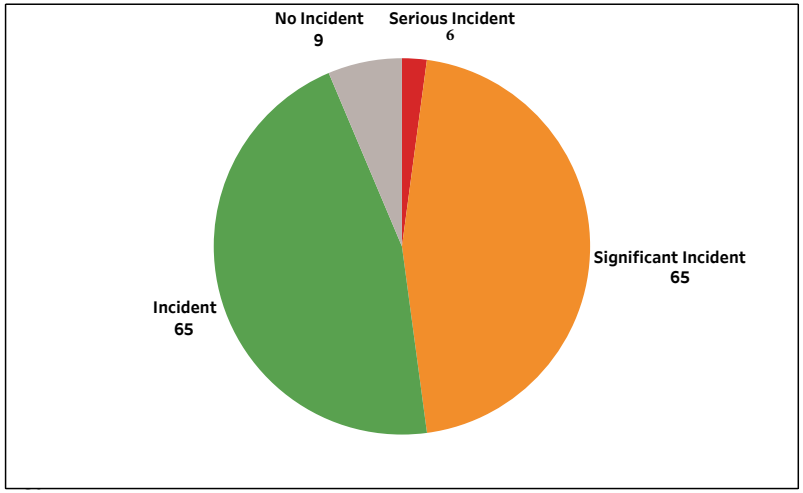
Following delivery of this programme theme, the programme board engaged with the GDC's Compliance team over the course of the summer to review and audit the work undertaken under four main activities. The audit report, published in November 2018, confirmed that the compliance team was satisfied that the programme had met its core objectives**,** and any outstanding issues raised have been addressed or actioned for example via the ongoing GDPR contract update project.

Appendix 1:Annual Data Breach Reporting 2018

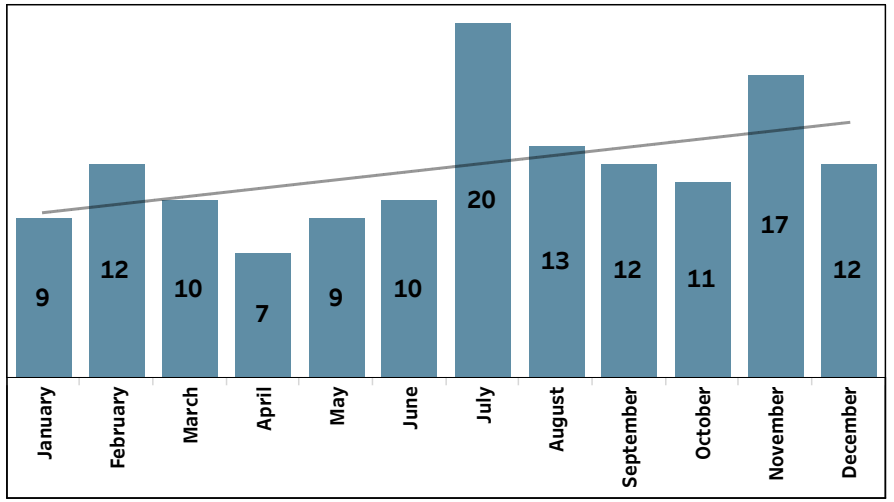
1. Incident Categories and Team Breakdown

