

## ISC16D023

**Title:** Information compliance annual report 2016  
**Author:** Raymond Scott (ISD)  
**Date:** 13 January 2017  
**Circulation:** ISSC - 31 January 2017  
**Agenda:** ISC16A002  
**Version:** Draft v0.1  
**Status:** Open

---

### Issue

To provide an annual report on all activities undertaken by the Information Compliance team including requests received by the University relating to Freedom of Information, Environment Information Regulations, Data Protection and Copyright.

### Recommendation

Recipients are invited:

- To receive the report.

### Resource Implications

This report covers the previous calendar year 2016. The period of the next 18 months through to May 2018 is a time where the University as coordinated by the information compliance team is expected to be preparing for compliance with the General Data Protection Regulation (GDPR) replacing the Data Protection Act 1998. The work required will have a significant impact on the information compliance team, who will also be working with a network of departmental contacts. There is also expected to be an impact on those contacts.

### Equality and Diversity

The report has no impact on groups with protected characteristics.

### Timing of decisions

No decisions are required.

### Further Information

- Raymond Scott (ISD), x3561, [r.scott@uea.ac.uk](mailto:r.scott@uea.ac.uk)

### Background

As a public authority, UEA is required to have processes in place for the receipt, handling and response to requests made under the Freedom of Information Act 2000 and Environment Information Regulations 2004. It also has obligations under the Data Protection Act 1998 and Copyright, Designs and Patents Act 1988. Request management and advice is provided by the information compliance team in ISD, and this report summarises activity over the last calendar year (Jan – Dec 2016).

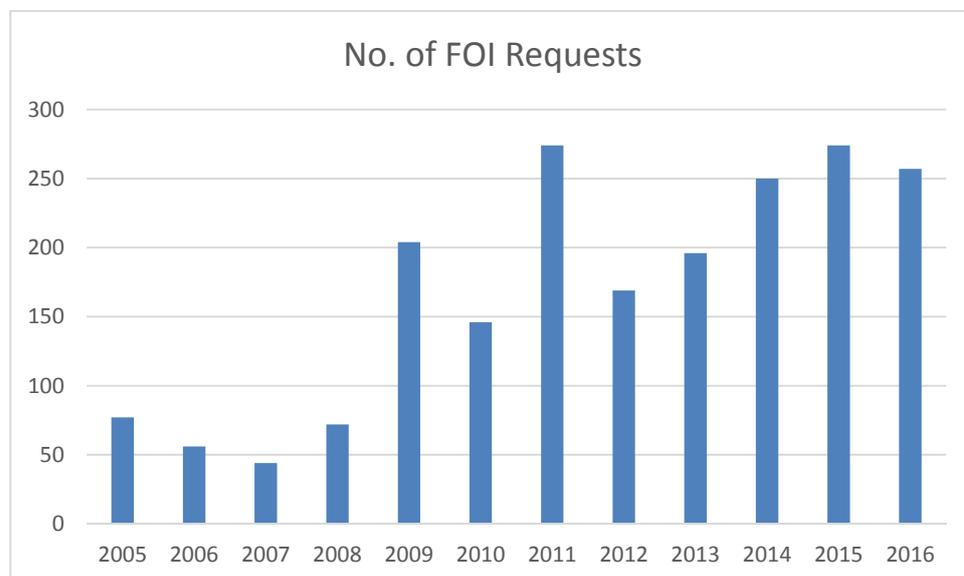
The information compliance team is also coordinating activity in preparation for the application of the General Data Protection Regulation (GDPR). This work is reported to ISSC separately.

## Discussion

### Freedom of Information Act/Environmental Information Regulations

There have been twelve years of requests since the Freedom of Information Act was implemented in 2005.

**Figure 1 No. of FOIA requests received since start of FOI in 2005**



With the exception of two unusual years in 2009 and 2011, and a surge of interest at the start of this period reflecting the initial publicity around the new legislation, the general trend is upwards.

In 2016, we received in total 257 requests for information (a small 6% decrease on 2015). Future years will show whether this is the start of a plateauing trend. Of these, six requests were processed under the EIR.

During the year, there were 3 cases where a requester was dissatisfied with a response and requested an **internal review**.

Where a requester is dissatisfied with the outcome of an internal review, they can register a complaint with the ICO, which may then lead to an **ICO investigation**. Investigations can last a number of years before they are concluded. During 2016, only one request was referred on to the ICO. The request was originally received in 2015, and the ICO ruled that the information should be released.

