NOT FOR PUBLICATION

REPORT TO:	**CILEx REGULATION BOARD**
FOR:	**DECISION**
DATE:	**26th February 2020**
REPORT TITLE:	**ITEM 11 – Information Governance (IG) Annual Report**
SUBMITTED BY:	**Stuart Dalton, Director of Policy, Governance and Enforcement**

PURPOSE OF REPORT:

1. This is the first Information Governance (data protection) annual report to be presented to the Board. The intention is to present a report annually going forward to ensure the Board is properly sighted and considers information governance compliance and good practice.

2. The report includes our level of compliance against current data protection standards. It highlights identified or potential issues and risks and provide assurance to board regarding our management of these risks against a background of developing data protection requirements.

BACKGROUND:

3. The implementation of the General Data Protection Regulations (GDPR) and subsequent Data Protection Act 2018 introduced stricter requirements in how organisations handle personal data with significantly higher penalties applicable for serious failings. In addition, the introduction of this legislation has resulted in greater public awareness of how organisations must behave, bringing with it higher risks of legal challenge and reputational damage.

KEY ISSUES FOR CONSIDERATION:

<u>Identifying Risk</u>

4. We are very conscious of the potential effect on our reputation as a legal regulator if we are accused of mishandling personal data and thereby breaching data protection law. Even if an accusation is unfounded, the potential damage would still be problematic, particularly if the complainant uses social media to air their grievance.

5. CILEx Regulation handles complex personal data, including special category data, to fulfil our purpose and regulatory objectives. However, we are a small organisation with limited resources. On this basis, we are developing an approach which attempts to balance the risk to personal data with a proportionate use of staff time.

6. We require a different legal basis for processing data for different membership grades.

7. Whilst the number of Subject Access Requests (SAR) remains low, a number of those received have been linked to current misconduct investigations. A significant proportion of SARS are made by people seeking to challenge enforcement decision-making.

8. It is also worth noting that, informally, other legal regulators have indicated a marked increase in SARs due to the publicity around GDPR rights and the removal of the fee for providing records that could be charged under the old Data Protection Act.

Work undertaken

9. CILEx Regulation has clarified our relationship with CILEx and agreed for the first time in the autumn of 2019, via a formal data sharing agreement, that we act both as separate data controllers and in some instances as joint data controllers.

10. Additionally, CILEx's Corporate Compliance team provided us with a member of their staff, at no cost, to assist in reviewing and developing our policies, processes and procedures. This work was undertaken over a period of around 2 months in the autumn of 2019 and culminated in an audit based on the Information Commissioner's (ICO) audit tool. This highlighted where further work needed to be undertaken. For additional reassurance, an external consultant undertook a one-day assessment in December 2019 to provide an independent view of our compliance. The audit and external assessment did not identify any major gaps in our information governance arrangements. Equally, they made a number of lower level recommendations which we will be progressing, which are set out further below.

What we are doing well

11. We have a positive staff culture with a good understanding of the importance of data protection. Staff have consistently shown a willingness to ask questions, learn and take responsibility for the protection of personal data and have felt able to speak up promptly if they believe they may have made a mistake. Together with a productive working arrangement with the CILEx Corporate Compliance team, we are able to develop and agree new ways of working in the office to further protect personal data.

12. For the first time we have produced a separate Privacy Statement from CILEx enabling us to specifically set out the purposes for which we use personal data.

13. We have a named Data Protection Officer, in-line with GDPR, Clare Harper Smith.

Key areas of ongoing work / Actions

14. The following areas require further work to strengthen data protection:

    - Data protection training for panellists, consultants and other third parties:

15. As a data controller, we carry significant responsibility under GDPR for the data supplied to third parties as our data processors. We are currently costing up an online training option to be rolled out for these individuals handling personal data on our behalf.

- Sign off for finalised data protection policies for CILEx Regulation

16. To strengthen our data protection processes, we are developing an independent set of data protection policies. This is linked to a wider piece of work to develop policies for IGR and regulator independence and is in hand for completion by July 2020.

- Development of processes to deal with Subject Access Requests

17. To assist in dealing with the increase in SARs, we are further developing process guides for use by staff. Whilst SARs are normally managed by the data protection officer (DPO), the time-limited nature of these requests means that dealing with a SAR cannot be delayed because of a period of leave.

Data breaches

18. CILEx Regulation records data breaches. There have been three data breaches recorded in 2019, although none met the criteria to inform the ICO for more serious breaches.

19. The three data breaches related to:

- A myCILEx account being made accessible to another member (initially reported to the PAS team).

- CILEx Regulation data potentially viewable by CILEx staff following CRM data migration – the assessment was it was highly unlikely the data was viewed by any CILEx staff.

- Information emailed to the wrong recipient – no sensitive data was disclosed.

20. The first two breaches were dealt with by CILEx. As part of the response to the third breach, we have reminded staff about e-mail security.

Outstanding Issues (exception reporting)

21. There are no other issues to report to the Board.

Conclusion

22. CILEx Regulation, working in conjunction with CILEx and an external consultant, has achieved good progress in developing strong working practices around data protection. There are no significant information governance compliance issues to highlight to the Board. We can demonstrate robust review of our information

governance arrangements and a plan to further improve those arrangements identified from the audit and independent external assessment. Staff are fully engaged with the importance of data protection and contribute on an ongoing basis to related improvements.

RECOMMENDATIONS:

23. To **RECEIVE** AND **APPROVE** the report.