

## INFORMATION GOVERNANCE (DATA PROTECTION) IN HILLINGDON

<b>Committee name</b>	Corporate, Finance & Property Select Committee
<b>Officer reporting</b>	Raj Alagh, Borough Solicitor
<b>Papers with report</b>	None
<b>Ward</b>	All

### HEADLINES

This report advises the Select Committee of the information governance arrangements in place within Hillingdon and how the Council ensures full compliance with the General Data Protection Regulation (“GDPR”) and the Data Protection Act 2018.

### RECOMMENDATION:

**That the Committee notes the content of the report.**

### SUPPORTING INFORMATION

In May 2018 the European Union’s General Data Protection Regulation (GDPR) came into force. The general effect of the GDPR was to considerably strengthen the legislation relating to the processing of data by enhancing the protection given to individuals and to require data controllers (an example being the Council processing residents’ data) to demonstrate that they have a lawful basis for processing all data. The GDPR also introduced a requirement for organisations to conduct data protection impact assessments before new procedures that may impact on an individual’s privacy (such as the installation of new CCTV cameras or where children are involved) are introduced.

The Data Protection Act 2018 was also enacted in May 2018 and brought the GDPR into English domestic law and the GDPR and Data Protection Act 2018 are read together.

Importantly, GDPR requires organisations to only retain data for as long as is necessary and gives individuals the right to request that their data is erased and for any mistakes to be corrected. Further, it is for the Council to demonstrate why information has been retained or destroyed and in this regard ,organisations are required to show that they adhere to a Data Retention Schedule.

The GDPR enhanced the powers of the Information Commissioner (“ICO”) to impose fines in the event of the legislation being breached. Prior to 2018, the ICO could issue a fine of up to £ 500,000 for the most severe breaches of data protection. The GDPR now permits a fine of up to £ 17.5 Million to be issued.

For the first time the GDPR required all organisations to appoint a statutory Data Protection Officer. The Borough Solicitor was appointed to this role in January 2018. In order to ensure that the Council was fully prepared for GDPR a working group chaired by the Borough Solicitor and

comprising representatives of Legal Services, Policy and Internal Audit was established to review all of the Council's existing data protection policies and procedures to ensure that they remained fit for purpose and to raise awareness of GDPR across the Council.

Approximately 40 training sessions were held for Council employees prior to May 2018 and all employees and contractors were required to undertake a compulsory online GDPR Training Module once GDPR came into force.

At its meeting in May 2018 Cabinet approved a number of policies and procedures which demonstrate how the Council complies with the GDPR, including:

1. Data Protection Policy.
2. GDPR Golden Rules.
3. Information Governance Policy.
4. Data Protection Impact Assessment Policy.
5. Data Retention and Deletion Policy.

All of these policies are readily available to staff on Horizon (the Council's intranet).

Cabinet also resolved that all members of the Council would receive data protection training from the Borough Solicitor which was duly delivered.

### **Responsibility within Hillingdon**

All staff are responsible for ensuring compliance with all Council policies and procedures and accountability for their service areas rests with corporate directors. The Borough Solicitor, as statutory Data Protection Officer, is responsible to the ICO and can be required to provide any information in connection with data protection. The Data Protection Officer must report any data breach that affects the rights and freedoms of others to the ICO within 3 days and the ICO has extensive enforcement powers including conducting audits of the Council's working arrangements, serving improvement notices and the imposition of fines for breaches of the legislation.

Training is ongoing with all staff required to undertake an annual GDPR electronic training module. Prior to lock down in March 2020 weekly training sessions were taking place to raise awareness of data protection requirements, particularly relating to freedom of information and subject access requests.

The arrangements for elected members are different within Hillingdon. Each councillor maintains their own individual registration with the Information Commissioner and is responsible for ensuring compliance with the legislation. As stated above, all elected members have received training on the GDPR and this training will again take place after the next local elections in May 2022.

### **Hillingdon's Compliance**

Over the last year 1 data protection breach had to be reported to the ICO. This concerned the loss of confidential papers which had been sent to an old address of a panel member. The ICO decided not to take any formal action in respect of this breach but recommended that Council

procedures were tightened to minimise the risk of any future breaches. In this regard, any confidential papers which need to be delivered outside of the Council (at the time the panel was working remotely) will now be delivered by a courier who is instructed to return the documentation if it cannot physically be handed to the addressee.

The most common cause of data breaches within the Council is by documents being sent to the wrong email address, largely because of the use of predictive text. In order to minimise this possibility, staff are recommended to double check with a colleague that the correct email address has been used when sending sensitive information. However, this is not always possible when staff are working remotely.

As stated above it is a general rule that information concerning an individual cannot be disclosed to a third party without their consent and it is for the Council to demonstrate that consent has been freely given or that the Council has other lawful authority to disclose information about an individual.

In this regard, the GDPR authorises the disclosure of information without the consent where, for example, information is requested by the police in order to prevent or detect crime or where information is requested by a medical professional or other statutory body for safeguarding purposes. Similarly, the Council is frequently served with court orders requiring it to disclose information about an individual where that information is relevant to legal proceedings, the most frequent example being family disputes. In order to protect the Council's interests, these cases are all dealt with by the Information Governance Lawyer.

The Hillingdon Information Assurance Group (HIAG) comprises senior representatives from all Council departments and meets on a quarterly basis to discuss any information governance issues. HIAG has authority to implement any changes that are necessary to ensure full compliance with the legislation. In addition, HIAG is responsible for sharing best practice across the Council and ensuring that lessons are learnt from all data protection breaches and other problematic cases.

Further, in 2020 Internal Audit conducted a review of the Council's data protection arrangements and made a number of recommendations for improvement. All of these recommendations have been implemented, including ensuring that the Council's Data Retention and Destruction policy is fully up to date and reflects best practice as well as the legislation.

In conclusion, the Council has done everything possible to ensure that there is a robust data protection regime in place across the whole spectrum of its services. However, it is inevitable that human error will arise from time to time within such a large organisation but to date, the Council's data protection policies and practices have ensured that it is able to satisfactorily address any challenges which have arisen.

The Borough Solicitor will attend the Select Committee meeting and will be happy to answer any questions which Members may have.

### **Implications on related Council policies**

There are no implications on Council policies that arise from this report.

### **How this report benefits Hillingdon residents**

Having robust data protection policies and practices in place helps to safeguard residents' personal data in their dealing with the Council.

### **Financial Implications**

There are no direct financial implications arising from this report. Non-compliance with GDPR leading to data breaches would expose the Council to the risk of significant financial penalties.

### **Legal Implications**

The Borough Solicitor confirms that the legal implications are included in the body of the report.

### **BACKGROUND PAPERS**

NIL