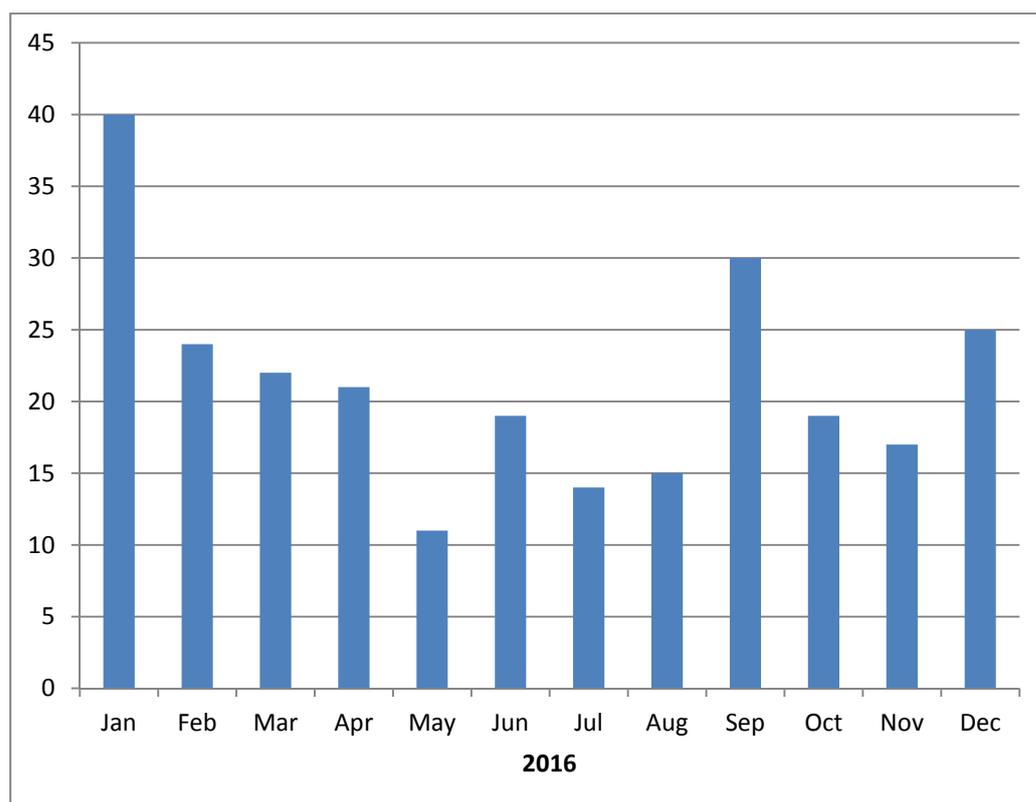
Where a requester is dissatisfied with the outcome of an ICO investigation, the case can be brought to the attention of the **First Tier Tribunal (Information Rights)**. During 2016, we did not need to handle any complaints taken to the First Tier Tribunal.

#### **Changes to FOI request handling**

In 2016 we undertook a review of the FOI request handling process. We now receive additional administrative support, which has enabled one of the IPCMs to dedicate the majority of their time to data protection work, and the planning required for GDPR compliance.

Requests received during 2016 break down as follows:

**Figure 2 No. of information requests per month**



As for previous years, there is no particular pattern to receipt of requests through the year (average 21.4 per month). For example, in 2014, April was the busiest month, in 2015 it was the quietest, and in 2016 it was somewhere in the middle. In 2016, January was the busiest month, mostly due to the receipt of 12 requests from the same requester on a single day. The following day all requests were withdrawn.

