Following its consideration by the Audit and Accounts Committee on 6 November 2019, this report has been redacted due to the likely disclosure of sensitive information in relation to Derby City Council's information security arrangements.

For more information email committee@derby.gov.uk

AUDIT & ACCOUNTS COMMITTEE
06 November 2019

Derby City Council

Report sponsor: Andy Brammall – Director of Digital & Customer Management
Report author: [redacted]

ITEM 09

Information Security Update

Purpose

1.1 This report provides Members of the Committee with an update on information security breaches across the Council for the first six months of the financial year 2019/20, with consideration to the current threats, success of improvements delivered and ongoing improvement plans.

Recommendation

2.1 To note the report and to request a further Information Security Assurance update at the February 2020 meeting.

Reasons

3.1 The Audit & Accounts Committee is responsible for providing assurance to the Council on the effectiveness of the governance arrangements, risk management framework and internal control environment.

3.2 The Council holds a significant amount of confidential and sensitive information. It is essential that this information is managed properly to reduce the amount of breaches, in particular serious (reportable to the Information Commissioner's Office) breaches likely to attract regulatory action or claims for compensation.

Supporting information

4.1 This update report provides an update across the area of:

- Information Security Breaches

Following its consideration by the Audit and Accounts Committee on 6 November 2019, this report has been redacted due to the likely disclosure of sensitive information in relation to Derby City Council's information security arrangements.

For more information email committee@derby.gov.uk

4.2 **Information Security Breaches**

Status

From 1 April 2019 to 30 September 2019 there were [redacted] information security incidents reported to the Information Governance Team. On investigation, there were [redacted] actual personal data breaches, with the remaining [redacted] considered 'non-breaches'. Of these breaches, [redacted] serious breaches were voluntarily reported to the Information Commissioner's Office (ICO). [redacted] Out of the [redacted] breaches, [redacted] have been closed without further action from the [redacted].

4.3 It is reassuring that staff are recognising personal data breaches and they are being reported. This may be a positive indicator that the GDPR and Cyber Security e-learning content is effective and staff are recognising the difference types of incidents.

4.4 Comparably, in the first six months of the 2018/19 financial year there were [redacted] incidents reported to the Information Governance Team, of which [redacted] were actual breaches. There were [redacted] serious breaches reported to the ICO for the period. All breaches from the previous financial year are closed.

4.5 [redacted] to the Information Governance Team for this period. Of these incidents, actual breaches and non-breaches reported to the Information Governance Team have [redacted]

4.6 The [redacted] the number of breaches submitted to the ICO for their decision [redacted]

4.7 Serious breaches reported to the ICO by organisations put them at risk of sanctions and reputational damage, as the incident itself potentially causes life-changing harm to the data subjects through the infringement of personal rights. The specific risks to DCC for each breach vary between the ICO providing an undertaking which the Council must comply with, to the ICO imposing a maximum fine of €20 million (approximately £17.3 million).

4.8 The online and direct guidance discussions with the ICO encourage a positive reporting culture, in line with the accountability principles of GDPR. [redacted] it is reflective of correct measures undertaken by the Council to respond appropriately to the subjective details of each incident. The fact that [redacted]

Following its consideration by the Audit and Accounts Committee on 6 November 2019, this report has been redacted due to the likely disclosure of sensitive information in relation to Derby City Council's information security arrangements.

For more information email committee@derby.gov.uk

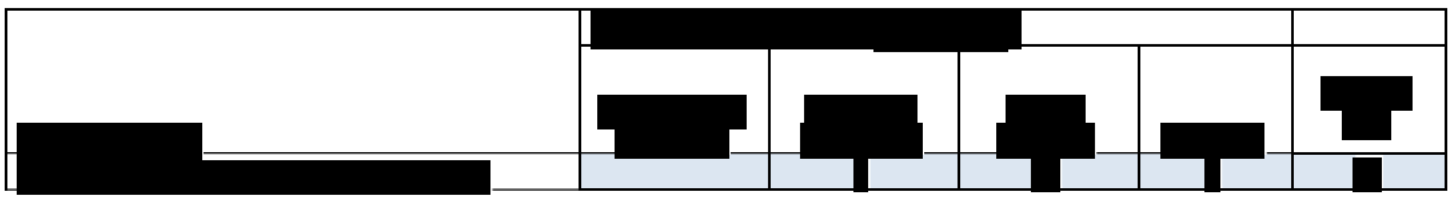
4.9 The People's Directorate continue to report the majority of incidents which is in part a reflection of the complex nature of their service and the amount of sensitive personal information that they handle and in part a reflection of their continued dependence on paper based and manual processes.

