Audit Committee, 10 June 2020

Information Governance Annual Report

Introduction

1.1 The Information Governance (IG) function within the Governance Department is responsible for the HCPC's ongoing compliance with the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR), the Data Protection Act 2018 (DPA) and the General Data Protection Regulation 2016 (GDPR). The Department also manages the HCPC's relationship with the Information Commissioner's Office (ICO), the information rights body.

1.2 FOI and EIR legislation provide public access to information held by public authorities. Public authorities are obliged to publish certain information about their activities and members of the public are entitled to request information from public authorities. Both Acts contain defined exemptions to the right of access, which means that there are clear criteria on what information can and cannot be requested.

1.3 The DPA governs the protection of personal data in the UK. It also enables individuals to obtain their personal data from a data controller processing their data. This is called a subject access request. Data subjects also have certain other rights under data protection legislation. Namely:

- to be informed – the right to be informed about the collection and use of their personal data.
- to rectification – the right to have inaccurate personal data rectified or completed if it is incomplete.
- to erasure – the right to have personal data erased. The right is absolute and only applies in certain circumstances.
- to restrict processing - the right to request the restriction or suppression of their personal data. The right is not absolute and only applies in certain circumstances.
- to data portability – the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- to object – the right to object to processing based on the legitimate interests or performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processes for the purposes of scientific/historical research and statistics.

- in relation to automated decision making and profiling – the right to be provided with information about automated individual decision-making including profiling.

1.4 This report provides an update on IG activity for the period 1 April 2019 to 31 March 2020.

Information requests

2.1 During the reporting period we received a total of 559 requests for information. This is an increase to the total of 478 information requests received in the previous year. A breakdown of the annual figures can be found at Appendix 1.

2.2 94% (248) of the 264 FOI requests completed within the reporting period were responded to within the statutory timeframe of 20 working days.

2.3 92% (186) of the 202 subject access requests (SAR) completed within the reporting period were responded to within the statutory timeframe of one month. We received several more complex requests which required a search of more than one system including some SARs from members of staff. Some delays also occurred when requests are not passed to the Information Governance team within the statutory time frame.

2.4 On 2 December 2019, Social Work England took over as the regulator for social workers in England. Consequently, we have seen the number of information requests reduce by approximately 20%.

2.5 FOI requests of note received during the reporting period included, information about EU and non-EU registrants, registrants with annotations, ethnicity of registrants (which we do not hold information on) and fitness to practise hearing transcripts (under our FOI Policy we charge a fee for transcripts that we do not already hold).

2.6 Subject access requests (SARs) most often related to fitness to practise cases. For example, a request for a copy of the case file, usually from the registrant but also from the complainant. We also received several requests for 'all information held,' expert reports and individual medical records.

2.7 Under the FOIA organisations are required to carry out an internal review of an initial response where someone expresses dissatisfaction. Whilst not specified in the DPA, we also conduct internal reviews of subject access requests where asked. We received 34 internal review requests.

2.8 The team responded to three data erasure requests.

Information incident management

3.1 The HCPC encourages an open incident reporting culture, with an emphasis on analysis and learning in order to identify any weaknesses in our processes and make appropriate changes.

3.2 Since February 2015, all incidents, regardless of how minor they may initially appear, are reported centrally and risk scored. A breakdown of the number of incidents that were reported can be found at Appendix 2.

3.3 In the reporting period, the HCPC recorded 87 incidents. This compared to 79 recorded for the previous year.

3.4 The majority of incidents reported occurred in FTP followed by Registration. These areas of the organisation handle large volumes of personal data.

3.5 The main cause of incidents was human error. This often caused where people are working under pressure and across multiple cases at once.

3.6 No incidents were reported to the ICO.

ICO Complaints and decisions

4.1 Part of the role of the Information Commissioner's Office (ICO) is to improve the information rights practices of organisations by gathering and dealing with concerns raised by members of the public about information rights issues.

