

# Information Governance Annual Report 2019/2020

As Director responsible for Information Governance (IG) and as the Senior Information Risk Owner (SIRO) for the Trust, I am pleased to present the annual report on the Trust's Information Governance arrangements for the 1 April 2019 to 31 March 2020. Key areas of information governance include confidentiality, data protection, records management, freedom of information, information security and cybersecurity.

IG within the Trust provides a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards, in a modern health and social care service. Our staff must be able to deal with the many different information handling requirements, relating for example, to patients, clients and staff. The Trust aims to safeguard patient/client confidentiality and maintain data security whilst empowering staff to perform their role using key information governance principles.

The IG Department faced many challenges during the year particularly around the retention of experienced staff. Two staff members were successful in their

application for promotions within other Health & Social Care organisations. This coupled with the Industrial Action, November 2019 to January 2020 impacted the Department's ability to meet legislative compliance for responding to requests for information.

The Information Governance Team played a vital role in supporting Trust services during the Coronavirus pandemic. This was evidenced through their work with a number of services to enable service users to engage with their healthcare practitioner via virtual platforms; ensure the appropriate sharing of information to enable enhanced community services for vulnerable clients and, through the advice and guidance provided to enable vital COVID-19 research projects to commence in the Trust.

I would like to thank the IG Team for all their hard work and support to the Trust throughout this challenging year.

**Myra Weir**  
Director of Human Resources  
& Corporate Affairs / Senior  
Information Risk Owner



## Key Facts & Figures for 2019/2020

### Subject Access Requests (SARs)

- 5,407 SARs received for access to records
- 86% of SARs processed within legal timeframe.

### Form 81

- 216 Form 81 requests received.

### FOI Requests & Enquiries

- 430 requests/enquiries received
- 77% of requests/enquiries processed within legal timeframe.

### IG incidents

- 219 - IG incidents were recorded on Datix
- 2 - IG incidents were reported to the ICO.

### IG Training

- 2, 811 staff completed mandatory data protection training.

### DPIAs Approved

- 40 Data Protection Impact Assessments (DPIA) were processed.

### DAAs Approved

- 25 Data Access Agreements were approved.

### ICO Communications

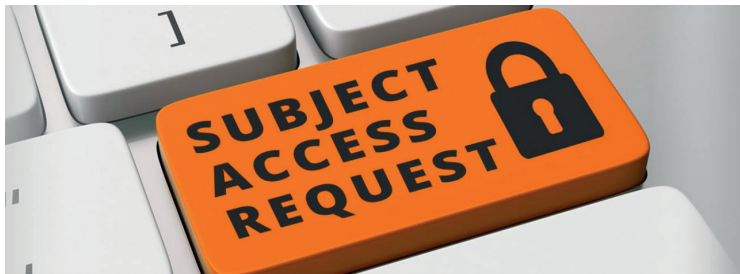
- Six complaints received from the ICO in relation to how information was being handled, the Trust's decisions were upheld by the Information Commissioner. One Tribunal held during this period. Case was withdrawn post hearing.

# Information Governance Structure



The Information Governance Steering Committee (IGSC) is a sub-committee of the Corporate Control Committee. Its role is to oversee the IG strategic agenda and it also has a responsibility to lead and foster a culture that values, protects and uses information for the public good. The IGSC continued to roll-out a challenging programme of work during the year, primarily based around the embedding of GDPR across the Trust.

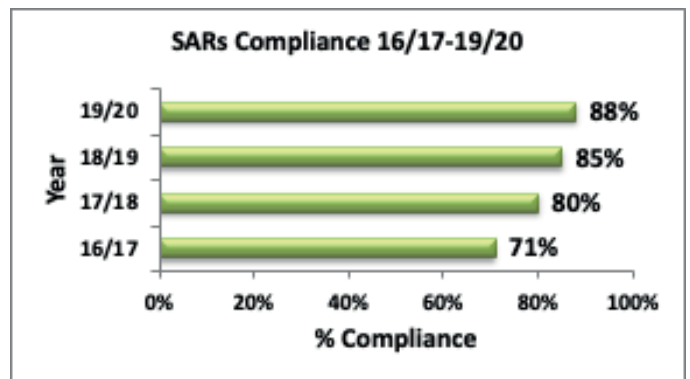
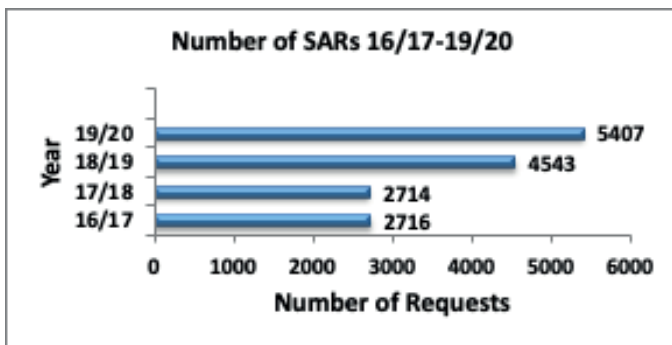
The Trust has appointed a SIRO and a deputy SIRO (Mrs M Weir and Ms R Coulter), 2 Personal Data Guardians (Mr CJ Martyn, Mrs B Mongan), a Chief Clinical Information Officer (Dr D Wilson) and a Data Protection Officer (Miss L McAree). Within the Trust there are 34 nominated Information Assist Owners (IAOs) who are at Assistant Director level. They are supported in their role by Information Asset Assistants (4<sup>th</sup> level management tier).



