POLICY AND RESOURCES SCRUTINY COMMITTEE – 3RD OCTOBER 2017

SUBJECT: **DATA PROTECTION REFORM**

REPORT BY: **ACTING DIRECTOR OF CORPORATE SERVICES AND SECTION 151 OFFICER**

---

1. PURPOSE OF REPORT

1.1 To inform Members of requirements of upcoming data protection reform and corporate action to address these requirements prior to the presentation of this information to Cabinet.

1.2 To request consideration by Members of updates to the Council's Information Risk Management Policy, prior to its approval by Cabinet.

2. SUMMARY

2.1 On the 13th September 2017 the UK government presented a draft Data Protection Bill to the House of Lords to replace the Data Protection Act 1998 and provide a comprehensive legal framework for data protection in the UK, supplementing the requirements of the General Data Protection Regulation (GDPR) which will be directly applicable in the UK from 25th May 2018. In summary, the changes mean a greater requirement for accountability and Privacy by Design. There are also greater rights for data subjects, including rights to know what the Council will do with their data, and mandatory breach reporting within 72 hours. The Bill is scheduled for consideration at a second reading on 10th October 2017.

2.2 The maximum monetary penalty for breaching the Data Protection Act currently set at £500,000 will increase to the equivalent of €20 million or 4% of global annual turnover under GDPR. Monetary penalties could be levied for any breach of the new Act, for example failing to evidence accountability or to report breaches on time, which is an expansion of the current focus on security or marketing breaches.

2.3 GDPR and the forthcoming implementation of the new Data Protection Act comes at a financially challenging time when services must become leaner, requiring more efficient ways of working and collaborations with other organisations. Efficiencies gleaned from new technology, outsourcing, and sharing information with partners needs information governance structures to reduce risk of data breaches as well as risk of poor quality information leading to inappropriate decisions. There are opportunities to make better use of the Council's information assets to benefit service delivery and potentially save costs, as well as addressing increasing demands of requests made under FOI and associated information rights legislation. Members will recall receiving a report on Information Governance at the Policy and Resources Scrutiny Committee in June 2017.

2.4 The Council's Information Risk Management Policy is key in enabling the Council to monitor compliance with these changes, as well as overseeing that Council is making most effective use of its information assets. Cabinet approved this policy on 16 October 2013, and are requested to approve updates to the Policy.

3. LINKS TO STRATEGY

3.1 Information governance is a key part of the Council's corporate governance arrangements and is reflected in the Corporate Services Directorate Risk Register and Annual Governance Statement section of the Statement of Accounts.

3.2 Effective governance of the Council's information underpins all Council activities, safeguarding information assets and using them to maximum effect to help achieve the Council's Priorities and Wellbeing Objectives, as well as the seven Well-being Goals of the Future Generations Act (Wales) 2015:

- *A prosperous Wales*
- *A resilient Wales*
- *A healthier Wales*
- *A more equal Wales*
- *A Wales of cohesive communities*
- *A Wales of vibrant culture and thriving Welsh language*
- *A globally responsible Wales*

4. THE REPORT

What reforms are expected next year?

4.1 On the 13th September 2017 the UK government presented a draft Data Protection Bill to the House of Lords which brings together:

- requirements of the General Data Protection Regulation (GDPR) - directly in force in the UK on 25 May 2018 regardless of Brexit;
- the Data Protection Law Enforcement Directive - UK must implement by 6 May 2018;
- and separate rules for processing personal data for national security purposes.

The Bill is scheduled for consideration at a second reading on 10th October 2017.

4.2 The draft Bill will replace the outdated 1998 Data Protection Act, which was passed a generation ago, before the ubiquity of personal computers, smartphones, Artificial Intelligence, social media, and the myriad components of the digital world that we now live in. In the foreword to the Minister of State for Digital's 7 August publication setting out the intention to develop this Bill, the Minister said that the intention is '…to allow people to be sure they are in control of their personal information while continuing to allow businesses to develop innovative digital services (predicted to benefit the UK economy by up to £241 billion between 2015 and 2020) without the chilling effect of over-regulation…'. The Bill also aims to ensure consistency of data processing both within the EU and outside, with the three stated objectives described as:

- maintaining public trust in handling personal information,
- facilitating future international trade,
- and ensuring security.

