Reference	BOT21.FEB.24
Date	3rd February 2021

Board of Trustees

Data Protection Report

Report from the Chief Operating Officer

FOR NOTING

The Board of Trustees is asked to note the contents of the Data Protection Report.

1. Summary

1.1 Since the introduction of the 2018 Data Protection Act changes have been made to ensure the institute complies with data protection regulations and has the culture characteristic of an organisation where the protection of personal data is a business priority.

1.2 Since the last meeting of the Board of Trustees there has been two data breaches. The breaches were not reported to the Information Commissioners Office (ICO). One breach involved a colleague accidentally accessing unauthorised information on an internal HR system and the other two members accessing cached website information on two other members through a failure in the DDoS software. Limited data was accessed, none of which was sensitive and the software faults responsible for bot have been rectified.

1.3 Following one of the breaches reported to the BOT in February a claim for damages was received from the solicitors acting for a data subject. Solicitors engaged by our insurers advised the claim had no merit and this was communicated to the claimant. A further representation was received in the form of a Subject Access Request. Despite the difficulties of dealing with the request when offices were closed it was complied with fully. The data file provided has not been access but a further damages claim was received and has been dismissed by our solicitors.

1.4 Although good progress has been made in ensuring there is greater data protection compliance within the institute the recent data breaches have indicated the need for continued actions to support compliance. SET have identified this as a priority and work is underway to improve the institutes regulatory compliance.

2. Progress on Data Protection Compliance

2.1 In May 2018 the Board of Trustees were made aware of long running non-compliance with the 1998 Data Protection Act including:

- The institute was not registered with the ICO as required by law.
- Unclear or inadequate data protection responsibilities and roles.
- No adequate British Standards accredited procedures or facilities for storing and destroying documents containing personal data or confidential information.
- Lack of institute wide understanding of the importance of securing personal data.

- Evidence of un-audited locally held databases where personal data was collected, held and processed in contravention of legal requirements.
- Poor housekeeping procedures and lack of visitor control compromised data security.
- There were data breach incidents of a frequency and seriousness well above the levels seen in comparable organisations.

2.2. A great deal of activity has been committed to putting in place processes and procedure to meet existing legal obligations and comply with the introduction of new regulations under the 2018 Data Protection Act and the EU General Data Protection Regulation GDPR. This activity has included:

- The introduction of the institutes CRM which provides a central, compliant data collection and processing solution incorporating the legal need to obtain permission from data subjects as well as provide them with data access and meet their right to removal.
- Investment in the latest Microsoft GDPR modules for the CRM through BOT reserves funding (Written Resolution WR19/JUL/01).
- Decommission all non-compliant databases.
- A new data breach reporting procedure with SET and BOT transparency.
- Online data protection training modules completed by all RTPI colleagues annually with a knowledge test based audit.
- Introduction of a revised 'Data Privacy Statement'.
- Data sharing agreements set up for all major supplier partners.
- Introduction of a revised Data Retention Policy.
- Auditing and housekeeping of digital file storage systems to meet subject access requests and data removal.
- Recruitment of a qualified part time Data Protection Officer to deliver audit, training and reporting in line with ICO requirements.

3. Data Breaches

3.1 Despite the investment and activity data breaches continue to occur. There have been two breaches since the last BOT Data Protection Report (BOT20.SEP.23). The details of all breaches are recorded in the Data Breach Log (see appendix). Data Breaches recorded in this log comprise of:

	Number of Breaches	ICO Reportable Breaches
2016	2	-
2017	1	-
2018	11	1
2019	7	1
2020	6	-
2021	1	-

3.2 SET reviews all reported breaches. The 2018 DPA requires some breaches to be reported to the ICO for investigation and SET takes the decision on whether a breach should be reported. Reporting is based on the severity of the impact on the data subjects and the sensitivity of the data released. In 2018 and 2019 breaches were reported to the ICO but no action was taken by them against the institute. SET allocated £15,000 to support the data cleansing that was necessary as a result of the 2018 breach. A prosecution by the ICO or a Data Subject could

result in a significant fine, damages, restrictions on the institutes ability to collect, store and process data and reputational damage. A reportable breach may increase the likelihood of a future ICO investigation or audit.

3.3 BOT is immediately informed of all breaches reported to the ICO and informed of all breaches in written reports at BOT meetings. SET agreed the most recent data breaches were not reportable.

3.5 In January 2020 a breach occurred when P45 documents for two former members of staff were mailed to a third former employee by mistake. The recipient immediately destroyed the documents and informed the RTPI. In line with obligations under the DPA the two data subjects were informed of the breach with the reassurances from the investigation, resulting actions and likelihood no personal data was in fact breached. One data subject subsequently made a claim for damages resulting from the distress caused by the breach. Advice from our insurers legal advisers was that there was no merit in this claim and they wrote to the claimant to this effect. No further representations have been received regarding this claim but a Subject Access Request (SAR) was received on April 16th. This request involves providing c4,000 items of data, mostly emails all of which require redacting for other personal data. The exercise to complete the data retrieval, review and redaction involves c175 hours work in order to respond in the three-month legal time period.

3.6 Whilst this exercise was handled by a colleague it is obvious that the Institute does not have the resources to deal with investigations of this sort. It should be noted that this was an example of a very small data retrieval and redaction. It is estimated that even for an average exercise between 875 and 1,100 hours would be required. In future external resources will be brought in to deal with requests and SET have put aside an annual budget of £20,000 in connection with this.

3.7 The data file provided has not been accessed but a further claim for damages was made which our solicitors dismissed. No further communication has been received from the claimant's solicitor.

3.8 The continued high number of data breaches suggests there is still a problem to address. In January 2020 SET took the decision to increase the risk score for Risk 02 (Failure to comply with data protection legislation) and Risk 19 (Data assets compromised) in light of the breach. New actions are being implemented to mitigate the increased risk, return the risk scores to an acceptable level and introduce a data protection culture characteristic of an organisation passionate about protecting its most sensitive asset. Further activity is planned in 2021 to look at strengthening compliance with all regulatory obligations across the Institute.

4. Health and Safety Implications

There are no Health and Safety implications.

5. Equality and Diversity Implications

The inability to collect personal data will compromise the ability of the RTPI to fulfil its EDI agenda. This data is more likely to be characterised as 'sensitive' personal data. Members need to be confident that this data is protected in line with data protection laws.

6. Resource Implications

Resources have and will continue to be made available to support compliance with all legal and regulatory obligations across the Institute.

7. Governance and Compliance Implications

The RTPI seeks to comply with the 2018 DPA at all times.

8. Communications Implications

Members will be kept informed of their rights under the 2018 DPA and the collection, storage and processing of personal data will be undertaken in a way that is legally compliant and does not compromise cyber security.

9. Corporate Strategy - Climate action

Whilst there are no direct implications, the work to remove documents in favour of safer digital records has implications for reduced print, ink and paper use.

10. Corporate Strategy - GROWPLAN

Member confidence in their Institute to comply with legislation and protect their data will support trust and member retention.

11. Corporate Strategy - Digital Transformation

Digital solutions like the new CRM will continue to be used to create safer data storage and retrieval processes. The risks associated with cyber security increase all the time. New software is being used to protect the Institute and its data assets from cybercrime.