4.2 We received six complaints from the Information Commissioner as follows:

- A registrant's personal data was disclosed to an unauthorised third party in a joinder application made to the Conduct and Competence Committee. The registrant also complained to the ICO that their email address was included in an email that was intended only to be sent to internal colleagues. The ICO determined that we should remind our staff that they must make it clear to the people subject to joinder cases that their personal data may be disclosed/ dealt with in this way.
- A registrant's request for rectification was not dealt with within the statutory time limit of one month of receipt. The ICO advised us to take steps to address this infringement to ensure that we respond to individual's requests within one month of receipt. We conducted our own investigation into this matter and found that the request had not been passed to the Information Governance team. We sent a reminder to the department responsible that they should ensure that such requests are passed onto the team without delay.
- In two separate cases we withheld some information in response to two subject access requests. In both cases the ICO decision was that we had correctly applied the DPA/GDPR exemption and they closed the complaints with no further action.
- In verifying a registrant's email address, the complaint to the ICO was that we had disclosed her personal data to an unauthorised third party. The ICO asked that we revisit the way we handled the matter. We conducted our own investigations into the matter. We found that the third party (an employment agency) was listed as her current employer at the time the

verification email was sent, so we concluded that no data breach had occurred.

- A registration application form which had been sent by Royal Mail special delivery service went missing in our office. The ICO was happy with the way we had investigated the concern and the process changes we implemented as a consequence.

Information Governance

5.1 During the reporting period the Information Governance team continued to develop and improve the information governance framework; the way we manage and dispose of information, identify and respond to data security incidents and ensure compliance with the FOIA, DPA and GDPR.

5.2 FOI responses are reviewed, and appropriate data is published online on our FOI disclosure log.

5.3 In October 2019 we updated our Record retention and disposal policy. This contains our retention schedule for the records we keep across the organisation.

5.4 In March 2020 changes were made to our Privacy Notice. The changes now reflect the personal data we publish in the online Register search and that we will share information about fitness to practise investigations where there is a legitimate or statutory requirement.

5.5 During the year, data privacy impact assessments (DPIA's) became a more formal part of our procurement and project management processes. The team has advised and assisted colleagues complete the screening questions and on those pieces of work requiring a full DPIA.

5.6 The Information Governance team works closely with the Chief Information Security & Risk Officer (CISRO) who delivers information security training to all staff (including contractors). Partners and Council members are also asked to complete the training.

5.7 At the time of writing, 98% of staff have completed information security training. The target is for 95% of staff to complete the training.

Decision

The Audit Committee is requested to discuss the report.

Appendices

Appendix 1 – Annual information requests 2019/2020
Appendix 2 – Annual information incidents 2019/2020

