

REPORT TO: Business Efficiency Board

DATE: 21 November 2018

REPORTING OFFICER: Strategic Director – Enterprise,
Community and Resources

PORTFOLIO: Resources

SUBJECT: General Data Protection Regulation
(GDPR)

WARDS: Borough Wide

1.0 PURPOSE OF THE REPORT

1.1 This report provides an update regarding the implementation of the new GDPR Data Protection legislation and overall update on the Council's position regarding information governance.

2.0 RECOMMENDATION: That the Business Efficiency Board notes the content of the report.

3.0 BACKGROUND

3.1 The Senior Information Risk Owner (SIRO) is the officer responsible across the whole Council for Information Governance. The SIRO is responsible for the strategy, acts as an advocate for good practice in Information Governance and is required to provide a statement of assurance as part of the Council's Annual Governance Statement. The Strategic Director, Enterprise, Community & Resources is Halton Borough Council's SIRO and is supported by the Divisional Manager, Service Improvement who is the Assistant SIRO and the Council's Data Protection Officer.

3.2 Information governance means the effective management of information in all its forms and locations. It encompasses efficient ways of handling information, robust management of the risks involved in the handling of information, and compliance with regulatory and statutory guidance including Data Protection and Freedom of Information.

3.3 Information governance is about electronic and paper based information, about how it is held, used and shared. The importance of good information governance has been highlighted by the Information Commissioner (ICO) and the Permanent Secretary for the Department for Communities and Local Government. Members of this Committee will have read the stories of significant fines faced by other public sector bodies for failures to manage information properly.

3.4 Information governance is also concerned with keeping information safe and secure and ensuring it is appropriately shared when necessary to do so. This is a significant challenge for all organisations but particularly so for large complex public sector organisations, such as the Council, dealing with a wide range of functions.

4.0 The General Data Protection Regulation (GDPR)

4.1 Members were previously advised of the forthcoming General Data Protection Regulation (GDPR) which was intended to strengthen and unify data protection for individuals and became applicable to this Council and Members from 25th May 2018. It heightens the standards required as well as imposes new obligations.

4.2 Among the regulations, there are changes to the potential legal justifications for processing data, significant changes to the requirements for consent, heightened requirements for privacy notices and increased rights for the data subjects.

4.3 GDPR required various modifications to how the council processes its data across the organisation and with its partners, providers and members of the public and work is ongoing across directorates to facilitate this. In recent months, the ICO has been providing helpful guidance and clarity in relation to GDPR that is being used across the organisation.

4.4 The regulations allow for the ICO to impose administrative fines up to a maximum of 20 million Euros (approx. £18m) for infringements. The ICO, in recent months, have made it clear that they intend to proportionately regulate, notwithstanding their new and increased powers.

4.5 To prepare for the legislation, officers across the council have been looking at the readiness of directorates for the necessary changes. A number of progress reports were made to the Management Team and in the Autumn of 2017 and Spring 2018 and a significant number of meetings took place across the council in developing readiness for GDPR.

4.6 Changes to policies, in the light of guidance received from the ICO have been approved and overseen by the Information Governance Group and the ICT Strategy Board and have been circulated to all relevant staff.

4.7 It must be remembered that the organisation has not allocated additional resource to deliver this significant change and officers are delivering this in addition to their “day jobs”.

- 4.8 The council has adopted a proportionate response to compliance with GDPR and this will mean that work is on-going. As part of our learning culture, we will continue to reflect on decisions by the ICO and develop and amend our policies as the regulation begins to be enforced.
- 4.9 The Information Governance Service have worked in conjunction with the Corporate Communications team to raise awareness in relation to GDPR through updates in “News in Brief” to build knowledge and awareness.
- 4.10 Further updating of staff took place during the spring / summer with weekly updates on the necessary steps and preparation ahead of May.
- 4.11 Members received initial training on information governance and data protection as part of their induction sessions after the election in May. Given the impact of the new regulations on Members have been offered individual training on the GDPR.
- 4.12 Staff training was provided in the autumn and spring as an overview of GDPR and the repercussions of this new legislation on their particular areas of work.
- 4.13 Implementation of GDPR has now passed the intensive phase. The project is being led by Divisional Manager, Service Improvement supported by the Information Governance Service together with officers on an Information Governance Group.
- 4.14 The Information Governance Group was established in 2010 with representation from across the organisation and had been meeting on a monthly basis to work through the GDPR project plan to follow and implement the ICO guidance notes and to achieve readiness.
- 4.15 The Information Governance Service are supporting colleagues across the Council in the renegotiation of Information Sharing Agreements with the Council’s partners that underpin much of the multi-agency work in Halton – this again is on-going work.
- 4.16 GDPR requires organisations to appoint a Data Protection Officer. The DPO’s basic tasks are defined in Article 39:
 - a) To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
 - b) To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.

- c) To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

4.17 The Board will also be aware that Internal Audit undertook a recent review of the Council's arrangements in preparation of the GDPR regulations and gave a 'substantial' rating.

5.0 Update on Information Governance Training

5.1 Members of this committee will be aware that officers are required on a mandatory basis to complete training on Data Protection and Information Governance. This mandatory training requirement has been extended to include GDPR and all officers will be required to undertake the training.

5.2 Given the enhanced obligations placed on the Council by GDPR, it is the view of the Monitoring Officer that consideration should be given to Members also being required to complete the training that is mandatory for staff.

5.3 The training is an online and interactive course that can be undertaken via the Council's intranet.

6.0 Data Breaches

6.1 Information Governance Service maintains a log of personal data breaches that have been investigated and referred to the SIRO to agree on the level of the breach and whether the breach should be reported to the ICO.

6.2 There are formal arrangements to identify and mitigate risk in accordance with Council's information governance requirements and there are effective mechanisms in place to report and manage serious untoward incidents.

7.0 Ongoing Work

7.1 A full review of Council's Information Governance requirements continues, includes:-

- Ongoing work required for the 2018 General Data Protection Regulation for the authority and schools
- Completion of a Corporate Information Asset Register
- Compiling a master set of GDPR Privacy Notices
- Training material on GDPR for members of the Council
- IG toolkit assessment for 2018/2019
- Follow up Internal Audit's recommendations following review of SAR process

8.0 POLICY IMPLICATIONS

8.1 There are no specific policy issues associated with this request.

9.0 OTHER IMPLICATIONS

9.1 As mentioned earlier in the report, no additional resources have been used to ensure the Council is prepared for the GDPR. All work has been undertaken within existing resources.

10.0 IMPLICATIONS FOR THE COUNCIL'S PRIORITIES

10.1 Sound information governance is important for the delivery of all of the Council's priorities.

11.0 RISK ANALYSIS

11.1 There are significant risks both financial and reputational if the Council does not have robust arrangements in place to use personal data only for the purposes it collects it for. Individuals trust the Council with their data and those individuals rely on the Council to use it appropriately. It is important that the Council keeps those arrangements under review and improves them in the light of experience and technological advances.

12.0 EQUALITY AND DIVERSITY ISSUES

12.1 There are no equality and diversity issues associated with the report.

13.0 LIST OF BACKGROUND PAPERS UNDER SECTION 100D OF THE LOCAL GOVERNMENT ACT 1972

13.1 None.