Item 12
For Noting

Glasgow Kelvin College

Audit and Risk Committee Meeting of 22 February 2022

Governance Update

Report by Director of Corporate Services

1. Introduction

The purpose of this report is to provide an update to members in relation to various areas of corporate governance.

2. Protect Duty Consultation Response

In February 2021, the Government launched a consultation paper seeking views on how the Protect Duty can make the public safer at publicly accessible locations; the consultation consisted of 58 questions spread across 4 sections. This was shared and discussed with the College's Incident Management Team and Operational Management Team and the subsequent feedback collated. Glasgow Kelvin College's response was submitted by the deadline date of 2 July 2021.

On 27 January 2022, the Government published their response document along with the summary of responses received.

Government Response Document

This document aligns to the responses submitted by the College i.e.:

- *Section 1: Who (or where) should legislation apply to?*
  7 in 10 respondents agreed that those responsible for publicly accessible locations should take appropriate and proportionate measures to protect the public from attacks. This included ensuring staff were trained to respond appropriately.

- *Section 2: What should the requirements be?*
  In general, there were very strong views expressed on the need for accountability within the Duty. This predominantly referred to the need for clear roles and responsibilities, particularly amongst event organisers, and those at senior level within venues and organisations.

- *Section 3: How should compliance work?*
  Just over 50 percent of respondents were in favour of an inspectorate which would support improvements to security culture and practices within organisations in scope. Their reasons were most commonly that it would identify key areas for improvement or vulnerabilities, act as a means of sharing best practice, and to deliver the key objective of the Duty to improve public safety.

- *Section 4: How should Government best support and work with partners?*
  Just over half of respondents, that operate or own a publicly accessible location, currently accessed information regarding threats and mitigations provided by Government. The College has access to these resources to inform tabletop exercises run with the Incident Management Team to test the Business Continuity Plan.

To further support the public and private sector, the Home Office is collaborating with the National Counter Terrorism Security Office (NaCTSO) and Pool Reinsurance to develop a new interactive online platform, due to launch publicly this year.

Throughout the document it is clear that responders felt that the requirements for organisations under the Protect Duty should be proportionate, appropriate and should not place a financial burden on the organisation.

3. Claims Digest – UMAL

The UMAL Claims Digest provides the College with topical news/insights directly from expert claims handlers. This enables us to be alert to legal developments/trends and aids our understanding of various subjects affecting the further and higher education sectors. The Claims Digest is contained within Appendix 1 - Claims Digest

College senior staff are fully aware of the matters contained therein and are implementing measures as appropriate in these regards.

4. Business Interruption Claim

As indicated at a previous meeting, the College pursued a Business Interruption Claim with our insurance providers UMAL in respect of the negative impact of Covid-19 on business operations.

This was an extensive piece of detailed work conducted by the Head of Finance and Director of Corporate Services with very significant input by the College Accountant and involved meetings with loss adjusters and our insurance company.

In accordance with the limit of the Notifiable Diseases Extension under our Business Interruption cover, we were awarded £250,000. These funds were transferred early in 2022.

5. Resource Implications

There are no negative resource implications arising as a consequence of matters contained within this report.

6. Equalities

There are no equality implications arising as a consequence of matters contained within this report.

7. Risk and Assurance

This report seeks to provide members with assurance that a number of governance matters related to the smooth running and operations of the College are being taken forward accordingly and will be carefully handled.

8. Data Protection

There are no data protection implications arising as a consequence of this report. The new Director of Digital Services is acutely aware of the rise in cyber attacks across the sector and his report at agenda Item 13, covers his work since commencing in post.

9. Recommendations

It is recommended that members:

i) note the content of this report, its link and appendix.

10. Further Information

Further information can be obtained from Lisa Clark, Director of Corporate Services - lisaclark@glasgowkelvin.ac.uk

Lisa Clark
Glasgow Kelvin College
February 2022

Claims Digest

The Claims Digest has been developed in order to provide our Members with topical news and insights directly from our expert claims handlers. By virtue of dealing with claims against universities and colleges on a daily basis and by being alert to legal developments they can recognise trends and make recommendations that may be relevant to our Members, giving them unique understanding into various subjects affecting the further and higher education sectors.