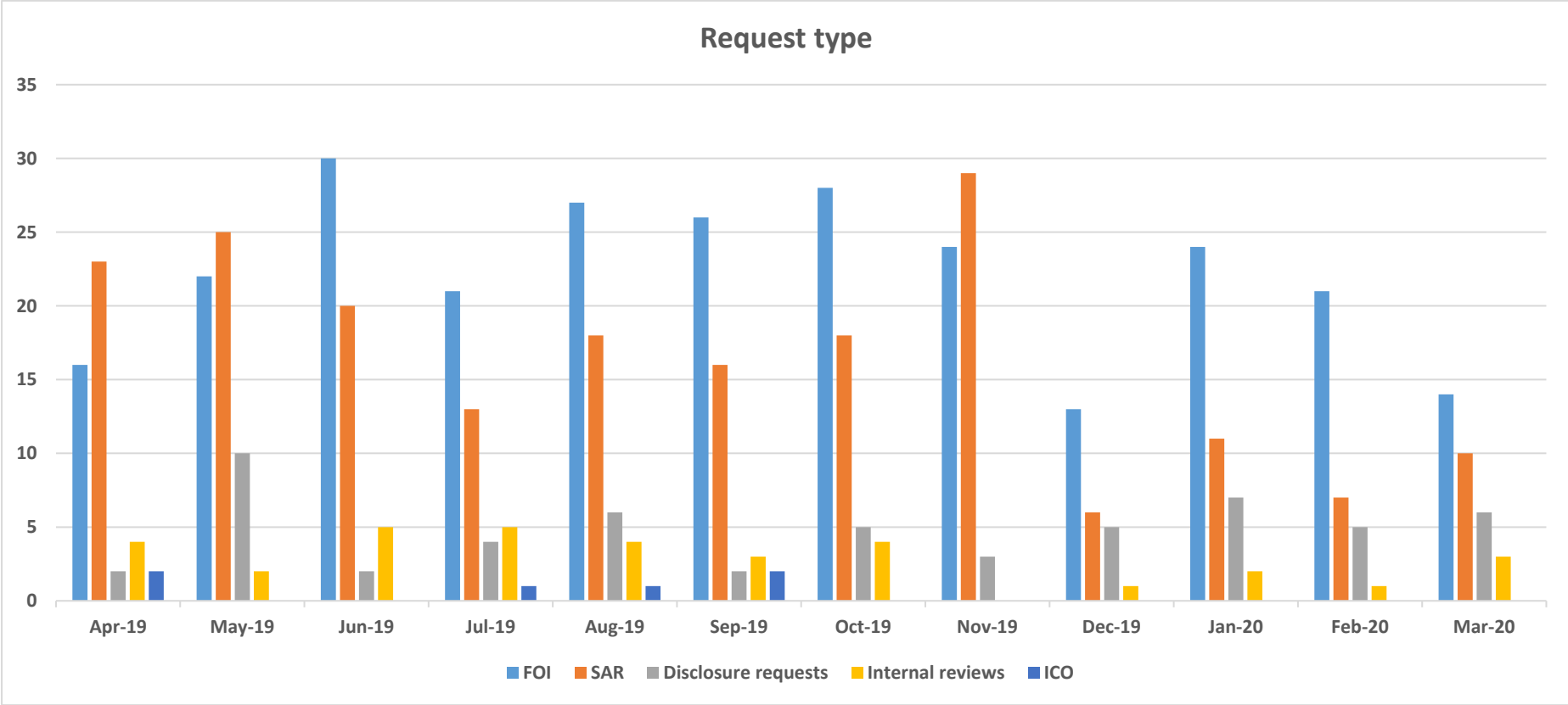
Date of paper

6 May 2020

Appendix 1 – Annual information requests

Table A - All information requests received

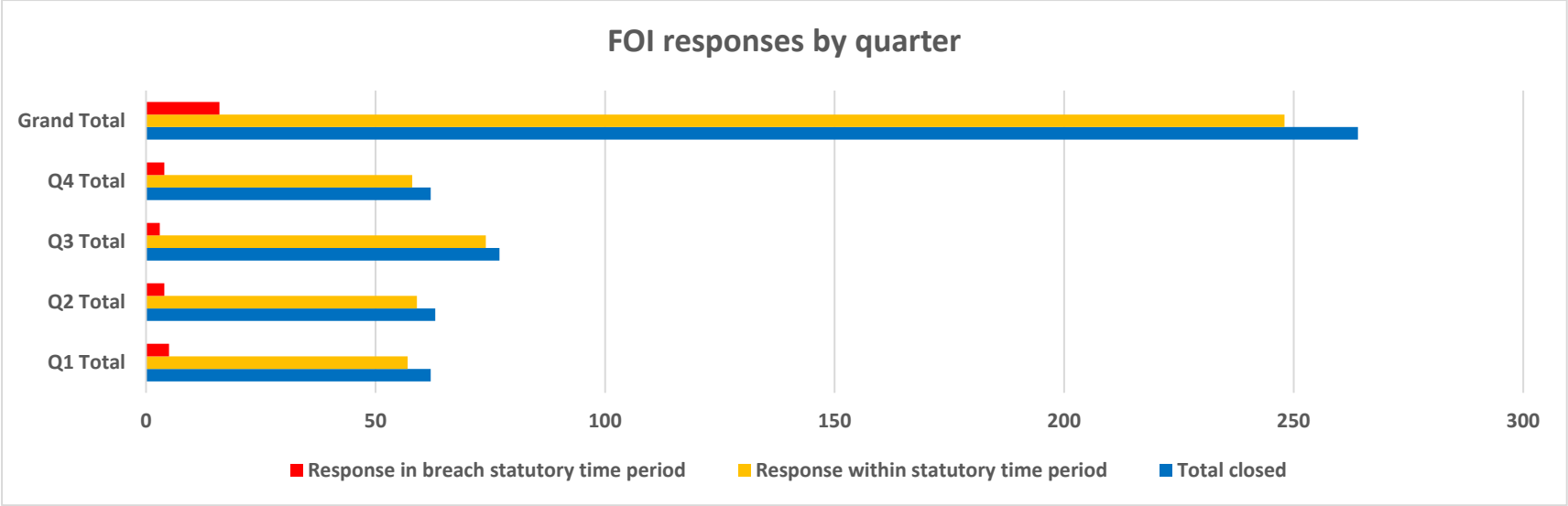
	Apr-19	May-19	Jun-19	Jul-19	Aug-19	Sep-19	Oct-19	Nov-19	Dec-19	Jan-20	Feb-20	Mar-20	Total
FOI	16	22	30	21	27	26	28	24	13	24	21	14	266
SAR	23	25	20	13	18	16	18	29	6	11	7	10	196
Disclosure requests	2	10	2	4	6	2	5	3	5	7	5	6	57
Internal reviews	4	2	5	5	4	3	4	0	1	2	1	3	34
ICO	2	0	0	1	0	2	1	0	0	0	0	0	6
Total requests received	**47**	**59**	**57**	**44**	**55**	**49**	**56**	**56**	**25**	**44**	**34**	**33**	**559**
% within statutory period	**94%**	**93%**	**97%**	**96%**	**90%**	**93%**	**93%**	**94%**	**96%**	**97%**	**92%**	**94%**	**94%**