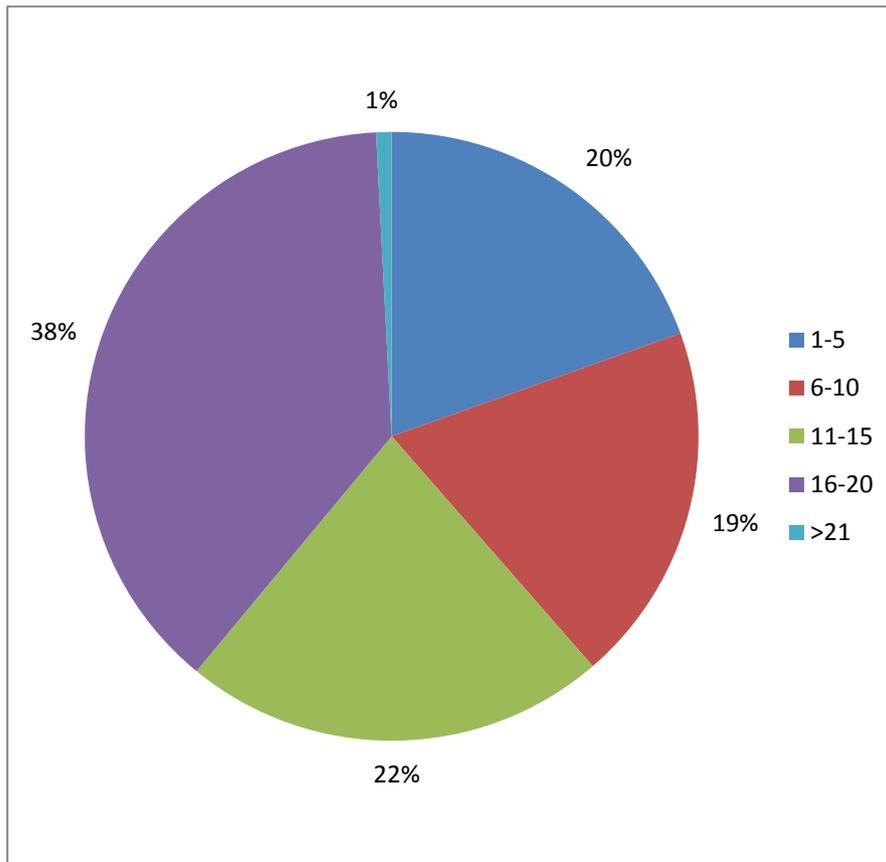
The ICO (Information Commissioner's Office) is particularly interested<sup>1</sup> in ensuring that public authorities provide responses within the statutory deadline of 20 working days after receipt. 99.6% of requests received responses within 20 working days with only one request being provided outside this period. An EIR extension was applied to the one request which took longer than 20 days.

We are expected to provide responses as soon as possible, and therefore look each year to see if we are improving the timeliness of our responses. This can be seen by comparing the percentage of requests completed within 5 and 10 days of receipt. In 2014, 17% of responses were provided within 5 days, in 2015 this was 19%, and in 2016 this was 20%. In 2014, a further 22% were provided within 10 days, in 2015 this was 24%, and in 2016 this was 19%.

It should be noted that the timeliness of responses is not completely within the control the SPC team as the location and retrieval of requested information is the responsibility of the unit holding the information and FOIA requests are often prioritised by those units in a different manner than which the SPC might do. However, procedures within the SPC unit have been amended to monitor more closely the progression of requests and endeavour to push them along more rapidly.

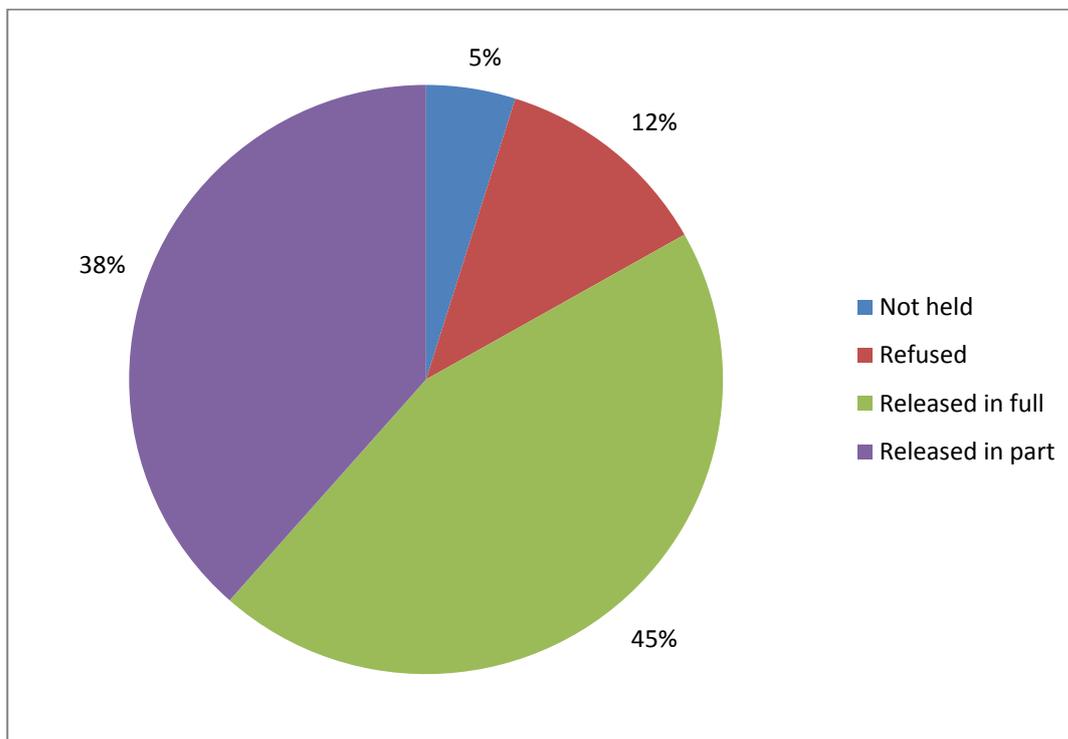
<sup>1</sup> <https://ico.org.uk/action-weve-taken/monitoring-compliance/> The ICO may place an organisation under monitoring if it fails to provide a response within the statutory deadline for at least 85% of requests. The new commissioner, Elizabeth Denham, has spoken of increasing this threshold to 90%. <http://www.bbc.co.uk/news/uk-politics-37201283>

