Ref	BOT21.JULY.11
Date	Thursday, 22nd July 2021

RTPI
Royal Town Planning Institute

Board of Trustees

Data Protection Report

Report from the Head of Human Resources and Compliance

FOR NOTING
The Board of Trustees is asked to note the new data breaches as set out in section 03 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 data protection report in April 2021 there have been two data breaches. The breaches were not reported to the Information Commissioners Office (ICO). Further information about the breaches can be found in section 3.

1.3 Since data breach reporting was adopted the record of breaches is as follows

	Number of Breaches	ICO Reportable Breaches
2016	2	-
2017	1	-
2018	11	1
2019	7	1
2020	6	-
2021	4	-

1.4 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. This request was complied with although to date the data provided has not been accessed. Instead a further threat of legal action was received and the institute's solicitors advised reaching a settlement with an offer of £1,500 compensation (costs inclusive). The offer was made and rejected. On the advice of our solicitors and insurers, the institute has now made an offer of £500 plus reasonable costs and we await a response.

1.5 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 identified this as a priority and work is underway to improve the institute's 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.
- New and improved e-learning data protection training modules will be rolled out during July 2021. The training will be completed by all RTPI colleagues and Trustees annually with a knowledge test based audit.
- Time will be set aside in all colleagues diaries every month to complete a suite of e-learning modules and refreshers covering a variety of essential matters including data protection, health and safety and cybersecurity.
- 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. Recent Data Breaches

3.1. In April 2021 and email intended for two membership assessors was sent querying comments in a PCS assessment. Unfortunately, the email went to a different individual who had the same name as one of the assessors. This resulted in a name, membership number and comments on

an application to be disclosed. The data subject was notified and colleagues have been reminded to take care when sending emails and to check email addresses in full.

3.2. In June 2021 emails were sent inviting Trustees to an event. An incorrect invitation letter was mistakenly attached to two of the emails. This resulted in the home address of a member to be disclosed to two Trustees. Unfortunately, when the breach was reported it was copied to two further Trustees which extended the breach of data to four individuals. Colleagues and Trustees are reminded to take care when sending emails which contain personal information.

4. A New Approach to Compliance for 2021

4.1. Despite the investment and activity data breaches continue to occur. At the start of the year the SET decided to act decisively by creating a new role of Head of Compliance. This role adds expertise and resource to strengthening compliance with legislation and regulation across the institutes operations. It has as its focus the creation of a new compliance culture not just relating to the Data Protection Act but all the institutes legislation and regulatory obligations. These include the Health and Safety at Work Act, the Bribery and Corruption Act, all statutory employment law including the Employment Rights Act, the Employment Relations Act, the Companies Act and Charity Commission Regulation. The Data Protection Officer and the Governance team now report to the Head of Human Resources and Compliance.

5. Health and Safety Implications

There are no Health and Safety implications.

6. 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 and colleagues need to be confident that this data is protected in line with data protection laws.

7. Resource Implications

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

8. Governance and Compliance Implications

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

9. 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.

10. 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.

11. Corporate Strategy - GROWPLAN

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

12. 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.