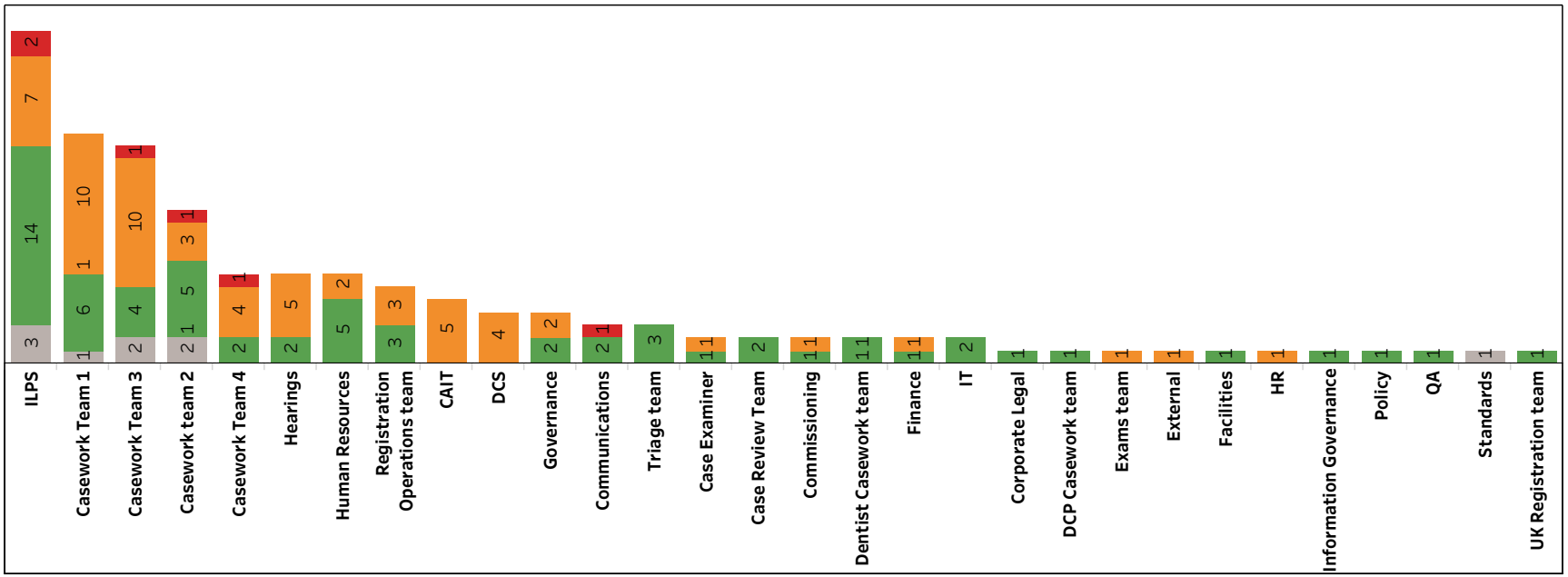
GDC | PMO

Incident Category



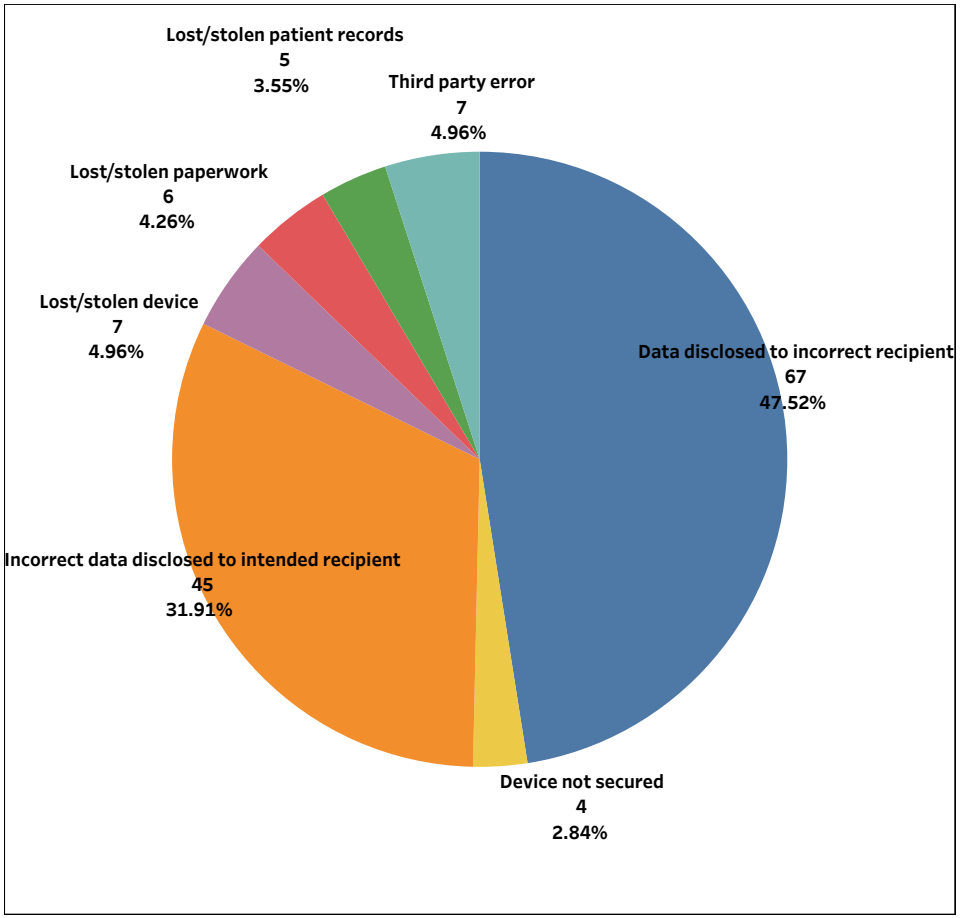
Year totals



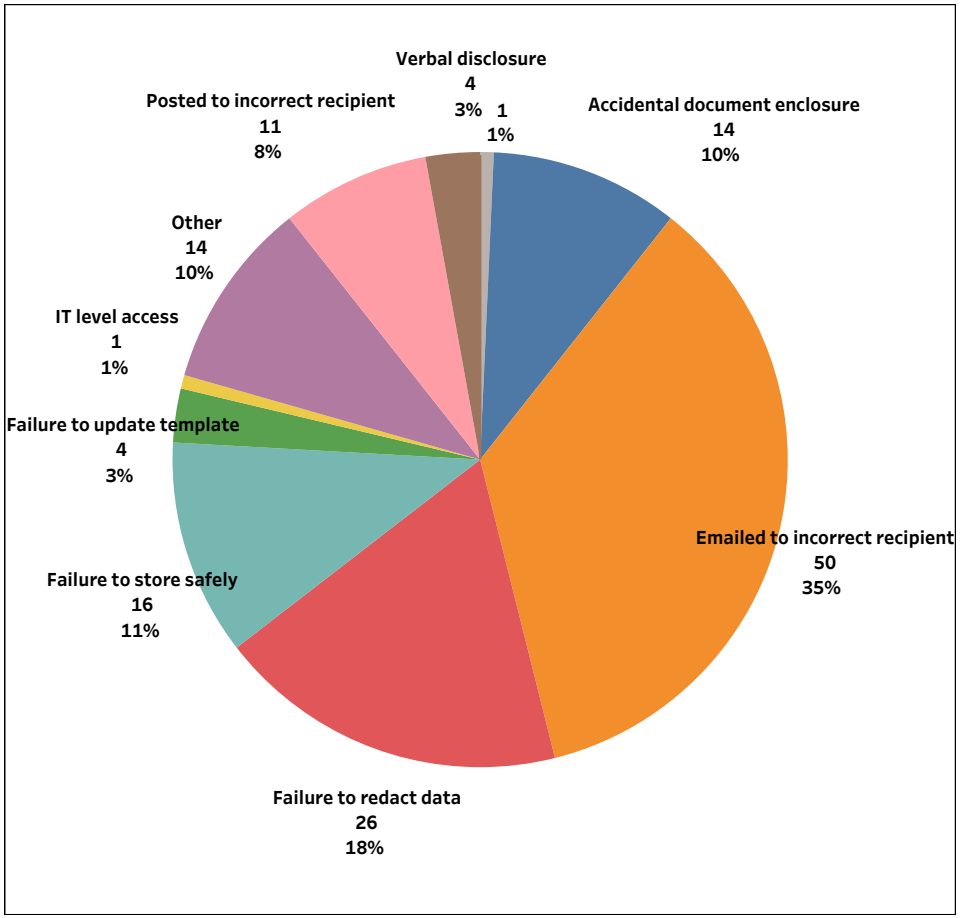


2. Incident Types and Sub-types

Incident Type