**Figure 3 No. of days to provide a response 2016**



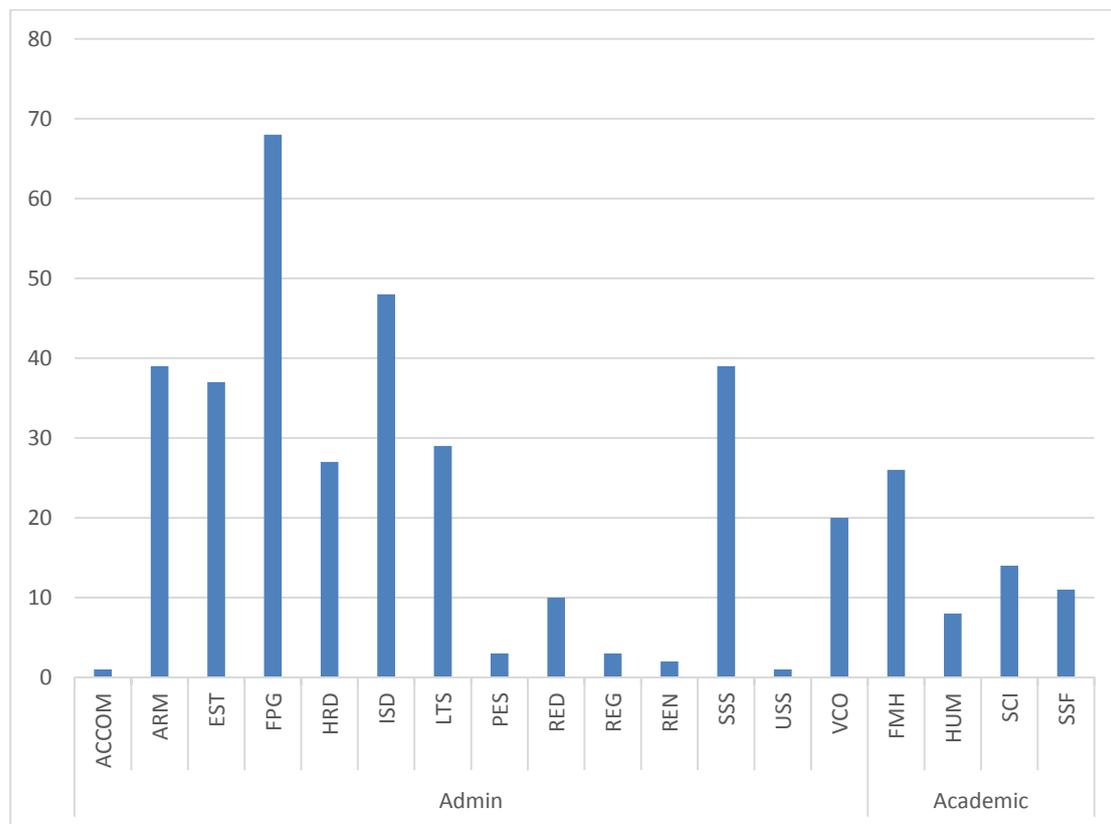
Responses to requests can be: not held at all, not held in part, refused, released in full, or released in part. In 83% of requests, the requester received some or all of the requested information.

**Figure 4 Type of response 2016**



Since 2012, we have been recording a note of those departments involved in the handling of requests so we could present a departmental breakdown of request activity. (Note that some requests might involve two or three different departments.)