Request type
35
30
25
20
15
10
5
0
Apr-19
May-19
Jun-19
Jul-19
Aug-19
Sep-19
Oct-19
Nov-19
Dec-19
Jan-20
Feb-20
Mar-20
FOI
SAR
Disclosure requests
Internal reviews
ICO

Breakdown of SAR and FOI requests completed 1 April 2019 to 31 March 2020

Table B – Quarterly breakdown

	Q1 Total	Q2 Total	Q3 Total	Q4 Total	Grand Total
FOI					
Total closed	62	63	77	62	**264**
Response within statutory time period	57	59	74	58	**248**
Response in breach statutory time period	5	4	3	4	**16**
% within statutory period	92%	94%	96%	94%	**94%**
SAR					
Total closed	69	44	62	27	**202**
Response within statutory time period	66	39	56	25	**186**
Response in breach statutory time period	3	5	6	2	**16**
% within statutory period	96%	89%	90%	93%	**92%**


FOI responses by quarter
Grand Total
Q4 Total
Q3 Total
Q2 Total
Q1 Total
0
50
100
150
200
250
300
Response in breach statutory time period
Response within statutory time period
Total closed

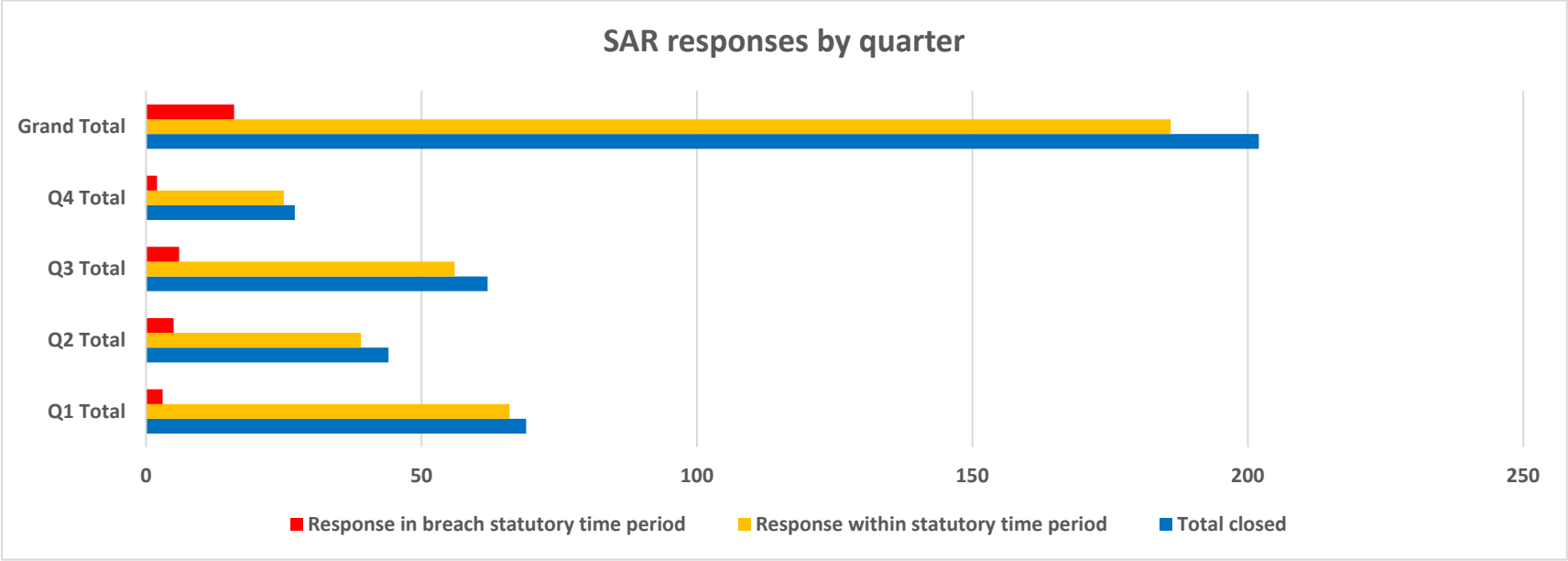
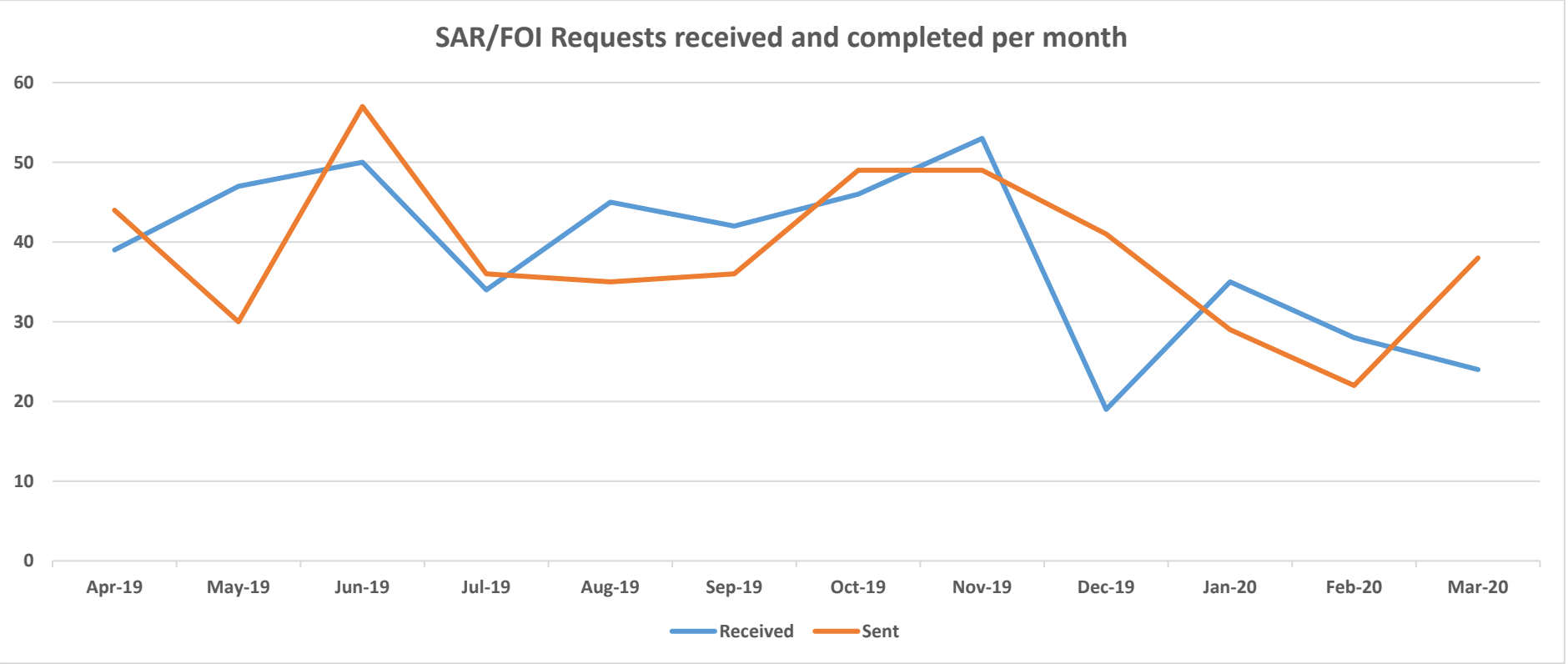

SAR responses by quarter
Grand Total
Q4 Total
Q3 Total
Q2 Total
Q1 Total
0
50
100
150
200
250
Response in breach statutory time period
Response within statutory time period
Total closed