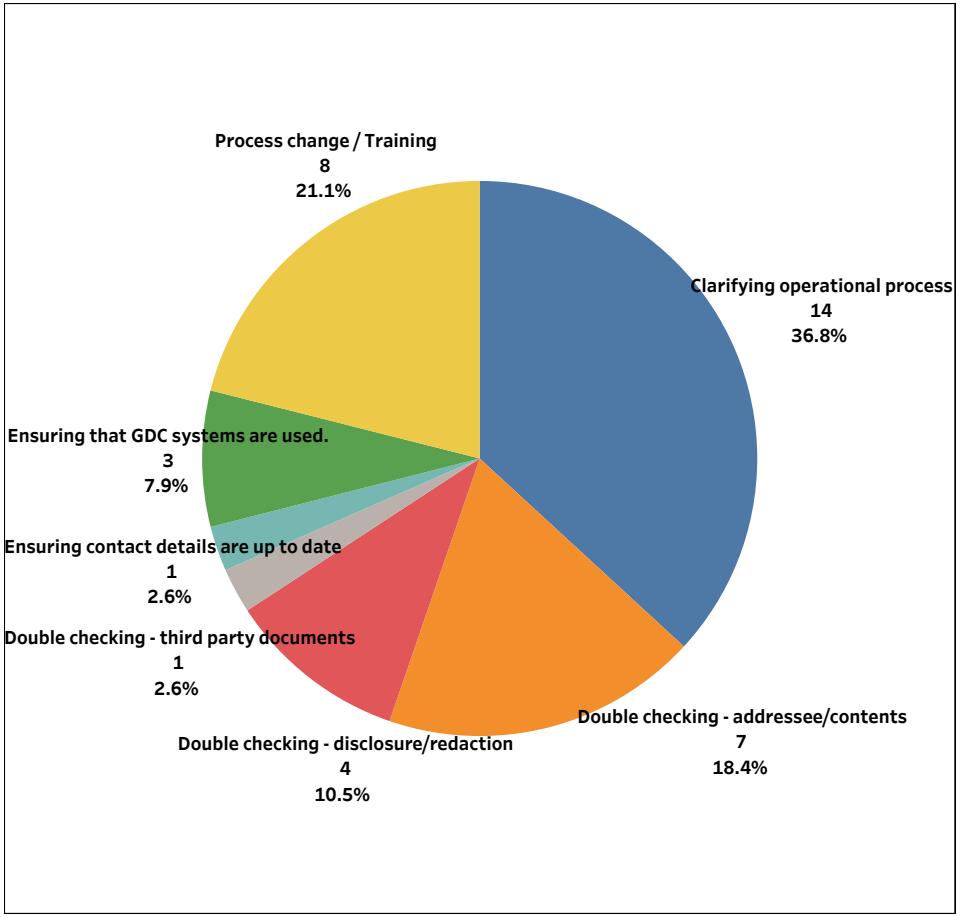


Incident Sub-Type

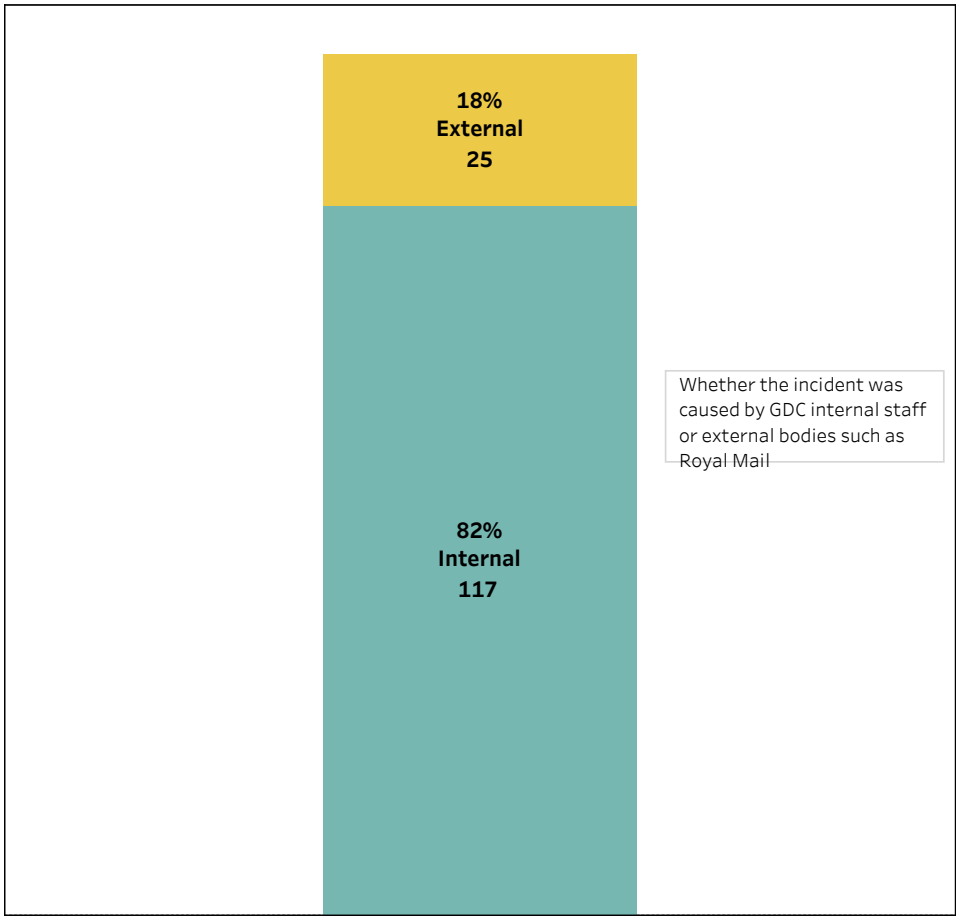


3. Learning Themes, Internal v External

Learning Themes



Internal v External



Appendix 2: Annual DPA/FoI Figures