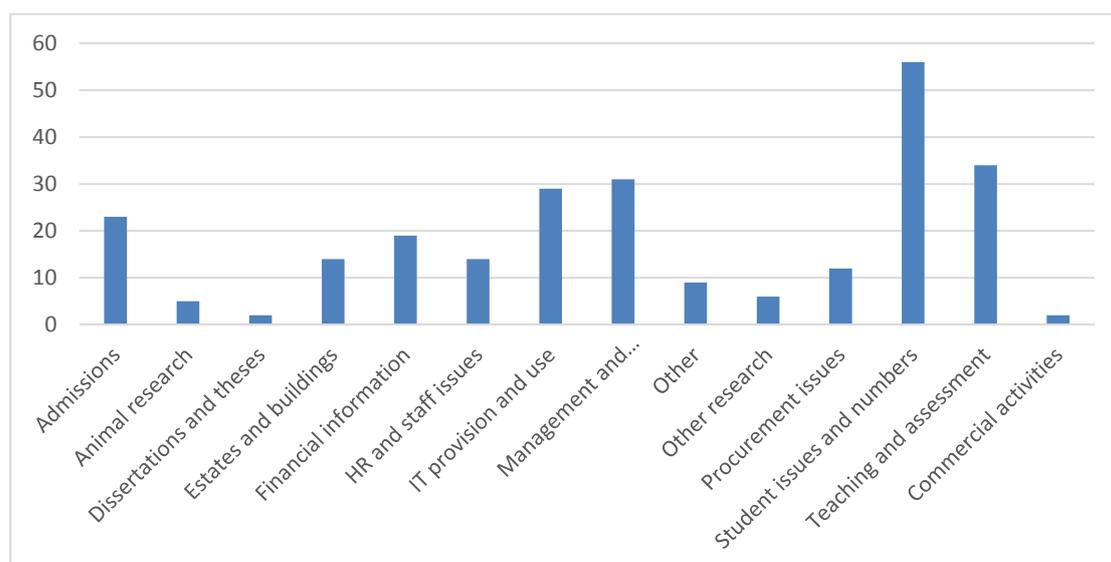
**Figure 5 No. of requests per department 2016**



The busiest department in 2016 was FPG (including finance and BIU), though ARM, EST, ISD, and SSS have all been involved in the handling of 30 or more requests during the year.

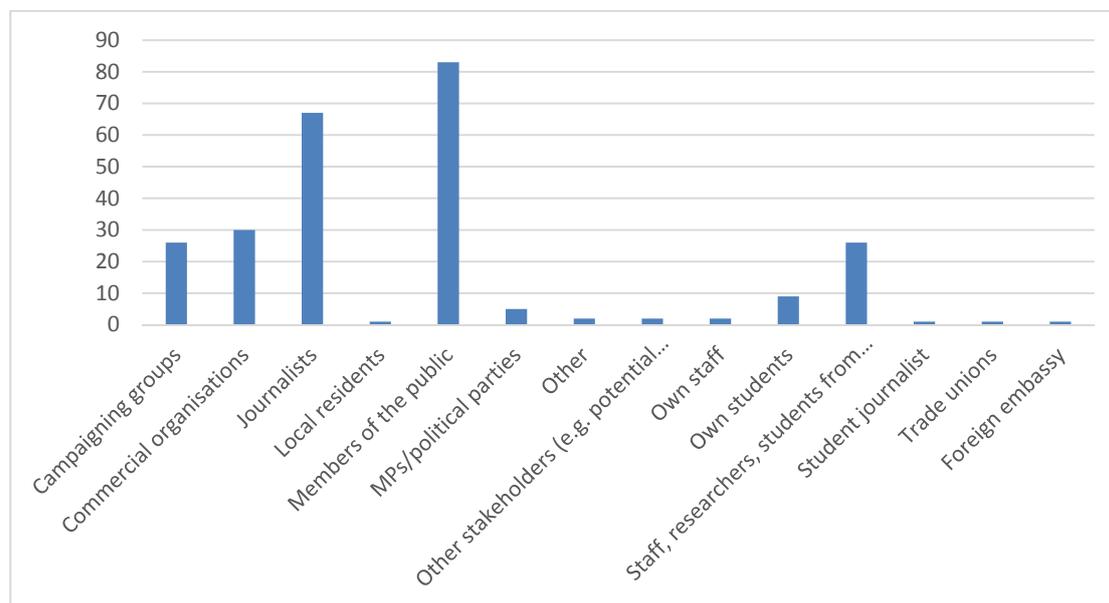
Among academic departments, the busiest is FMH, whose schools were involved in handling 26 requests for information.

