Reference	BOT19/FEB/10
Date	Wednesday 6th February 2019

RTPI
Royal Town Planning Institute

Board of Trustees

Data Protection Report

Report from the Director of Commercial and Corporate Services

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

1. Summary

1.1 In the last year changes have been made to ensure the institute complies with data protection legislation and the culture characteristic of an organisation where the protection of personal data was a priority, is adopted.

1.2 Since the last meeting (November 2018) of the Board of Trustees there has been two data breaches (none recorded in the last report).

1.3 Good progress has been made in ensuring there is greater data protection compliance within the institute including adherence to the new 2018 Data Protection Act (2018 DPA). Further progress is required and additional investment is planned in new roles and responsibilities.

2. Progress on Data Protection Compliance

2.1. In May the Board of Trustees were made aware of long running contraventions of the 1998 Data Protection Act (1998 DPA) including:

- Lapse of registration with the ICO.
- Unclear or inadequate responsibilities in key data protection 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 outside of DPA protocols.
- Poor housekeeping procedures and lack of visitor control.
- Data breach incidents of a frequency and seriousness well above the levels seen in comparable organisation.

2.2. A great deal of activity had already been committed to putting in place processes and procedure to meet legal obligations. Improved reporting was been adopted including more comprehensive reporting to the Board of Trustees:

- All notifiable data breaches are immediately reported.

- All data breaches are reported in a standing board meeting paper.
- Data protection status and actions are in a standing board meeting paper.

3. Current Data Protection Legislation and Compliance

3.1 The UK's third generation of data protection law in the form of the 2018 DPA has now been in place for nearly six months. It incorporates the EU General Data Protection Regulation (GDPR), as well as extending data protection laws to areas that are not covered by the GDPR. It is intended to provide a comprehensive package to protect personal data to ensure it is:

- Processed lawfully (the lawful basis), fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2 The new law sets out a much higher standard for consent requiring a positive ‘opt in’ in place of assumed or default consent common under the 1998 PDA. Individuals have new rights, specifically the right to be informed, of access, rectification, erasure, to restrict processing and the right a right to data portability.

3.3 The RTPI collects stores and processes personal data including sensitive personal data. This is in connection only with providing membership services, rather than secondary commercial activities or fundraising so carries a lower level of data protection risk. The RTPI had been preparing for the introduction of the new legislation. Since the last report these have included:

- An audit of all RTPI databases identifying and decommission non-compliant databases.
- Online data protection training modules have been made available and completed by all RTPI colleagues.
- An communications programme for all RTPI colleagues has started including circulation of FAQ’s
- A new Data Privacy Statement has been agreed and is in use.
- All members have been informed of new DPA policies and the new Privacy Statement.
- Internal communications to officers has been agreed and a communications plan commenced.
- Data sharing agreements set up for major supplier partners.

4.2 The planned introduction of a new Customer Relationship Management system will vastly improve the control and monitoring of data protection compliance in future. More immediate priorities include:

- Auditing and updating organisation file structures to support individual's rights to access, rectification and erasure.
- A data retention policy is being drawn up.
- Investment in new software to allow committee and meeting papers to be despatched in a secure and compliant way.
- New processes to support confidential volunteer communications.
- New training for officers and volunteers at induction and mandatory refresher modules.
- The new role of Data Manager is to be recruited. This role will take up responsibility for the chief RTPI data asset, the new CRM. It will also take over the Data Officer role currently being performed through the governance function.

4.3 In September 2018, the RTPI's Data Protection Officer left the institute. It was intended to incorporate the role of Data Protection Officer in the new Data Manager role. Difficulties in recruiting to this role led to the separation out of data protection as this was seen as a barrier to attracting candidates. The responsibilities of Data Protection Officer are covered in an extension (one day a week) to a HR Officer role. In 2019 it is proposed to extend this responsibility and include some breach reporting responsibilities in a new role working in the membership team in the spring of 2019.

5. Data Breaches

5.1 Since the last Data Protection Report there have been two data breaches.

Date	Nature of Breach	Description of Breach	Actions
November 16th	Unauthorised disclosure of confidential details	A data subject complained that confidential information had been disclosed to a number of RTPI colleagues without authority. A Subject Access Request (SAR) was submitted and formal complaint made to the ICO.	The complaint and SAR were withdrawn on 12/12/2018.
December 11th	Unauthorised disclosure of e-mail address	A student auto-enrolment data base provided by the University of Birmingham contained data errors. The e-mail addresses of at least four data subjects were recorded incorrectly meaning that they could be accessed by other data subjects on-line.	New database requested. Changes made to existing data to correct discrepancies.

5.2 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 data subjects and the sensitivity of the data released. One breach was reported to the ICO by the Data Subject. This reporting was subsequently withdrawn. The second breach was not considered to require ICO reporting.

5.3 As reported in the September Data Protection Report a significant data beach occurred in July resulting in a Data Breach Report being made to the ICO on July 31st. There has still been no action taken by the ICO as a result of this report.

6. Health and Safety Implications

6.1 There are no health and safety implications.

7. Communication Implications

7.1 Members will be kept informed of their rights under the 2018 DPA and their permission to collect, store and process their data will be sought in line with the 2018 DPA.

8. Legal Implications

8.1 The RTPI seeks to comply with the 2018 DPA.

9. Jurisdiction and Devolution Implications

9.1 The 2018 DPA is UK and EU wide legislation.

10. Equality and Diversity Implications (EDI)

10.1 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 the tougher new data protection laws that include new rights. The adoption of an 'ultra-sensitive' approach to data security is likely to be appropriate to maintain member confidence and trust.