[redacted]

Table 1

[redacted]

Table 2



Following its consideration by the Audit and Accounts Committee on 6 November 2019, this report has been redacted due to the likely disclosure of sensitive information in relation to Derby City Council's information security arrangements.

For more information email committee@derby.gov.uk

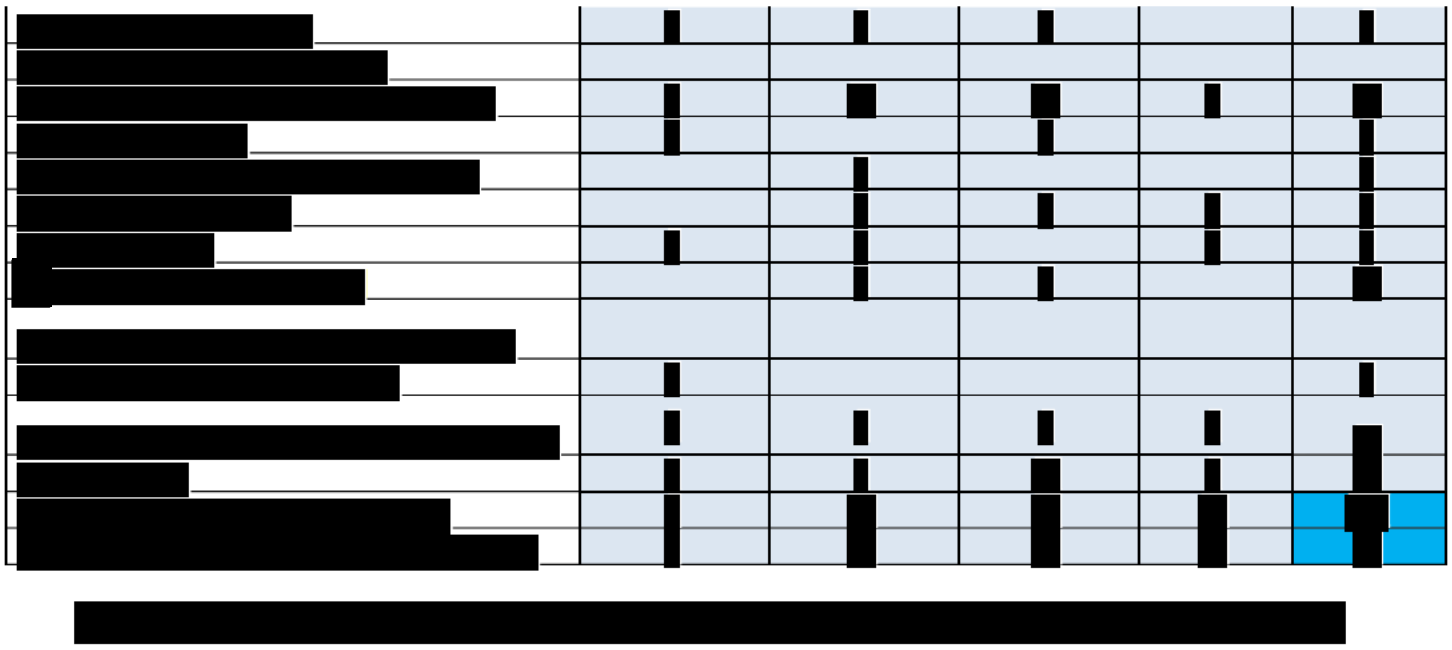


Table 3

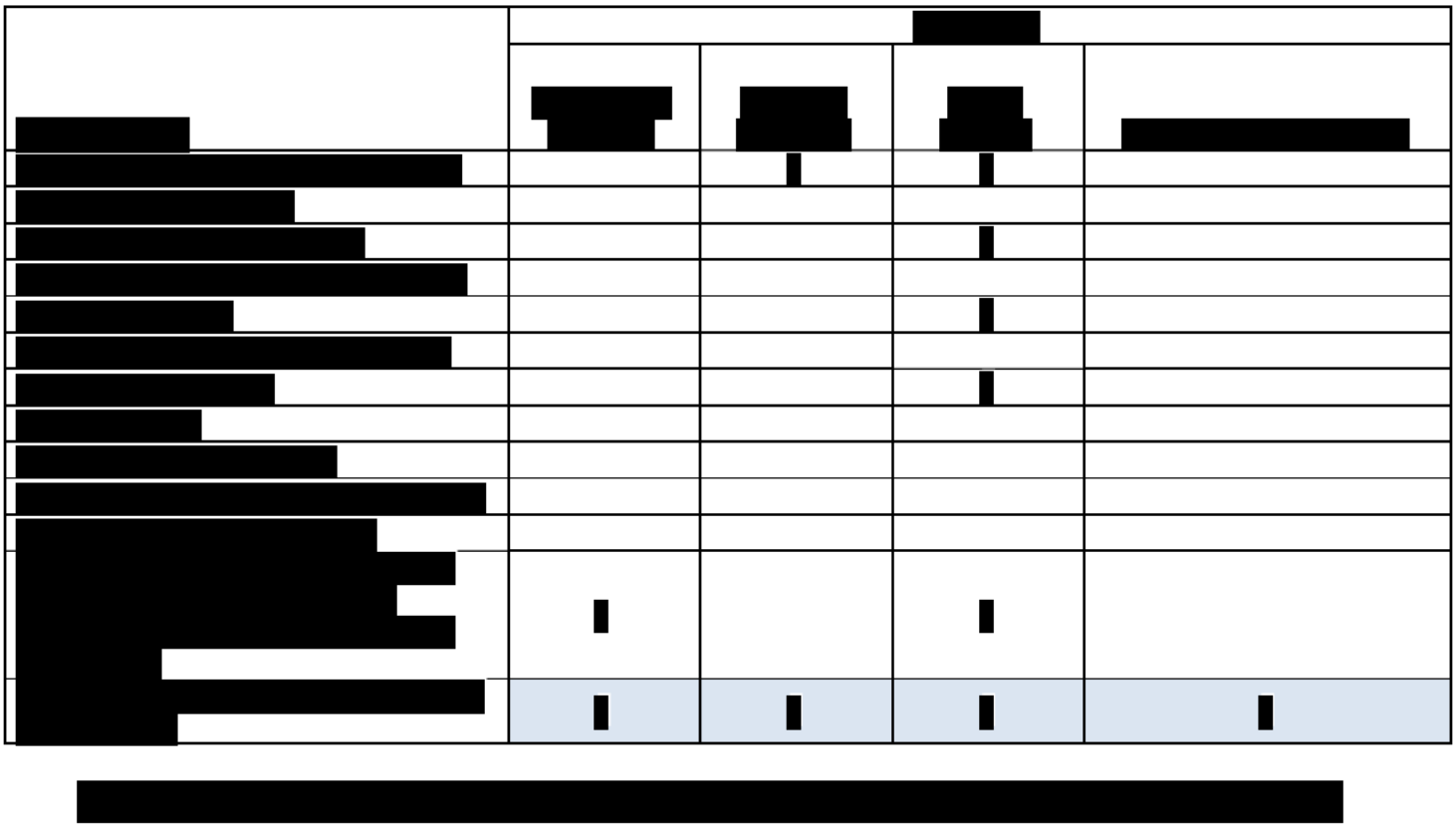
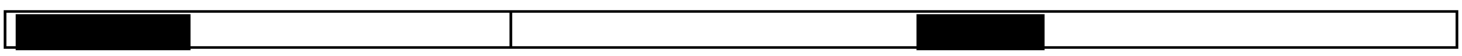
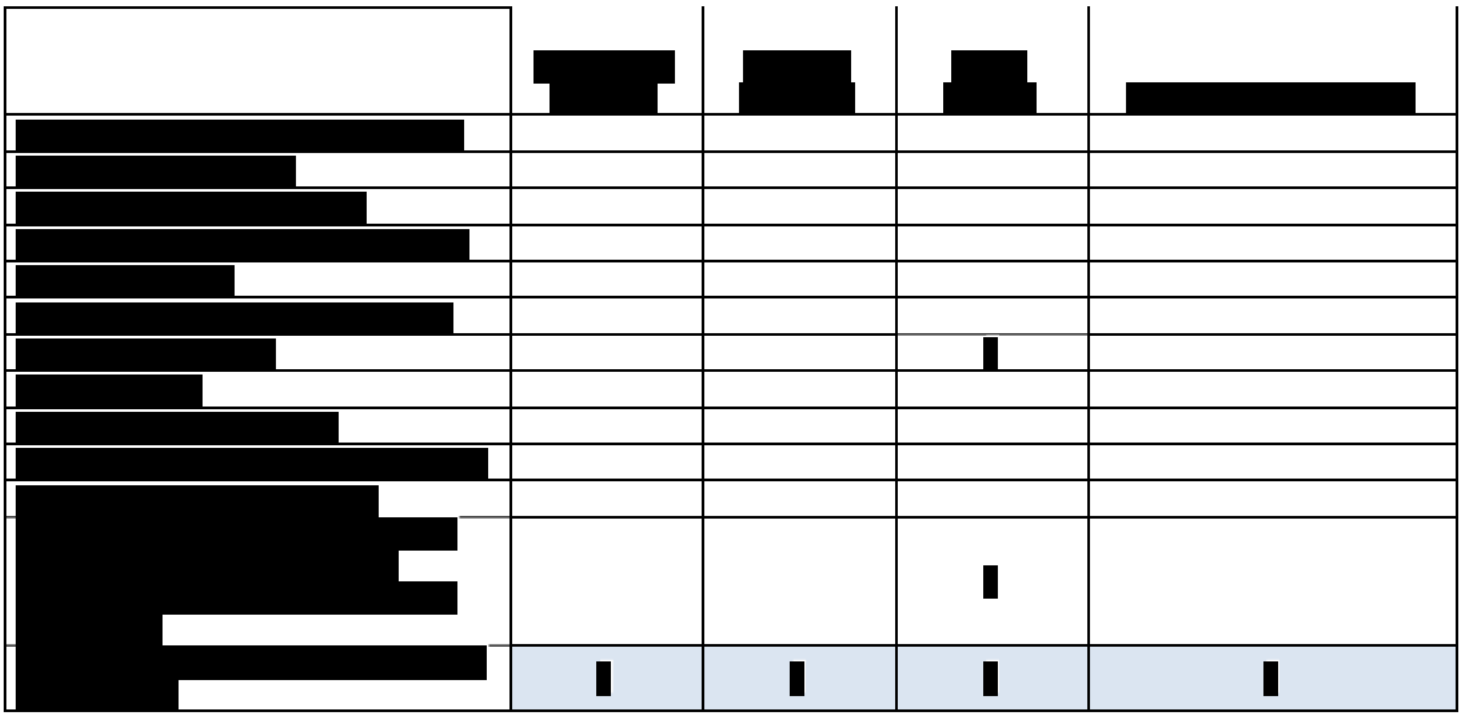


