BSS/16/17
Corporate Services Scrutiny Committee
28th November 2016

DATA PROTECTION RISKS
Report of the Head of Digital Transformation and Business Support

1. Summary

This paper is submitted following the discussions that took place at the committee meeting in June 2016, regarding the Data Protection breach risk recorded on the Corporate Risk Register. The Committee have requested further clarity on what a Data Protection breach is; how they are managed; what the impact is if a breach occurs and what are individuals' responsibilities in respect of this.

For clarity, the Data Protection risk recorded on the Corporate Risk Register is as follows:

> *'The council may incur fines and legal actions for damages following incidents of misuse, loss, accidental or deliberate disclosure.'*

2. Definition of a Data Protection breach

The Data Protection Act 1998 (the Act) places a legal obligation on organisations to handle personal data[1] securely, in order to avoid that data being put at risk from unauthorised or unlawful processing[2], accidental loss, destruction or damage.

If an organisation fails to do this and the personal data is put at risk, this may result in a breach of the Act. In Devon County Council, we commonly refer to these as '*security incidents'*. The following are examples of Data Protection breaches/security incidents:

- Personal data being posted to an incorrect address which results in an unintended recipient reading that information;
- Dropping or leaving documents containing personal data in a public place;
- Personal data being left unattended at a printer enabling unauthorised persons to read that information;
- Not locking away documents containing personal data (at home or work) when left unattended;
- Any action which allows an unauthorised individual access to Devon County Council buildings or computer systems (e.g. through losing a Smart Card, disclosing passwords or writing down passwords etc.);
- Verbally disclosing to or discussing personal data with someone not entitled to it, either by phone or in person;

[1] 'Personal data' means any data that is held about a living individual who can be identified from that data or from other information that may be known about that individual.
[2] In essence, 'processing' means obtaining, recording, holding, disclosing, using or viewing data

- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.

- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to Devon County Council's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

This list is not exhaustive and is provided to illustrate types of data protection breaches.

3. Security incidents

The Council actively encourages (it is part of policy) that all staff have an obligation to report a security incident as soon as they are aware that it has occurred. All security incidents in the council are investigated by the council's Information Governance Team. The Council classifies its incidents into three categories:

1. **Security incident** – these are incidents where minimal personal data have been or could have been put at *minor risk* from unauthorised access etc. and are *not likely* to cause the data subject[3] distress or damage

2. **High risk *internal* incident** – these are incidents where sensitive[4] personal data have been put at *serious risk* from unauthorised access etc. and *could* cause the data subject *some distress* (but no damage)

3. **High risk *reportable* incident** – these are incidents where sensitive personal data have been put at *serious risk* from unauthorised access etc. and are *likely* to cause the data subject *significant distress and/or damage*.

   The investigation will ensure action is taken to minimise any impact, recover the information and that appropriate action is taken to prevent similar occurrences. The Council has an obligation to report High Risk incidents to the Information Commissioner's Office (ICO) - the UK Data Protection Regulator, so they can take a view as to whether the Council acted appropriately and did everything it could have done to prevent the incident. Where an organisation has caused a serious breach of the Data Protection Act, the ICO has the power to fine that organisation up to £500k.

When determining the category of risk, the Investigating Officer considers the nature of the incident, the sensitivity of the information involved, the impact and likelihood of any adverse consequences (for the data subject and/or the Council), and the number of data subjects affected.

Out of the 21 incidents reported to the ICO since 2011, the ICO has only found on **one** occasion that the Council did not have adequate security measures in place to protect the personal data it holds. This incident occurred in 2012 and the council was fined £90k for this error. It should be noted that any member of the public is entitled to report a Data Protection Breach direct to the ICO, regardless of whether the organisation holding that data have reported it themselves.

---

[3] Data subject means the person who the data is about

[4] The Data Protection Act defines 'sensitive' personal data as personal data relating to a data subject's racial or ethnic origin; political opinion; religious or other similar beliefs; whether he is a member of a trade union; his physical or mental health; his sexual life; commission or alleged commission of an offence

Given staff are encouraged to report incidents regardless of how minor they may be, the key measure is the number of High Risk incidents. The table below sets this out over the last 5 years. The number of incidents should be seen in the context of the massive amount of information handling that the Council carries out safely and securely on a daily basis. The increase from 2013/14 to 2014/15 follows a series of actions to ensure all security breaches were being reported.

	2011/12	**2012/13**	**2013/14**	**2014/15**	**2015/16**	**2016/17 (projected)**
High Risk *Internal*	5	3	8	34	31	24
High Risk *Reportable*	3 (no action taken by the ICO)	9 (the council was fined £90K for 1 incident)	1 (no fine issued by the ICO however a consensual audit was carried out	3 (no action taken by the ICO)	3 (no action taken by the ICO)	4 (no action taken by the ICO to date)

Key roles

Information Governance Team and County SIRO

The Information Governance Team's role is to investigate all security incidents as they occur and provide actions to services on how to improve their procedures to reduce the likelihood of incidents reoccurring. It also has a proactive role in supporting services by actively promoting security awareness, creating security guides and policies and delivering training to teams as required.