## Subject Access Requests (SARs)

A key part of data protection legislation allows individuals to request a copy of any personal information we hold about them. The number of SARs received by the Trust increased by 19% in 2019/2020.

The majority of requests are received from individuals or their advocates. On average the Trust receives 450 SARs per month.



The Trust is legally obliged to respond to SARs within a defined time period, ie. within a calendar month for routine cases, or if the request is complex, this can be extended by a further two months. A complex case is defined regionally as a request that *“crosses one or more services, involves more than one volume/file of records, requires retrieval from hybrid systems, ie. manual and electronic, requires redaction or pertains to historical information”*.

SARs received by the Trust, particularly requests relating to family and child care and social work records, are generally considered complex. These records require significant review and redaction and due to the complexities and voluminous nature of the work involved, and the sensitivity of the records, delays in responding to requests have incurred.

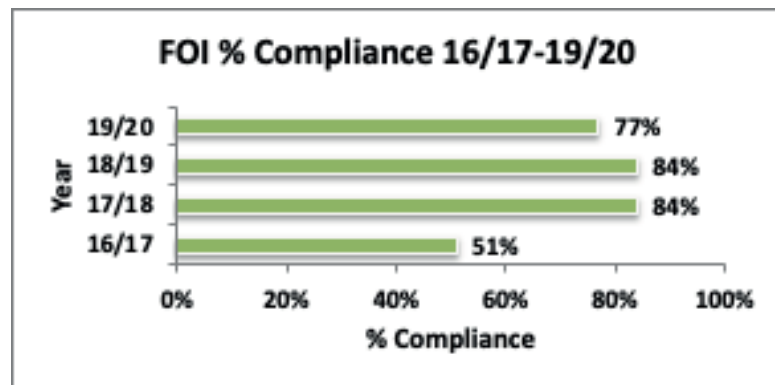
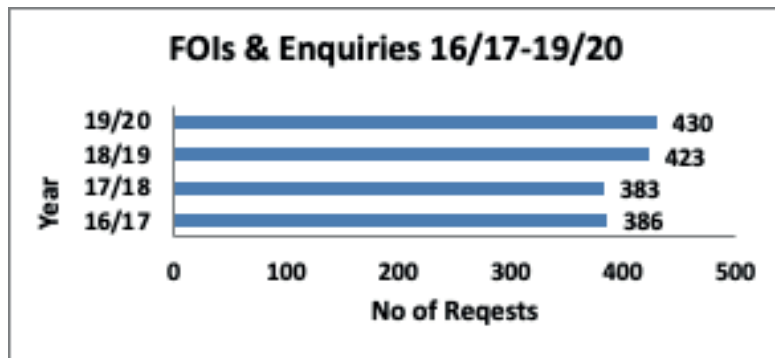
Despite the 19% increase in requests, the compliance rate increased to 88%. The previous year recorded 85% compliance.



## Freedom Of Information Requests (FOI)

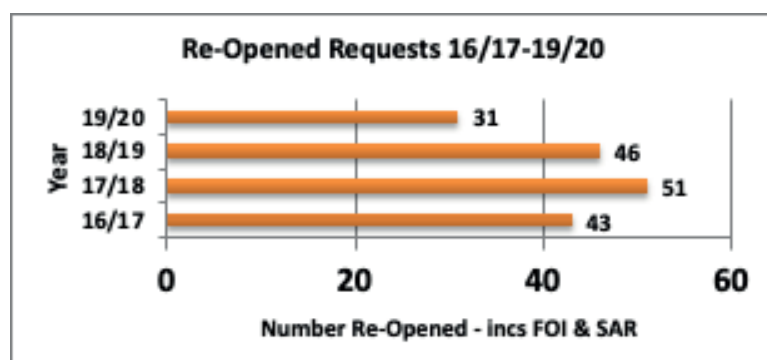
Under the FOI Act individuals have a legal right to access information held by the Trust, subject to certain conditions and exemptions contained in the Act.