**Figure 6 No. of requests by subject area 2016**



Each request is categorised according to a subject area classification provided originally by JISC Infonet and used in the Jisc annual survey<sup>2</sup> of HE information compliance. At UEA, by far the most popular subject is 'Student issues and numbers', followed by 'Teaching and assessment' and 'Management and administration of the institution'. The same subject categorisations are used to organise the Disclosure Log<sup>3</sup> of completed requests for information.

**Figure 7 No. of requests by type of requester 2016**



Members of the public was the largest group of requester, with the second highest category being journalists (the same as for 2015). It is often not clear whether a request has originated from a specific group, therefore 'members of the public' is the default where no other information is available.

Since the start of 2015 we have provided a link to an online questionnaire in our responses, to gather feedback on how requesters feel we have handled their FOI / EIR request. Few requesters have chosen to complete this form, but the four that did so agreed or strongly agreed they were happy with our handling of their request.

### **Data Protection**

While the majority of time spent handling requests for information relates to FOIA/EIR, in 2016 partly in response to the news that a new data protection legislative regime had come into force, we altered the balance of workloads within the team to allow for more time to be spent proactively addressing matters relating to our compliance with the Data Protection Act 1998.

#### *Subject access requests (SARs)*

In 2016, 25 initial requests for personal data, otherwise known as subject access requests (SARs) were received (a small increase on 2015). Fourteen of those cases were actioned as the remaining 11 requesters did not provide the necessary fee or identity verification documentation.

We have 40 calendar days to respond to a SAR. All responses were provided within this timescale.

#### *Breaches*

An increasingly significant part of the role of the IPCM in maintaining our compliance with the DPA, and this concerns advising on data processing and sharing agreements, consent forms,

<sup>2</sup> <https://www.jisc.ac.uk/reports/information-legislation-and-management-survey-2015> Note that Jisc have informed us that the 2016 survey will be the last that they undertake.

<sup>3</sup> <https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies/freedom-of-information/disclosure-log>

and the investigation of personal data breaches. An organisation is expected to keep personal data secure, and where that has not been achieved, we are expected to follow a set procedure covering four stages of breach management: recovery and containment of the lost data; assessment of risk on those affected; notification of the breach to those affected and other bodies (such as the ICO); and evaluation and response to determine the cause and identify remedial action.

During 2016 we investigated 16 data breaches, none of these were notified to the ICO. Brief descriptions of these breaches are provided below:

- Misdirected email with attachment containing sensitive data x 3
- Misdirected email with attachment containing disciplinary action details x 2
- Misdirected email with attachment containing personal data.
- Misdirected email due to incorrect information being held in system.
- Customer feedback email sent out using CC instead of BCC thus disclosing all email addresses to all recipients.
- Email containing personal information of external distributed to mass email lists.
- Unsecured publically accessible website displaying dates of staff absences.
- Unsecured publically accessible website displaying peer assessment details.
- System error which caused a logged in user to see the account details of another user.
- System configuration error which allowed users to view data relating to ex-students.
- Names of staff members were included in an FOIA response due to their inclusion in a free text description field for purchases.
- System configuration error allowed module evaluation comments including names of staff to be viewed by all staff.
- Unencrypted hard drives holding personal data were placed in publically accessible recycling bins without first being securely wiped.
- Unauthorised disclosure of sensitive personal data to external contact.

In addition, notification of insecure practices relating to the handling of confidential waste disposal using blue bins prompted an extended engagement across campus with all users of those bins. In effect, we conducted an audit of the service.

#### *Advice and guidance*

We also provide ad hoc advice and guidance to University staff on DPA, and in some cases, students. (See sections below on enquiry handling and training for further details.)

#### *Research ethics*

The IPCMs also serve as members of the University Research Ethics Committee providing input on data protection issues to the Committee. We attended two such meetings during the year.

#### *Other*

Other notable activities during the year include:

- Recording of activities relating to breaches, data sharing agreements, privacy impact assessments, privacy notices and complaints was organised into a single system. We found that data protection activity may spin out a number of different activities, and we wanted a way of tracking them and linking them together.
- Approval for a new way of conducting searches centrally for material held in Office 365 relating to a request for information. A protocol was drafted and approval for its use was provided by ET-P.
- Planning towards implementation of the General Data Protection Regulations, including allocating specific staff resource, developing a roadmap for compliance.
- We received legal advice from M&R to update our template data processor agreement.
- Creation of a new network of data protection 'champions'
- New guidance was published on the ISD website covering:
  - o Data breaches
  - o Data protection reform
  - o Handling of lost or stolen devices

## Copyright

SPC continue to work with the Library on ensuring compliance with the scanning activities permitted by our CLA licence. Copyright compliance work is increasingly devolved to other parts of ISD, but that we retain a coordinating role, in particular with regard to licences. Answering queries and providing advice and training remains the main work in this area.

