South Eastern Health and Social Care Trust

Paper No. SET/40/18	
	Tick One ✓
For discussion	
For approval	
For information/noting	

Date of Trust Board Meeting: 21 June 2018

Confidential or Public Agenda: Public

Agenda item: Update on implementation of General Data Protection Regulation (GDPR)

1.0 Introduction

This paper provides a final update on the Trust's implementation of the new General Data Protection Regulation (GDPR) which came into force on 25 May 2018.

Miss McAree, Head of Information Governance & Directorate Support attended Trust Board on 27 September 2017 to brief members on the requirements of the new Regulation and the impact of same on the Trust.

Attached with this paper is an updated copy of the Trust's GDPR Action Plan.

2.0 Background information

As a public body, the Trust has a statutory responsibility to know what personal data is held, how and why we process it, who has access to it, and with whom it is shared. This requirement has been strengthened by the Regulation, particularly around the need to demonstrate accountability.

As a data controller and processor of personal data, the Trust takes its responsibilities for processing personal data seriously and has a robust information governance structure in place.

In preparation for the new Regulation, the Information Governance Steering Committee (IGSC) which includes Directors, Assistant Directors and Senior Managers from across the Trust oversaw the implementation of the Trust's GDPR Action Plan (copy attached). This plan complemented the Regional Health & Social Care (HSC) GDPR Action Plan.

In addition, the Data Protection Act 2018 received Royal Assent and its main provisions (immigration, law enforcement, national security & responsibilities of the Information Commissioner's Office) were also brought into effect on 25 May 2018. This paper will however concentrate on the Trust's compliance with the GDPR (the Regulation).

3.0 Brief summary of key points regarding General Data Protection Regulation (GDPR)

Both the Regional HSC and the Trust's Action Plans were developed in line with the Information Commissioner's Office (ICO) *12 Steps To Take Now* (May 2017) and included the need to revise and update for example, the Subject Access Process; the review of contract terms & conditions; the revision and issue of Fair Processing Notices (FPNs); the review of extant policy / procedure and the review and updating of Data Protection training. Awareness raising was also a key component of the Trust's action plan.

As at 31 May 2018, the Trust is confident that it has significantly progressed and implemented the necessary changes with regard to the *12 Steps*.

In an effort to further assure compliance with the Regulation, Internal Audit will be auditing aspects of the new Regulation in August/September 2018 across all HSC Trusts and the results of this will be reported back to a subsequent Audit Committee.

Below is a synopsis of Trust's progress with the *12 steps* using a self-assessed compliance rate. Further information on the detail of each of these steps is highlighted below in summary format and in detail in the attached action plan.

Step 1 – Awareness – 100% Compliance

- *To ensure the Trust Board/Executive Management Team and Managers are aware that the law is changing and the impact this is likely to have.*

Step 2 – Information Held – 95% Compliance

- *To ensure the Trust documents what personal data is held, where it came from and who it is shared with.*
- *To ensure accuracy of information held and processes are in place to allow for correction of inaccuracies.*

Step 3 – Communicating Privacy – 100% Compliance

- *Ensure that we tell people what we do with the information we hold on them via a Fair Processing Notice.*

Step 4 – Individual Rights (Erasure & Data Portability)

- *Not a significant HSC issue at this time.*

Step 5 – Subject Access 100%

- *Update procedures & plan how to handle requests with timescales and provide any additional information.*

Step 6 – Legal Basis for Processing Personal Data – 100% Compliance

- *Identify the lawful basis for processing activity, document it and update your privacy notice.*

Step 7 – Consent – 100% Compliance

- *Review how consent is obtained.*

Step 8 – Children Conditions applicable to child's consent in relation to information society services – (allowing children access to internet)

The Trust does not gather ID data when visitors link to Trust wifi.

- *Not an issue for the Trust at this time*

Step 9 – Data Breaches – 100% Compliance

- *Ensure data breach management processes are put in place to detect report and investigate a personal data breach.*

Step 10 – Data Protection by Design & Data Protection Impact – 90% Compliance

- *Ensure Privacy Impact Assessments (PIA) are undertaken when necessary.*

Step 11 – Data Protection Officer – 100% Compliance

- *Designate someone to take responsibility for data protection compliance and assess where this role will sit within the Trust's structure and governance arrangements (this role is held by the Head of Information Governance – Miss Lynda McAree).*

Step 12 – International – 100% Compliance

- *Where cross-border processing is being carried out, need to determine lead data protection supervisory authority.*

Over the coming months, the Information Governance Department will monitor compliance with new process particularly our ability to meet the 30 day compliance rate for dealing with Subject Access Requests. The Information Governance Steering Committee will continue to receive regular updates in respect of both the Regulation and the provisions of the Data Protection Act 2018.

4.0 Recommendation/s for the Trust Board (please state if the paper/s is for information/noting or for approval by Board members)

Trust Board is asked to note progress with the implementation of the GDPR. The Internal Audit report on GDPR compliance will be shared with the Audit Committee in due course and implementation of any actions will be monitored by the Information Governance Steering Committee.

Lead Director: Mrs Myra Weir

Designation: Director Human Resources & Corporate Affairs/Senior Information Risk Owner (SIRO)

Date: 31 May 2018