4.3 Whilst many of the direct requirements of GDPR are known, national derogations are as yet undecided by the UK government. We are closely monitoring announcements from the government and the regulator, the Information Commissioner (ICO), and if there are further significant impacts on the Council, we will update Members.

Why is additional protection for personal information required?

4.4 Personal information, whether it enables an individual to be identified or whether it is in aggregate, anonymised form, is valuable to businesses and the economy, and organisations that benefit need to abide by rules to protect individuals. It can be distressing for an

individual's personal information to be disclosed to an unexpected third party or to be used in an unanticipated way (with some limited exceptions, e.g. crime detection). Misuse of even basic information such as telephone numbers and email addresses can lead to distressing consequences such as 'cold-calls' and unwanted junk mail – irritating enough for anyone, but particularly harmful to vulnerable people.

4.5 If the Council were responsible for misuse of information this is likely to lead to loss of trust in the organisation, which not only causes reputational damage but could pose a barrier to delivering critical services to service users. There could also be very real financial detriment to service users if key information about them enabled criminals to steal their identity or if financial information was misused. This is illustrated by a 2015 breach by Talk Talk, which led to personal data of 157,000 customers being compromised, including bank details, leading to a £400,000 monetary penalty.

4.6 Risks inherent in handling personal information are reflected in the increase in monetary penalties increasing to €20 million or 4% of global annual turnover under GDPR. The ICO has not been reticent to use the monetary penalty sanctions on publicly funded bodies, with the largest fine for a local authority of £250,000 for Scottish Borders Council for pension records being found in supermarket recycling bank. GDPR changes the landscape, by opening up the possibility of a monetary penalty for breaching any part of the Regulations, not just security or marketing breaches that are currently the focus of monetary penalties.

Benefits for service delivery in financially challenging climate

4.7 The challenges presented by data protection reform are an opportunity to make better use of all the Council's information assets, not just those containing personal data. Services are becoming leaner to meet financial challenges and more efficient ways of working are sought, which will include greater collaborations with other organisations. This increases information risk, but risks can be reduced and the Council's information assets used more effectively by streamlined records management. This will ensure that only necessary information is created, retained and stored for officers to locate quickly to support timely and appropriate decision-making, and saving costs of storing unnecessary records, in hard copy or electronic format.

4.8 Greater openness of non-confidential information across the organisation will also encourage re-use of information assets to benefit other parts of the organisation and ultimately the citizen. Maintaining details of each information asset will benefit other service areas, who will not need to recreate information if they can check whether it exists in another service. It will also help in dealing with information requests under Freedom of Information to statutory timescales, thereby avoiding monitoring by the ICO. There is a government drive to open up public sector information to the public to benefit the economy, and the City Deal's open data initiative is a good example of this in practice.

Key impacts of data protection reform:

4.9 Key changes set out in the GDPR from the existing 1998 Act are listed below, together with detail of how the Council has addressed these changes so far via the Information Governance Project Team work programme.

	Key impacts:	**Addressed by:**
a.	Accountability The 8 existing data protection principles will still apply but are reformatted into 6 principles underpinned by a new principle of accountability. This means that we need to evidence how we have considered privacy in everything that we do, and that all employees are aware of their responsibilities.	Training for all staff on Protecting Information has been in place since 2013, including for non-computer users, to supplement workshops offered since 2005 and the requirements of the Employee Code of Conduct. A review is underway of the Council's existing Data Protection Policy and Information Risk Policy as well as supporting procedures for Privacy Impact Assessments; information sharing (e.g. contract conditions and WASPI agreements); breach reporting; Subject Access Requests, IT security arrangements; etc.
b.	Privacy by Design Closely linked to accountability, Privacy Impact Assessments (PIA's) are a critical part of the new law. Impacts on privacy of processing of personal data, especially if high risk, must be undertaken as early as possible, similar to the consideration of equality impacts that we have become accustomed to over the years.	PIAs balance citizen's privacy against benefits of using personal data to enable a decision on acceptability of risk. PIAs can be very detailed or a simple analysis of pros and cons of an activity, depending on requirement. It is encouraging that PIAs are used increasingly within the Council, not only to reduce privacy risk but also to identify potential obstacles early in a new project to avoid having to repeat work.
c.	Transparency for data subjects People must understand what the Council will do with their data, so clear summary privacy notices must be given as soon as possible, with more detailed information available if required.	Review existing fair processing notices on forms/leaflets/websites. Identify additional processing that requires a Privacy Notice. Layer Privacy Notices by giving GDPR compliant information on website.
d.	Greater rights for data subjects: • to request erasure of information (Right to be Forgotten); • to request correction of inaccurate data; • to seek redress if the Council makes a mistake, including compensation through the courts (action can also be brought on behalf of similarly affected individuals by a representative entity e.g. ombudsman or consumer bodies);	Awareness raising underway amongst all staff of the rights of data subjects so a request can be identified and addressed appropriately. Likely to be an increase in numbers of Subject Access Requests (SARs), which will impact on compliance timescales with other information rights laws such as Freedom of Information. Therefore Information Governance (IG) Stewards are working to make sure records are documented in Service Areas Information Asset Registers to enable prompt administering of all information requests, including SARs.