If you have any feedback or thoughts on future subjects that we might consider for the digest, please email Georgie.wilson@umal.co.uk

Sexual Misconduct Claims

Further to the Risk Alert we published in March, which remains available on our website and to the presentation delivered by Kennedys at the UMAL conference in April, we continue to see compensation claims being made. As we have previously observed, difficulties may be faced in defending sexual misconduct claims due to a failure to have specific policies in place or for a failure to adhere to them.

We recommend:

- In the absence of relevant policies, these should be developed and implemented;
- Universities UK require universities to have a stand-alone sexual misconduct policy or to integrate the policy into a bullying and harassment policy;
- The review of existing policies as to their scope and ability to flex to different contexts;
- Ensure policies are readily available, advertised to and accessible by all students and staff;
- Investigations must be carried out sensitively whilst recognising the obligations and duties to all of the parties involved;
- Ensure that the parties to a complaint fully understand the policies involved;
- Be sure to act in accordance with the relevant policies;
- Ensure diligence in documenting complaints, investigations, evidence obtained, findings and conclusions. All communications in whatever form should be carefully documented and retained, including minutes of any meetings.

Our Risk Alert of March (available via the link above) included our recommendations as to the components of a sexual misconduct policy.

Claimant Legal Costs

In personal injury liability claims the claimant's legal costs can make up a large proportion of the overall settlement. Whilst the majority of claims worth under £25k will attract fixed solicitors costs plus disbursements, those claims that fall outside the fixed fee regime can see us facing disproportionately large claims for costs versus the damages.

Some recent examples are:

- Occupational stress claim – Damages settled at £75,000 and solicitor costs settled at £115,000;
- Harassment claim – Damages settled at £30,000 and solicitor costs settled at £29,687; and

- Shoulder injury – Damages settled at £24,000 and solicitor costs settled at £24,000.

Damages	Claimant costs	Total	Costs as a % of damages
£75,000	£115,000	£190,000	153%
£30,000	£29,687	£59,687	98%
£24,000	£24,000	£48,000	100%

There are things that can be done to mitigate the exposure to these costs. Proactivity is the primary strategy in combating claimant solicitor costs building activities. If we can approach the claim on the front foot from the very beginning, it puts UMAL and our legal team in a better position. Members can assist in the following ways:

- Do not delay or ignore legal correspondence. Forward letters of claim, legal proceedings and other correspondence promptly to UMAL for us to address.
- Engage proactively with UMAL and our solicitors in evidence and document gathering. Retention and swift production of documentary or digital evidence is vital in assisting UMAL deal with these claims efficiently.
- All too often claimant solicitors will fail to engage and will provide very little information by way of update on their client's recovery from injuries suffered. If the claimant is an employee or current student, updates on their return to work or study are key to assisting the defence of claims and providing a better understanding of the potential value of claims.

Cyber Liability and Data Breach Claims

There has been much media attention in recent times describing the current adverse context of cyber risk. Alongside this, UMAL issued a Risk Alert in December 2020 (which remains available on the UMAL website) and, in September, the British Universities Finance Directors Group (BUFDG) issued its quarterly news bulletin, which included an article from the UMAL CEO Paul Cusition describing the current state of the cyber insurance market.

Following data breaches, we often see claims advanced for damages on multiple alleged causes of action:

- Misuse of private information (a common law privacy tort);
- Breach of confidence (also a common law privacy tort);
- Breach of Article 8 of the European Convention on Human Rights (right to respect for private and family life, home and correspondence);
- Negligence; and
- Breach of data protection legislation (including GDPR/UK GDPR/Data Protection Act 2018).

The market and the courts have been seeing greater numbers of these claims, which are often 'farmed' by claimant solicitor firms or other companies whereby individuals are encouraged to bring claims for compensation.