Table C – SAR/FOI Requests completed monthly breakdown

	Apr-19	May-19	Jun-19	Jul-19	Aug-19	Sep-19	Oct-19	Nov-19	Dec-19	Jan-20	Feb-20	Mar-20	Total
FOI													
Total closed	20	15	27	22	20	21	31	25	21	25	12	25	**264**
Response within statutory time period	18	13	26	20	19	20	28	25	21	24	11	23	**248**
Response in breach statutory time period	2	2	1	2	1	1	3	0	0	1	1	2	**16**
% within statutory period	90%	87%	96%	91%	95%	95%	90%	100%	100%	96%	92%	92%	**94%**
SAR													
Total closed	24	15	30	14	15	15	18	24	20	4	10	13	**202**
Response within statutory time period	23	14	29	14	12	13	17	21	18	4	9	12	**186**
Response in breach statutory time period	1	1	1	0	3	2	1	3	2	0	1	1	**16**
% within statutory period	96%	93%	97%	100%	80%	87%	94%	88%	90%	100%	90%	92%	**92%**

Table D – SAR/FOI Requests received and completed monthly breakdown

FOI/SAR	Apr-19	May-19	Jun-19	Jul-19	Aug-19	Sep-19	Oct-19	Nov-19	Dec-19	Jan-20	Feb-20	Mar-20	Total
Received	39	47	50	34	45	42	46	53	19	35	28	24	**462**
Sent	44	30	57	36	35	36	49	49	41	29	22	38	**466**



Appendix 2 – Annual information incidents

Table E- Data incidents monthly breakdown

	Apr-19	May-19	Jun-19	Jul-19	Aug-19	Sep-19	Oct-19	Nov-19	Dec-19	Jan-20	Feb-20	Mar-20	Annual Total 2019/2020	Annual Total 2018/2019	Annual Total 2017/2018
No. of data incidents	3	7	12	7	16	6	3	9	6	8	5	5	**87**	**79**	**66**