	• to seek access to personal information about yourself, known as a Subject Access Request (SAR) as long as the request is not "manifestly unfounded or excessive". The current £10 fee will be abolished.	*There will be specific exemptions for research organisations, including Gwent and Glamorgan Archives, for example for* SARs that are too burdensome or for updating/deleting data, subject to certain criteria.
e.	Legal basis for processing personal information There must be a documented legal basis for each instance of processing personal data. Legal conditions are more restricted under GDPR compared to DPA. If the legal basis is consent, there are new rules on consent being proactive, understood and regularly reviewed. Children must have parental consent until they are 13.	Information Asset Registers identify personal data being processed and the legal basis is currently being reviewed, including methods of obtaining consent. Elected Member consent to act on behalf of constituents to be reviewed to make sure the existing process will comply with the new rules.
f.	Data breach reporting within 72 hours Mandatory if the breach is likely to result in a risk to the rights and freedoms of an individual. Previously this has only been a mandatory requirement for the health sector, although local authorities are encouraged to report significant breaches. Failure to report will increase the amount of any monetary penalty that is levied.	Existing data breach procedure is embedded, but the policy will be updated including criteria for reporting breaches, and awareness to be raised through training. Reporting of relevant IT security breaches will also be incorporated.
g.	Enforcement: Current ICO investigative powers (including the right to enter buildings), civil sanctions, criminal sanctions and monetary penalties still exist.	Once GDPR preparation is completed, Information Governance Project Team will turn its attention to ensuring the law continues to be properly adhered to, to reduce risk of being subject to enforcement action. Audit of Service Areas, partners and contractors will be considered.
h.	ICO register of Data Controllers There will no longer be a requirement to notify the ICO of personal data processing, but there will be a requirement for Data Controllers to know what information is processed and how it is managed.	Information Asset Registers for each service are under review to make sure they capture all information required, not just for GDPR compliance but also to enable better use of Council resources by all Service Areas. .

Oversight of preparation for data protection reform

4.10 There is a lot to do to make sure the Council is prepared by May 2018, and this is identified as one of two areas to improve in the Annual Governance Statement for 2017/18. The *Information Governance Work Programme drives preparation, and* progress is monitored through the Corporate Services Directorate Risk Register and by regular updates to Corporate Governance Panel. The *report to* Policy and Resources Scrutiny Committee on 6 June 2017 on Information Governance during 2015 and 2016 also informed Members of proposals.

4.11 The work programme is being led by the Senior Information Risk Owner (SIRO) and Corporate Information Governance Unit (CIGU). Key tasks are being undertaken CIGU (collaborating with other local authorities at South Wales Information Forum to share the workload where possible) and Information Governance Stewards for each Service Area. Progress depends on available resource as CIGU is handling increasingly complex information requests and high volumes of data protection advice, the latter triggered by raising awareness of data protection leading to officers Council-wide more aware of their responsibilities; and IG Stewards are preparing for the changes in addition to their substantive posts. Therefore an approach of prioritising the highest risks is being taken.