It is therefore pleasing to be able to advise there have been several positive court decisions for defendants over the summer and autumn, which may take some of the momentum out of this growth claims area.

In August, we saw the High Court judgment in *Warren -v- DSG Retail Ltd* where DSG was the victim of a cyber-attack by a malicious third party. The personal data of several million data subjects including that of the claimant was potentially compromised (his name, address, date of birth, email address and telephone number).

The claimant brought a claim for damages, alleging misuse of private information, breach of confidence, negligence and breach of data protection legislation.

The High Court struck out the claims in negligence, breach of confidence and misuse of private information, leaving the claim to proceed for a breach of data protection legislation for an alleged failure to implement adequate security measures to protect against the cyber-attack:

- The breach of confidence and misuse of private information causes of action were struck out because they required a positive wrongful act by the defendant, which was not a characteristic present in a third party cyber-attack; and

- The claim in negligence was struck out because negligence generally requires there to be injury to person or property, which was not a feature of the case, and in any event, the claim in negligence gave no better right of action than that available for a breach of data protection legislation.

The judgment is helpful to defendants who face compensation claims from data-subjects following a cyber-attack:

- The claims are simpler if brought purely on the basis of an alleged breach of data protection legislation;
- The removal of the breach of confidence and misuse of private information elements may strengthen arguments by defendants that many of these claims should be allocated to the small claims track where the claimant can only recover limited legal costs; and
- Premiums for After the Event (ATE) insurance, which covers a claimant's potential liability to pay the defendant's legal costs in the event the claim fails, remains recoverable from defendants in claims for breach of confidence and misuse of private information. If those are no longer viable causes of action in these claims then ATE premiums, which can often be several thousand pounds, will no longer be recoverable from defendants.

In October, the High Court gave judgment in *Rolfe -v- Veale Wasbrough Vizards LLP*. An employee of the defendant had accidentally sent an email intended for the claimant to the wrong individual. The email included a letter demanding payment from the claimant for unpaid school fees. The unintended recipient advised the defendant of the error and deleted the email.

A claim was brought for distress. The defendant applied to the court for the claim to be struck out on the grounds it was not realistic for the claimant to have been distressed beyond a *de minimis* threshold where an email that did not contain sensitive data had only been accidentally sent to one individual who had deleted it.

Finding for the defendant, the court held it was not credible that distress or damage over a *de minimis* threshold would be proved, adding "…that in this day and age it is inappropriate for a party to claim (especially in the High Court) for breaches of this sort which are, frankly, trivial…", and "…no person of ordinary fortitude would reasonably suffer the distress claimed in these circumstances in the 21st century, in a case where a single breach was quickly remedied…".

November saw another helpful judgment from the High Court in the case of *Johnson -v- Eastlight Community Homes Ltd* where an employee of the defendant had inadvertently sent an email to one of its customers that included rent statements of other customers, including the claimant. The personal data involved the claimant's name, address and details of recent rent payments. As in *Rolfe*, the unintended recipient notified the defendant of receiving the email and agreed to delete it.

The claimant brought legal proceedings against *Eastlight* claiming damages for distress of up to £3,000 for misuse of private information, breach of confidence, negligence, breach of Article 8 of the European Convention on Human Rights and breaches of GDPR and the Data Protection Act 2018. The claimant discontinued the negligence element of the claim prior to the court hearing.

The court held:

- The claims for misuse of private information, breach of confidence and Article 8 of ECHR added nothing beyond the claim for breach of data protection legislation and were struck out;
- Whilst damages for distress can be recovered, the distress must not be so trivial as to be *de minimis* in nature;
- That in this claimant's case the distress was more hypothetical than real and the issue to be determined was whether the *de minimis* threshold had been breached and, if so, whether the entitlement was to damages of a nominal or extremely low level;

- The proceedings should not have been commenced in the High Court and the fact they had been was an abuse of procedure; and
- The proceedings should be transferred to the small claim track for determination of the remaining issues.