Headlines for the Quarter

CSR Category1	Q1	Q2	Q3	Q4	Grand Total
DPA Request	18	20	29	27	94
FOI Request	64	61	44	49	218

Headlines for the Quarter - Month by Month

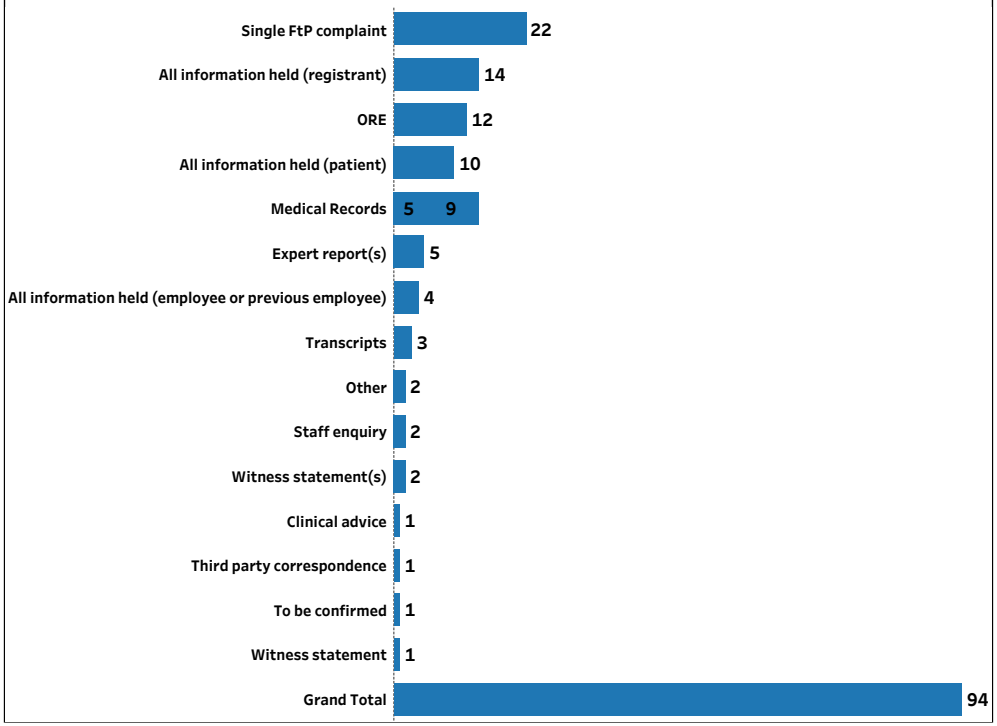
CSR Category1	January	February	March	April	May	June	July	August	September	October	November	December	Grand Total
DPA Request	3	6	9	6	8	6	9	11	9	11	7	9	94
FOI Request	22	20	22	25	18	18	21	16	7	18	18	13	218