Table 4



Following its consideration by the Audit and Accounts Committee on 6 November 2019, this report has been redacted due to the likely disclosure of sensitive information in relation to Derby City Council's information security arrangements.

For more information email committee@derby.gov.uk



Risks to the Council

5.1 Personal data breach hot spots are detailed in red in [redacted] above, with [redacted] Indications are that human error is the greatest factor in these breaches. These type of breaches identified are a similar trend to last year, in this period.

5.2 [redacted]

5.3 Outside the remit of the ICO, the individual subject to a breach has at their disposal the right to challenge the Council in a civil claim for compensation due to a breach of their personal data. There have been several occasions of this in the last financial year.

5.4 The forecast for the remaining financial year is that DCC will suffer a further [redacted] breaches, with [redacted] requiring submission to the ICO. This will bring the count to [redacted] actual personal data breaches and [redacted]

Following its consideration by the Audit and Accounts Committee on 6 November 2019, this report has been redacted due to the likely disclosure of sensitive information in relation to Derby City Council's information security arrangements.

For more information email committee@derby.gov.uk

5.5 The incident reporting culture within the Council has improved, and Colleagues are showing a greater understanding of Information governance.
This is highlighted by support calls to the IG team and the reduction in actual breaches. The expectation is that DCC can continue to reduce the amount of breaches suffered as awareness further matures. [redacted] The reality is that serious breaches are an anomaly, and each case must be reviewed on the information presented.

5.6 Generally, repeated serious data breaches of the same type reported to the ICO prompts the ICO to review those breaches and take action against an organisation where improvements have not been made or where their recommendations have not been implemented. [redacted]

5.7 The ICO have stated they received around 14,000 Personal Data Breach (PDB) reports from 25 May 2018 to 1 May 2019. For comparison, they received around 3,300 PDB reports in the year from 1 April 2017.

5.8 The positive reporting culture throughout the UK is further highlighted by the ICO:
"We closed over 12,000 of these cases during the year. Of these, only around 17.5% required action from the organisation and less than 0.5% led to either an improvement plan or civil monetary penalty. While this means that over 82% of cases required no action from the organisation, it demonstrates that businesses are taking the requirements of the GDPR seriously and it is encouraging that these are being proactively and systematically reported to us."