Approaches were made to REN to investigate ways in which the training in relation to copyright could be integrated within a larger intellectual property context across UEA.

## Training and support

During 2016, the IPCMs offered 22 one-off and regular training events. Feedback from the sessions has remained positive.

Type of session	Data Protection	Freedom of Information	Copyright
Number of sessions for staff	12	1	1
Number of sessions for students	2	2	2
Total numbers of students attending	45	48	46
Total number of staff attending	148	11	6

During 2016:

### *In-person training*

- A total of 60 persons attended some form of CSED-sponsored information compliance course, compared with 71 in 2015.
- Of the 148 members of staff who attended some form of training, most were support or administrative staff. Attracting academic staff to face-to-face training continues to be a challenge, particularly in regards copyright training.
- 12 different units/Schools were represented in the training.
- SPC once again presented an integrated session for all PGR students in each area of responsibility as part of the PGR PPD programme. Attendance was consistent across all areas with an average of 21 participants per session.
- SPC also contributed information to the ISD component of the new staff conference, which is run three times a year.
- We continued to provide a regular newsletter on all aspects of information compliance, published on the ISD web pages at <https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/news>
- We completely revised the data protection training offered via CSED. Instead of providing one long general session, we trialled splitting the sessions into four shorter, targeted workshops: an introduction (designed to offer an alternative to the online training), a session on sharing data, data security, and using personal data for research and reporting. Feedback was positive and we will continue to work with CSED to ensure staff training is fit for purpose.
- We started to offer specific training on the forthcoming General Data Protection Regulations, and have incorporated GDPR into the revamped CSED data protection offering. Further GDPR training is planned for 2017, including a session specifically for our new data protection contacts.

### *Online training*

In 2015, we publicised the new online training modules as an alternative, or addition, to face to face training. The data protection policy was amended to mandate completion of the DPA training at minimum for all staff handling personal data.

Several departments have engaged well with the training. SPC have supported these departments, as well as other areas, in monitoring training completion. PGR students are also now required to complete online compliance training as part of their PPD programme.

Online training offered	Cumulative total users to date (2015 in brackets)
Data Protection	1081 (570)
Freedom of Information	214 (82)
Records Management	80 (30)
Information Security	2587 (1228) <sup>4</sup>

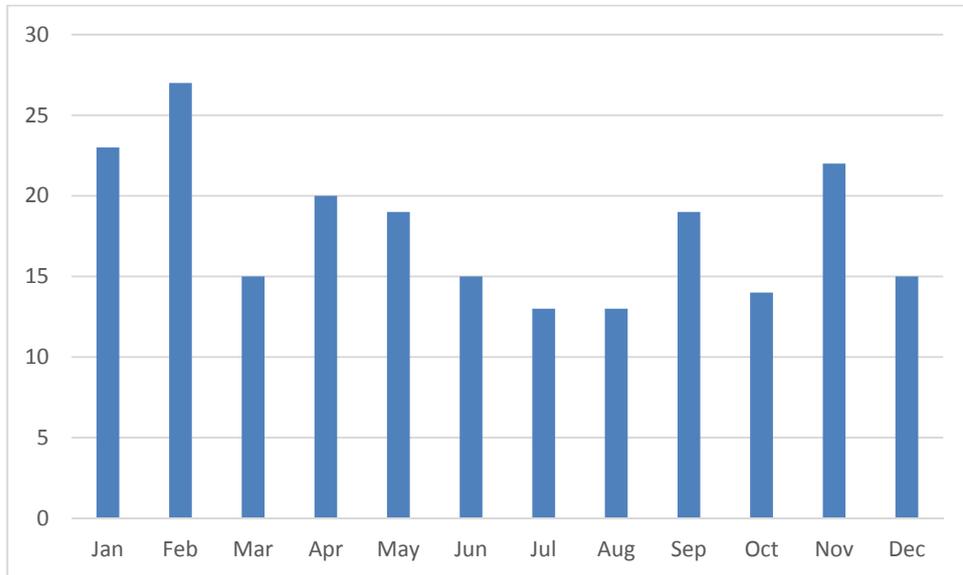
We continue to review all information compliance training available (face to face, ad hoc, online) to identify any particular gaps (subjects for particular audiences) and determine means of closing the gaps on priority areas.