The volume of FOIs received by the Information Governance Department averaged 35 per month with a large volume of requests coming from the media, [whatdotheyknow.com](http://whatdotheyknow.com) and commercial organisations. This is consistent with previous years. With regard to trends identified in the requests received, a significant number of FOIs relate to contract expiry dates, incident management and reporting, services provided in the community, activity management across the acute sector and staffing levels and reliance on locum and agency staff across disciplines and the associated costs.



Whilst there was a 2% increase in FOI activity during 2019/2020, compliance fell to 77%. The previous year recorded 84% compliance. This may be attributed to the impact of Industrial Action November 2019 – January 2020 (Q3) and COVID-19 pandemic (Q4).

A total of 31 requests were re-opened during the year, as the requester was dissatisfied with the response or sought further clarification in respect of their initial request. There was a 33% decrease on the number of re-opened cases in comparison with previous year.



## How well did we do?

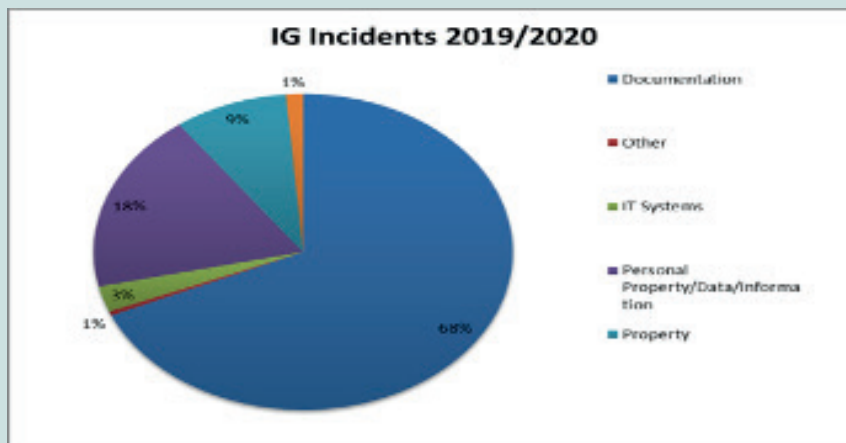
The Information Commissioner's Office (ICO) refers cases to the Trust if complaints have been received from members of the public. In 2019/20 6 cases were submitted for investigation to the ICO. The outcomes for the period 2016/17 - 2019/20 are summarised below:

Data Protection complaints	Complaints Received	Complaint Upheld	Complaint Not Upheld*	Request to take action
19/20	6	-	6	No
18/19	1	1	-	Yes
17/18	6	-	6	No
16/17	3	-	3	No

\*Agreed with Trust actions

### IG Incidents

In accordance with the GDPR legislation, the Trust is required to report any personal data breach that is likely to *“result in a risk to the rights and freedoms of natural persons”*. IG Incidents are reported in line with the Trust's incident reporting system. Throughout the year 219 IG breaches were recorded via Datix Web. This represents 1.4% of all incidents recorded by the Trust. Many relate to breaches of service users' confidentiality caused by inappropriate handling of personal data, e.g. Mis-sent emails, information sent to wrong individual, etc.



Of the 219 IG incidents reported, 2 met the criteria for reporting to the ICO.

Data Breaches reported to the ICO by year					
2019/20	2018/19	2017/18	2016/17	2015/16	2014/15
2	7	4	0	3	2

There is a clear requirement to ensure all staff are aware of the need to report any data breach to the information governance office as soon as possible. Both cases were reported to the ICO within the legal timeframe of 72 hours.

Both incidents were reported to the ICO as records missing, believed lost, damaged or stolen.

Learning from incidents is regularly published through IG Awareness updates and the Information Governance Steering and Lessons Learnt Committees. Examples will also be incorporated into the mandatory data protection training.

# TRAINING



## Information Governance Training

Data protection training is mandatory within the Trust and can be taken as e-learning, in classroom or as customised training. The IG e-learning module has been revised in accordance with the requirements of GDPR. As at 31 March 2020, figures indicate that the uptake for Information Governance training is 50%.