Also in November, the Supreme Court delivered its long-awaited judgment in *Lloyd -v- Google*. The claimant commenced proceedings for an alleged breach of the Data Protection Act 1998 and sought permission from the court on behalf of 4 million iPhone users in England and Wales to serve opt-out representative proceedings out of jurisdiction on Google in the US for alleged breaches of data protection legislation.

The Court of Appeal had given permission for the representative proceedings to be served out of jurisdiction and had also found that damages for loss of control of personal data were recoverable even if a claimant had not suffered any distress or financial loss. Damages in the order of £750 per claimant had been mooted along the way for a mere loss of control of data, which if accurate gave rise to potential damages of £3billion in aggregate across the affected individuals.

Google appealed to the Supreme Court which found in favour of Google, holding:

- Where damages were recoverable, claims had to be individually assessed which required the service of requisite evidence by a claimant. This meant the case was unsuitable to be considered by way of opt-out representative proceedings; and
- The Data Protection Act 1998 only permitted compensation to be recovered where a data-subject had suffered damage, which meant material damage or distress. Loss of control of data fell short of this.

Conclusion

1. The direction of travel of the courts in data breach claims seems to be of an increasing preparedness to look closely at the level of distress a claimant has allegedly suffered and whether this breaches a *de minimis* threshold, failing which damages may not be recovered;
2. When a data breach arises from a third party cyber-attack, claims for misuse of private information and breach of confidence are inappropriate. Even when a data breach does not arise from a cyber-attack, such claims will generally add nothing more than a claim for a breach of data protection legislation and may be struck out, the same for claims in negligence. This increases the likelihood of defendants being able to argue that claimants should not be able to recover often expensive After the Event insurance premiums and that claims involving modest levels of damage or distress should proceed via the small claims track where only limited costs can be recovered by claimant solicitors;
3. Although there is a possibility for future challenges on the grounds the *Lloyd -v- Google* decision of not to allow a loss of control of data claim was based on the provisions of the former Data Protection Act 1998 rather than the current data protection legislation, such claims are likely to remain difficult to bring in future;
4. The risk of representative proceedings being brought when there has been a data breach involving numerous claimants has reduced; and
5. Taken in the round these developments may reduce the likelihood of low-level data protection breach claims becoming a growth area for claimant solicitors and claims management companies.

Higher Education Freedom of Speech Bill

This is a Bill currently making its way through the House of Commons, before it goes on to be considered by the House of Lords and then on through to Final Stages.

The description of the Bill is “a Bill to make provision in relation to freedom of speech and academic freedom in higher education institutions and in students’ unions”.

The Bill requires higher education providers to have “particular regard to the importance of free speech”.

"Freedom of speech" is defined in the Bill as including a freedom to express ideas, beliefs and views without suffering adverse consequences, although there is no definition of what constitutes "adverse consequences" which

in its current form is vague. The Bill also introduces a statutory tort available to individuals who have suffered adverse consequences because of a failure by a university to protect free speech.

In view of the current Government majority, the Bill is expected to achieve successful passage. We would encourage Member universities to review the Bill, monitor its progress and determine any necessary policies required in consequence.

Update – Covid-19 Business Interruption Claims

A total of fifty-nine claims were received from Members following disruption arising from the Covid-19 pandemic.

To date fifty-two claims have been settled involving payments by UMAL of over £12.4million.

Seven claims remain open with reserves of £1.5million. Our loss-adjusters, Sedgwicks, continue to progress these claims to conclusion.

If you have any questions or follow up on anything in the digest, please contact claims@umal.co.uk

Author: Paul Francis, Head of Claims

This Claim Digest is for informational purposes only and not for the purpose of providing legal advice. Neither UMAL nor any of its directors or employees give any warranty in relation to the accuracy or reliability of any information contained within.

UMAL disclaims all liability to any party (including any indirect or consequential loss or damage to loss of profits) in respect of or in consequence of any action taken by any party in reliance, whether in whole or partial, upon any information contained in this Claim Digest; any party who chooses to rely in any way upon the contents does so at its own risk.