### Enquiry handling

In 2016, we continued to log enquiries relating to information compliance areas, to gain a better understanding of the requirements of the University community and also monitor the time spent responding to these enquiries.

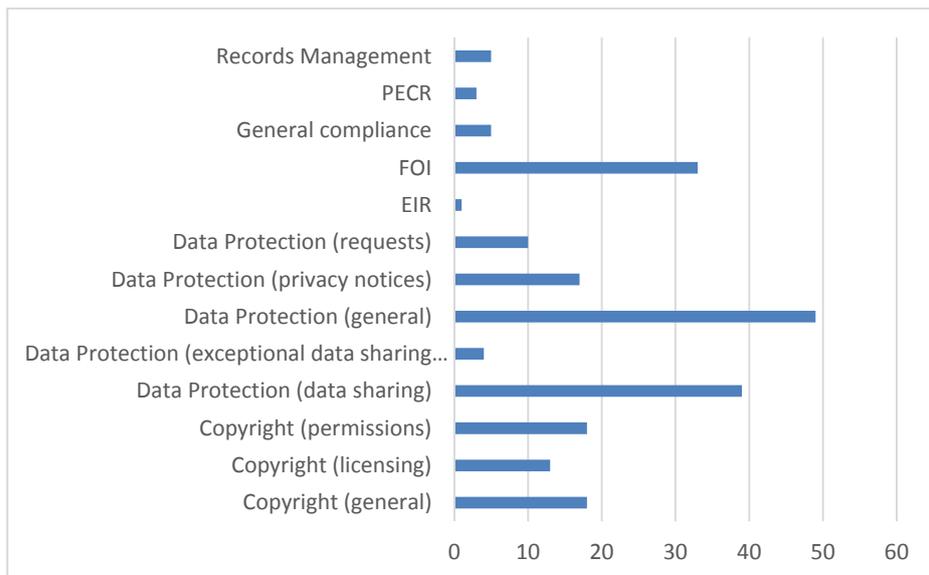
215 enquiries were logged in 2016, a decrease of 15% from 2015.

**Figure 8 Enquiries received by month 2016**

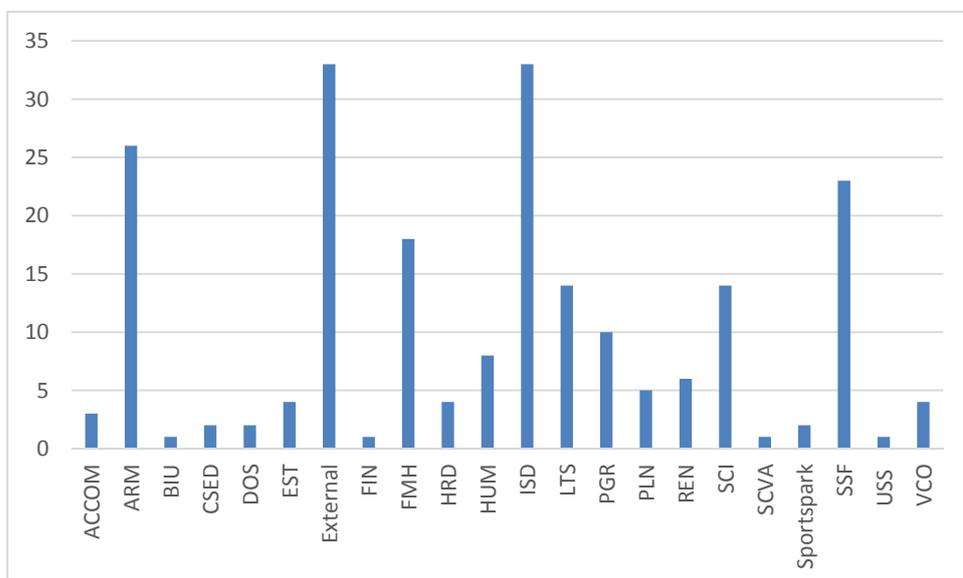


<sup>4</sup> This is a count of the number of people who have accessed the Information Security course. The numbers who complete the course and tests will be fewer. At present, it is not clear how progress is reported from the information for this course in the gradebook.

**Figure 9 Type of enquiries 2016**



**Figure 10 No. of enquiries by department 2016**



**Policy**

In 2016, the following policies were reviewed, updated and offered for approval to ISSC:

- File restoration policy (approved 9 Feb 2016)
- Compliance search protocol (approved at ET-P 23 Nov 2016)