4.12 Under GDPR organisations must appoint a data protection officer if the organisation is large and processes specific types of personal data. The DPO must:

- have professional experience and knowledge of data protection law;
- report to the highest management level of the organisation, ie board level;
- operate independently and must not be dismissed or penalised for performing their task;
- and have adequate resources (staff and skills) to meet their GDPR obligations.

Members are asked to note this requirement, a report on which will be presented to Audit Committee in the coming months. The Council has evolved a number of different arrangements for supervision of Information Governance since 1998 as legislative requirements have changed, and this is an opportunity to review arrangements to achieve more consistency.

Key evidence of accountability to ensure data protection compliance

4.13 The Information Risk Management Policy approved by Cabinet in 2013 has been updated to cover new data protection requirements, and approval for the updated version of the Policy in Appendix 1 is sought. The main changes include promoting use of Privacy Impact Assessments when necessary, and frequency of reports on Service Area Information Risk Registers to the SIRO changing from quarterly to six monthly. The latter reflects Corporate Governance Panel's assessment that as the registers are reviewed within Service Areas regularly, there are opportunities to update them immediately if a significant risk is identified, but in the main six monthly reports to the SIRO are sufficient.

4.14 A key tool to implement this policy is the Information Asset Register, which if fully updated gives the Council confidence that its information is not only compliant with data protection law, but also that information assets are used to best effect Council-wide. The updated Information Risk Management Policy emphasises the role of this Register in more detail than previously.

4.15 Whilst the Information Commissioner acknowledges that it is impossible to eliminate human error, evidence of processes to reduce risk are expected, with training and awareness-raising key, and this has been strengthened in the updated Information Risk Management Policy. Since 2013 Heads of Service committed via their Information Risk Registers to regular completion of Protecting Information training by all their employees, and all staff were requested to repeat the training in July 2017 to make sure their knowledge is up-to-date. The training is delivered mainly via a short e-learning course, supplemented by a booklet for non-computer users and additional awareness materials on the Information Governance intranet, including posters displayed Council-wide. Mandatory annual training will be relaunched next

spring to cover new data protection requirements, and a new method of delivering the training assessment is being developed so that Heads of Service can access readily available reports. The Elected Members mandatory annual Information Governance training covered the basics data protection reform during 2017, and more detail will be given when the training is repeated next year.

4.16 Improvements in line with the Council's Records Management Policy continue to ensure records are well managed to ensure GDPR compliance, to underpin service delivery with reliable, easily located information and to ensure compliance with the Lord Chancellor's Code of Practice on Section 46 of the Freedom of Information Act, which the Council can be audited against.

Upcoming risk areas

4.17 Contracts and agreements supporting existing partnerships and outsourcing arrangements need to be reviewed, highest risk first, but there are also increasing numbers of new collaborations and joint systems that require assessment of data controller relationships and privacy impacts at the outset. Examples are the Welsh Community Care Information System (WCCIS), Greater Gwent Pension Scheme, SenCOM, Education Achievement Service, and even schools. This requirement is strengthened in the updated Information Risk Management Policy.

4.18 Records backlogs in all formats (electronic, including email, as well as hard copy), are being addressed in line with the Council's Records Retention and Disposal Policy, to reduce risks of keeping records that have met their disposal date and also reduce impact of information requests.

4.19 Security threats (physical and electronic) are increasing, and are being considered by Corporate Security Group and by IT Security, in particular via compliance with the ISO270001 standard and stringent requirements to enable the Council's IT infrastructure to be part of the PSN network.

4.20 Information requests continue to be a challenge to answer on time as outlined in the table below, mainly due to growing complexity of questions and time available in service areas to respond. In 2017 the Information Commissioner revised her expectation of compliance from 85% to 90%, and will monitor organisations not achieving this target. Combined with abolition of the £10 fee and the inherent complexity of SARs, it is anticipated that compliance with information requests timescales will become even more challenging. Therefore data protection reform is being used as the impetus to improve management of all records. This includes maintenance of Information Asset Registers and proactive publication of information to give the Council better intelligence on what information is held and where they it is located, speeding up processing of information requests.