Compliance Tracker

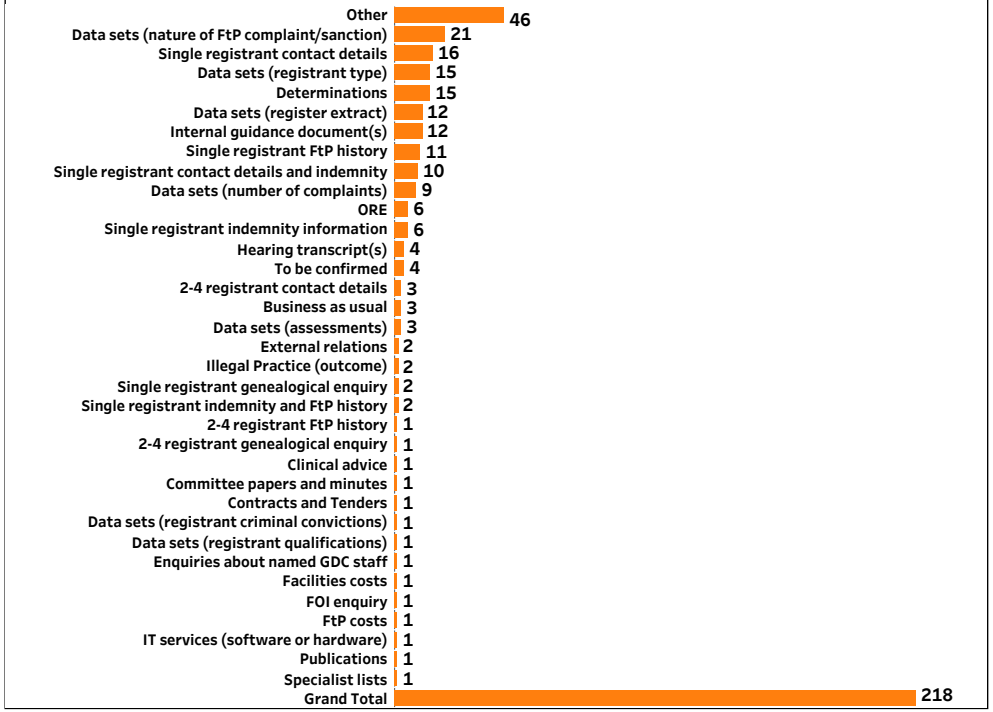
CSR Category1	Cal Days Compliance	Q1	Q2	Q3	Q4	Grand Total
DPA Request	DPA SLA Met	17	19	29	26	91
	DPA SLA Not Met	1	1		1	3

CSR Category1	Work Days Compliance	Q1	Q2	Q3	Q4	Grand Total
FOI Request	FOI SLA Met	63	60	44	48	215
	FOI SLA Not Met	1	1		1	3