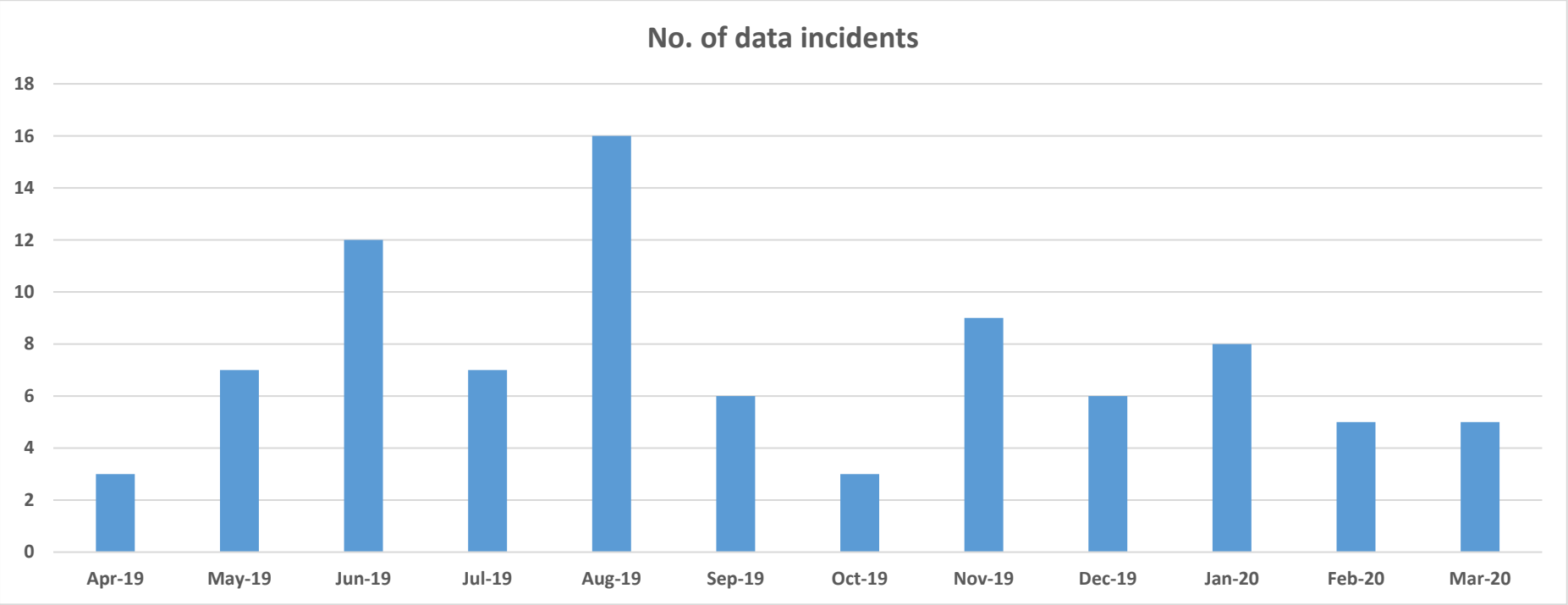


Table F- Data incidents by department

	Finance	FTP	Policy & Standards	Registration	Total
No. of data incidents	4	73	1	9	**87**

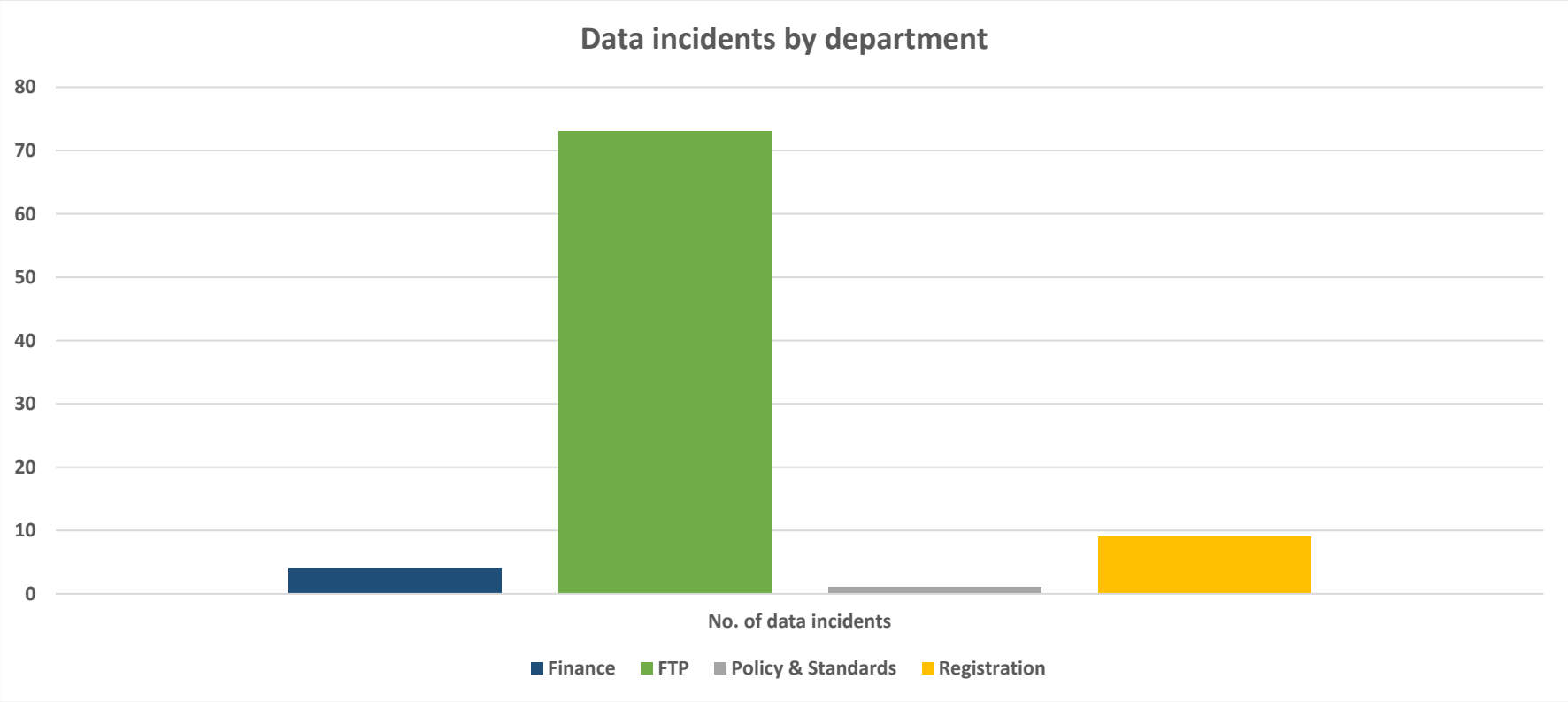


Table G- Data incidents by category