## Organisational Controls Assurance - Information Governance

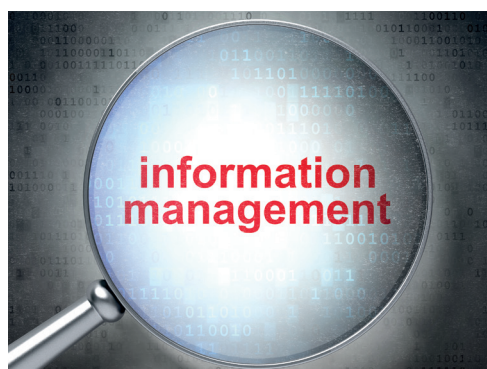
In 2018/2019 the Department of Health (DoH) introduced a new annual assurance programme for HSC organisations which included a standard for Information Management (IM). HSC organisations are now required to maintain the best practice standards set out in the guidance document in order to be able to both provide assurance to the DoH and for BSO Internal Audit purposes. BSO Internal Audit will continue to audit HSC organisations' IM compliance on a periodic basis.

In addition, the Trust's Information Governance & Information Technology & Telecommunication Departments undertook a joint audit of information systems in line with Internal Audit's recommendation (2014). Four systems were audited, and all recommendations raised through this audit have been addressed.

Each Directorate holds an extant information asset register and, in accordance with the IGSC's programme of work, each Directorate ensures that information risks are considered in conjunction with the Trust's Risk Management Strategy.

The Trust's Information Governance Department has also worked closely with the DoH, the Trust's Business Continuity Department and EU Exit lead to prepare for the end of the EU Exit transition period (December 2020) and any required mitigations to ensure the continued flow of health and social care information with EU countries and the Republic of Ireland in particular.

The Information Governance Department as part of the Risk Management & Governance Directorate was re-accredited as Investors in People (IiP) compliant, February 2020 and retains ISO accreditation.



# Information Commissioner Officer (ICO) Northern Ireland Health & Social Care (HSC) Trust Training Review 2019



In July & August 2019 the ICO undertook an audit of data protection training across all HSC Trusts. This consisted of an online survey which ran from June – August, 2019 and follow up telephone conversations with Trust staff. A summary of the ICO recommendations are listed below:

- The ICO welcomed the development of the Information Governance (IG) team and recommended comprehensive IG / Data Protection (DP) training for staff should be provided in a timely manner, to enable the team to operate with a high level of knowledge
- The Trust should consider providing resources for a dedicated IG/DP trainer to sustain and improve training compliance
- Efforts should be made by the Trust to raise the current training compliance rate of 80%
- The Trust should consider promoting access to protected training time to allow completion of training
- Ensure a mechanism is in place for review and monitoring uptake of training
- Consideration to be given to undertaking more frequent refresher training, currently required every 3 years
- The ICO acknowledged the range of awareness raising activities observed across the Trust.

A comprehensive action plan for the above recommendations is being progressed and is reviewed through the IGSC and reported to CCC.

## ICT & Cybersecurity

With dedicated cyber security teams now in place both locally and regionally, the Trust has benefited from an increased sharing of knowledge and cyber alerts between colleagues. Most recently, the COVID19 pandemic has resulted in the healthcare sector becoming a direct target of cybersecurity attacks, with an increase in COVID related phishing campaigns and ransomware attacks. Having the measures in place to protect the Trust from such attacks and increasing awareness to all staff is an ongoing process the cyber team will be continuing with into 2021.

Cybersecurity remains on the Corporate Risk Register.



## Information Quality

The Trust has a strong focus on data quality and its importance for patient safety.

The central training team work closely with information management teams and information technology colleagues to provide support and guidance to staff that are based across acute and community areas.

Within clinical coding area, performance is best in the region.

Performance is 100% against the standard “Clinical Coding to be completed within 3 months of discharge”. The number of clinical codes applied to an episode of care is a key indicator of coding quality. During 2019/2020 the average number of codes applied by the Coding team was 5.6 codes per episode of care against a regional average of 5.2 and the national recommended average depth of coding of **3.5**.

The information teams across acute and community areas provide regular data quality reports to service areas and data quality is monitored on a weekly basis. The Trust is also utilising Qlik software to identify data anomalies in real time.

Health and Care number coverage for 2019/20 was maintained at 99%.

The Trust continues to focus on data quality and its importance for patient safety. The Performance and Information team are working closely with the regional Data quality group that reports to the regional Information Standards Board to monitor data quality and take the necessary steps to continually improve. The Trust has been involved in the production of the annual regional data quality report and works with the regional team to address key areas of concern via a regional work plan. This includes work with groups such as the demographic improvement group, the data standards working group and the expediting of implementation of regionally agreed technical guidance across all its sites. It is recognised regionally that data quality requires a continual focus and increased resources to deliver sustained and improved data quality. Processes are in place to highlight areas for data quality improvement and to avoid errors occurring at source.



**Information Governance**

**Lough House, Ards Hospital, Church Street, Newtownards, BT23 4AS**

**T: (028) 9151 2201**

**E: [informationgovernance@setrust.hscni.net](mailto:informationgovernance@setrust.hscni.net)**