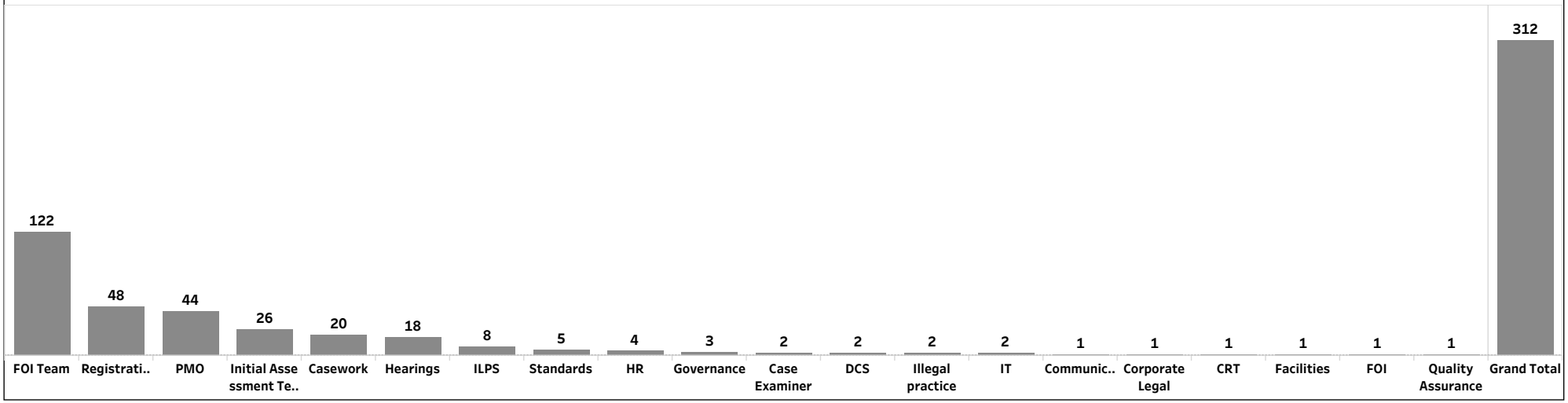
Headline DPA Categories

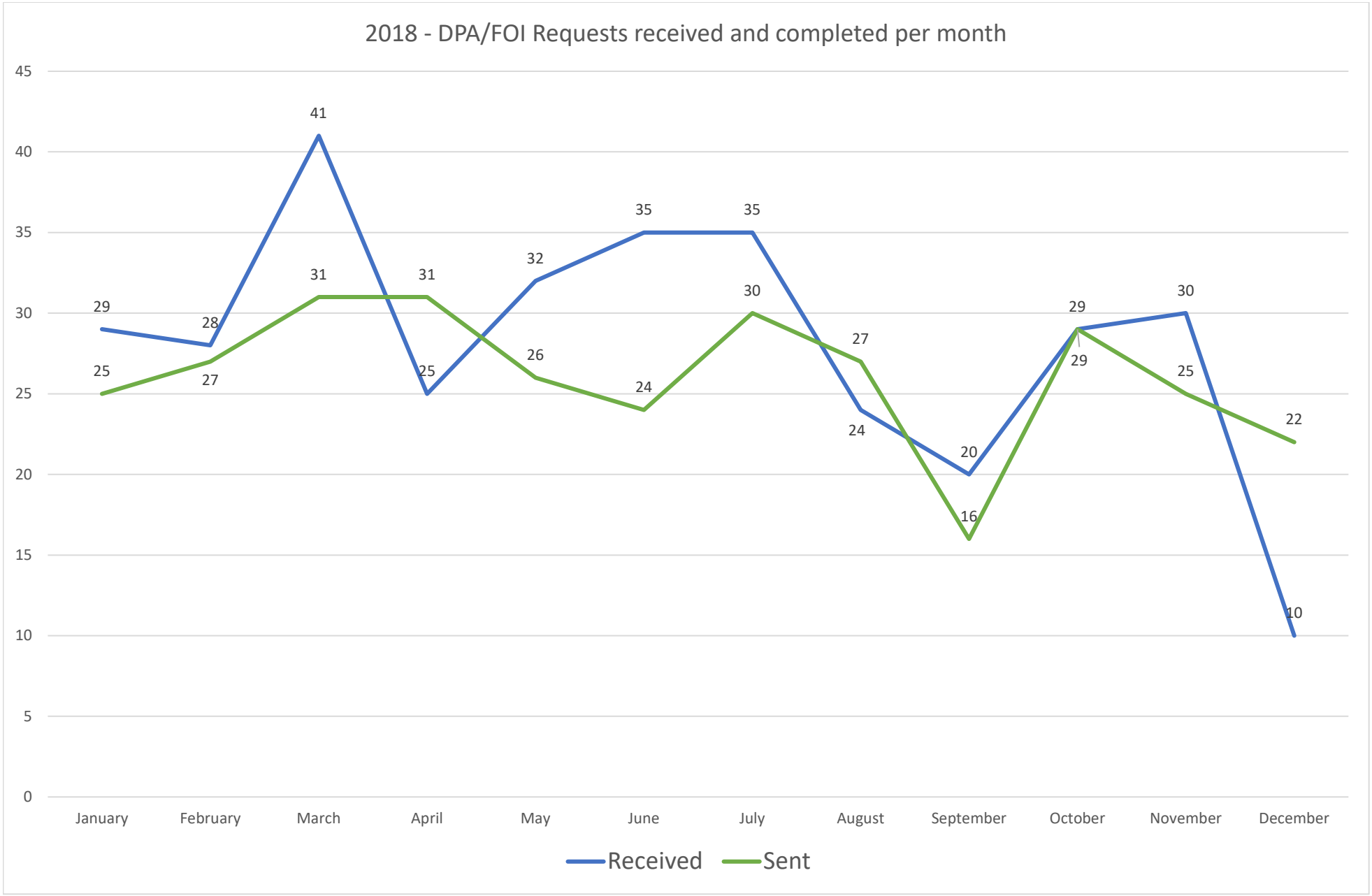


Headline FOI Categories



Total Distribution of Information Requests by Teams




2018 - DPA/FOI Requests received and completed per month
45
40
35
30
25
20
15
10
5
0
January
February
March
April
May
June
July
August
September
October
November
December
29
28
41
25
32
35
35
24
20
29
30
10
25
27
31
31
26
24
30
27
16
29
25
22
Received
Sent