5.9 [redacted]

Response Activities

6.1 The Information Governance team continues to address incidents reactively and proactively where incidents are logged, near misses, and serious incidents or trends are apparent. Work undertaken includes briefing notes to teams and Services, mandatory briefing sessions to staff groups, IG support drop-in sessions, communications though bulletins and the available array of media in the communications team, support and guidance.

6.2 Each incident of security breach is rigorously investigated and in each case learning applied both in respect of immediate response and more permanent prevention. A large number of improvements have been made both direct and corporate with significant effect.

Following its consideration by the Audit and Accounts Committee on 6 November 2019, this report has been redacted due to the likely disclosure of sensitive information in relation to Derby City Council's information security arrangements.

For more information email committee@derby.gov.uk

Addressing Areas of Significant Concern

7.1 Types of breach which present ongoing concerns include personal data [redacted]

Social Care and Business Support teams are particularly susceptible to breaches of significance, due to the sensitivity of data handled.

7.2 An information security improvement programme is underway to provide pro-active solutions to help reduce personal data breach occurrences. The programme also includes reactive work emerging from 'lessons learned' from breaches, to help prevent breaches of the same type occurring

7.3 A number of corporate approaches are currently being either enacted or researched to address threats in the short, medium and long term…

[redacted]

Following its consideration by the Audit and Accounts Committee on 6 November 2019, this report has been redacted due to the likely disclosure of sensitive information in relation to Derby City Council's information security arrangements.

For more information email committee@derby.gov.uk

[redacted]

8.2 [redacted]

The Cyber Security Programme

9.1 Cyber Security remains a tier 1 threat to the interests of the UK and subsequently the Council's systems and infrastructure and data are at risk from a range of international, national and local actors.

9.2 [redacted]

Following its consideration by the Audit and Accounts Committee on 6 November 2019, this report has been redacted due to the likely disclosure of sensitive information in relation to Derby City Council's information security arrangements.

For more information email committee@derby.gov.uk

9.3 It is imperative that the Council maintains its compliance with best practice of the National Cyber Security Centre, Public Sector Network Code of Compliance and the NHS IG Toolkit, which exist in a threat landscape which changes daily and requires constant improvement.

9.4 [redacted]

9.5 It is important that precise details of the Council's cyber defence arrangements and capabilities remain confidential as knowledge of these arrangements would permit focussed attacks on the Council's systems. A number of improvements have been implemented in the last 18 months and a rolling improvement programme continues to address emerging threats:

[redacted]

Public/stakeholder engagement

10.1 None applicable

Other options

11.1 None applicable

Financial and value for money issues

12.1 None directly arising

Following its consideration by the Audit and Accounts Committee on 6 November 2019, this report has been redacted due to the likely disclosure of sensitive information in relation to Derby City Council's information security arrangements.

For more information email committee@derby.gov.uk

Legal implications

13.1 None directly arising.

Other significant implications

14.1 Risk Management
Non-compliance with FOI and Data Protection legislation opens up the risk that the Council attracts a monetary penalty or other sanction from the ICO. This is particularly important going forward as from 25 May 2018 when the General Data Protection Regulations (GDPR) came into force then penalties for non-compliance can be up to €20 million. Information risks are monitored on a regular basis by the Director of Digital & Customer Management, Andy Brammall.

14.2 Equalities Impact

Data Protection also includes sensitive equality information. It is essential that we are able to do all we can do to prevent any breaches.

14.3 Corporate objectives and priorities for change

The functions of the Committee have been established to support delivery of corporate objectives by enhancing scrutiny of various aspects of the Council's controls and governance arrangements.

Following its consideration by the Audit and Accounts Committee on 6 November 2019, this report has been redacted due to the likely disclosure of sensitive information in relation to Derby City Council's information security arrangements.

For more information email committee@derby.gov.uk

This report has been approved by the following people:

Role	Name	Date of sign-off
Legal		
Finance		
Service Director(s)	Andy Brammall	
Report sponsor	Andy Brammall	
Other(s)		

Background papers:	
List of appendices:	[redacted]

Following its consideration by the Audit and Accounts Committee on 6 November 2019, this report has been redacted due to the likely disclosure of sensitive information in relation to Derby City Council's information security arrangements.

For more information email committee@derby.gov.uk

Following its consideration by the Audit and Accounts Committee on 6 November 2019, this report has been redacted due to the likely disclosure of sensitive information in relation to Derby City Council's information security arrangements.

For more information email committee@derby.gov.uk