The Information Governance Manager acts as the Council's Data Protection Officer and is the ICO's link Officer for high risk reportable incidents. This post reports to the County Senior Information Risk Owner (SIRO) on a monthly basis to discuss and assess potential high risk incident trends, consequences for the Council and impact on data subjects and whether mitigations being put in place by the services are adequate. The SIRO decides whether or not a high risk incident meets the threshold for reporting to the ICO.

Mitigations

Although human error is the primary root cause of most security incidents (which therefore cannot be prevented 100% of the time), the Council has put in place several organisational measures to help reduce the likelihood of incidents from occurring. For example:

- Public Sector Network Compliance – The County Council is accredited to the PSN which requires compliance with a wide range of security measures which demonstrates the County Council has the necessary security measures and procedures in place to share information with Central Government and other Public Sector partners. Accreditation is tested and renewed on an annual basis.

- The council has a Data Protection e-learning training package which is mandatory for all employees to complete (as required by the ICO following the fine in 2012 and audit in 2014). A new version will be rolled out across the council in early 2017;

- The Information Governance team has produced a suite of short security guides and policies for staff which is published on the *Keep Devon's Data Safe* pages on the Source and publicised in Insider and service specific newsletters.

- Regular advice and guidance on how to spot email and phishing scams are being provided via Insider.

- Key staff in services have received face to face training on how to handle personal data securely;

- Peer checking procedures have been implemented across teams who handle the most sensitive personal data and are therefore at greater risk of serious incidents occurring;

- Encrypted email (Egress Switch) has been rolled out to all employees so they can share information securely to partners and the public, which substantially reduces the risk of postal and electronic security related incidents occurring;

- Lockable cupboards have been deployed to all offices where personal data or confidential business data may be held to enable secure filing.;

- In Council buildings, where personal or confidential data may be held systems or protocols are in place to prevent unauthorised persons gaining access, these include the use of CCTV and controlled access (the smart card system). The systems and protocols are reviewed on a regular basis..

- Locked Printing – Multi Function Devices (print, scan, copy) all have the facility to ensure a 4 digit code must be entered before the printed copy can be produced.

4. Impact of breaches

Security incidents can have a huge impact on the Council and more importantly the people it serves. The ICO have the power to levy fines to organisations who suffer a security incident involving personal data up to £500k. As mentioned earlier in this report, the Council was fined in 2012 for such a breach and a consensual audit was carried out by the ICO on the Council in 2014, to ensure the council was taking remedial action to improve its security procedures across the board. There were a number of recommendations from this audit (although no major/urgent actions required) and all recommendations have been actioned.

The impact of breaches cannot solely be measured against financial penalties, reputational damage and compensation claims. There can be very real and damaging effects on the individuals whose data is put at risk.

5. Responsibilities of staff and Members

It is everyone's responsibility to complete the e-learning training, familiarise themselves with and follow the security guides and policies when handling personal data, always use Council ICT equipment and systems correctly and support and promote a security conscious culture. And of course to report an incident if something should happen or go wrong.

The Information Governance Team is available for advice or bespoke training on any of these aspects.

6. Data Protection Reform 2018

It is worth noting that there has recently been a major reform of the EU Data Protection Directive (95/46/EC), which has resulted in a new General Data Protection Regulation (GDPR) being approved, this will come into effect in May 2018. This new legislation will have a significant effect on the UK and the organisations that handle personal data. The GDPR enhances the rights of data subjects and increases the obligations on organisations that

process personal data. Security of personal data is a key theme within the GDPR. Under the new Regulations the ICO will have the power to issue fines to organisations that fail to comply with certain aspects of the GDPR (in particular serious security incidents which result in damage or distress to data subjects) up to a higher value of **20 million euros.**

The SIRO and the Information Governance Manager are in the process of considering the impact of the GDPR and any improvements that need to be made across the Council, to ensure future compliance.

7. Summary

Devon County Council recognises the value and importance of the information it holds and takes very seriously the security of that information. Continued improvement of internal processes, continued awareness and education to embed a security focussed culture and continued investment in technology and tools demonstrate that commitment.

In light of the risk mitigation and improvements set out earlier in the report the Current Data Protection Risk (after mitigating controls are put in place) has now been reduced from High (16) to Medium (12) and will not be elevated onto the Corporate Risk Register.

The importance of information security and the protection of the data we hold will continue to be a major priority and will need continuing assessment as more and more services move into the digital world.

Scrutiny may wish to consider how Information Security is built into all aspects of their work as the Council becomes more digitally developed and practically may wish to consider what role it can play in helping to promote the importance for all employees and Members of handling personal data securely in accordance with the our Keep Devon's Data Safe security guides and policies.

Rob Parkhouse
Head of Digital Transformation and Business Support

Electoral Divisions: ALL

Local Government Act 1972: List of Background Papers
[insert name of any applicable papers or type 'None']

Who to contact for enquiries:
Name: [Amber Badley, Information Governance Manager]
Contact: [01392 384682. Amber.badley@devon.gov.uk]

Cabinet Member: [insert Cabinet Member's name]