	Council target	**2014**	**2015**	**2016**	**2017 Jan - July**
Information request quantities (FOI and SAR)		1177	1144	1176	652
FOI request responses within statutory timescales (ICO expectation – 90%)	80%	76%	85%	83%	80%
DPA SAR request responses within statutory timescales	70%	80%	69%	59%	75%

5. WELL-BEING OF FUTURE GENERATIONS

5.1 This report contributes to the Well-being Goals as set out in Links to Strategy above. It is consistent with the five ways of working as defined within the sustainable development

principle in the Act in that effective management of the Council's information will ensure reliable, high quality information is held which could be shared with other partners to ensure a joined up approach to providing services and preventing problems, as well as to enable close working with communities affected by the Council's activities. Reliable information also ensures that decisions are more robust now and in the long-term and preservation of the Council's historic record means that current and future generations can hold the Council to account for its decisions and learn from previous activities.

6. EQUALITIES IMPLICATIONS

6.1 There are no potential equalities implications of this report and its recommendations on groups or individuals who fall under the categories identified in Section 6 of the Council's Strategic Equality Plan. There is no requirement for an Equalities Impact Assessment Questionnaire to be completed for this report.

6.2 The Council provides FOI information in the format that the applicant requests and this combined with Welsh language responses to FOI requests made in Welsh contributes to compliance with the Council's Strategic Equality Objective 4 – Improving Communication Access and the Council's Welsh Language Standards Compliance Notice.

7. FINANCIAL IMPLICATIONS

7.1 Financial implications may result from the programme of improvements necessary to assure the Council's information during this period of significant Council change.

7.2 Monetary penalties that can be levied for data breaches are increasing from £500,000 to the equivalent of €20 million or 4% of global annual turnover following the implementation of the General Data Protection Regulation (GDPR) in May 2018.

8. PERSONNEL IMPLICATIONS

8.1 The Information Governance Work Programme has implications on the workloads of staff Council-wide, but in particular on Corporate Information Governance Unit and Information Governance Stewards.

9. CONSULTATIONS

9.1 All responses from consultations have been incorporated in the report.

10. RECOMMENDATIONS

It is recommended that:

10.1 Members note requirements of upcoming data protection reform and corporate action to address these requirements.

10.2 Members consider the revised Information Risk Management Policy attached at Appendix 1 and provide their comments prior to its approval by Cabinet.

11. REASONS FOR THE RECOMMENDATIONS

11.1 To ensure the Council is compliant with changes required by data protection reform, to protect service users, employees and the organisation from data breaches and monetary penalties.

12. STATUTORY POWER

12.1 General Data Protection Regulation 2016.

12.2 Data Protection Act 1998 (still in force but due to be repealed by the Data Protection Bill).

12.3 The Data Protection Law Enforcement Directive 2016.

12.4 The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981.

12.5 Proposed UK Data Protection Bill (expected 2017-2018).

12.6 Other privacy legislation such as Privacy and Electronic Communications Regulations 2003 and Human Rights Act 1998.

12.7 Information rights legislation such as Freedom of Information Act 2000, Environmental Information Regulations 2004, Re-Use of Public Sector Information Regulations 2005, and INSPIRE Regulations 2009.

12.8 Section 60 Local Government (Wales) Act 1994 on duty to maintain records, supplemented by the FOI Section 46 Statutory Code of Practice on Records Management.

Author: Joanne Jones, Corporate Information Governance Manager
Consultees: Paul Lewis, Acting Head of ICT and Customer Services
Cllr Colin Gordon, Cabinet Member for Corporate Services
Corporate Management Team (21 September 2017)
Gail Williams, Interim Head of Legal Services & Monitoring Officer
Lisa Lane, Solicitor
Lynne Donovan, Acting Head of Human Resources and Organisational Development

References:

- Department for Digital, Culture, Media and Sport 'New Data Protection Bill – our planned reforms', August 2017 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf
- ICO Guide GDPR, including DPO https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/#dpos
- Policy and Resources Scrutiny Committee Report on Information Governance, June 2017

Background papers:
Policy and Resources Scrutiny Committee 6 June 2017 report on information Governance.
Cabinet 16 October 2013 report on Information Risk Management.

Appendices:
Appendix 1 – Information Risk Management Policy (see also paragraphs 4.13 to 4.17 of this report).