GENERAL DATA PROTECTION REGULATION (GDPR) COMPLIANCE / CYBER SECURITY

Executive Summary

This report deals with two matters. First, the Council's compliance with the requirements of the General Data Protection Regulation (GDPR). Second, cyber security issues affecting the Council.

General Data Protection Regulation (GDPR)

The GDPR came into effect on 25 May 2018. Together with the related Data Protection Act 2018, the GDPR introduced stronger data protection rights and controls.

At its meeting on 22 March 2018, the Executive was advised of the action taken, and to be taken, to ensure that the Council was GDPR compliant on 25 May 2018.

As part of the internal audit plan for 2018/19 agreed by the Standards and Audit Committee, the Council's Internal Auditor undertook an internal audit of GDPR at the Council. The internal audit report was published in July 2019.

This report provides the Executive with an update on the Council's compliance with the GDPR.

Cyber Security

Cyber security is the practice of protecting computers, networks, programs and data from malicious attacks.

At the end of 2018, the Council undertook a cyber-security stocktake sponsored by the Local Government Association (LGA). The stocktake assessed the measures that the Council has in place at the levels of:

Leadership, reporting and ownership

Governance structures and policies

Partnerships, information advice and guidance

Technology standards and compliance

The assessment resulted in a report containing details of where the Council can make improvements in our cyber security procedures, to mitigate the risk of being compromised by a cyber-attack.

Recommendations

The Executive is requested to:

RESOLVE That

the position regarding the Council's compliance with the General Data Protection Regulation (GDPR), and the cyber security issues affecting the Council be noted.

Reasons for Decision

Reason: To ensure that the Council has oversight of GDPR and cyber security issues affecting the Council.

The Executive has the authority to determine the recommendation set out above.

Background Papers: None that are public.

Reporting Person: Peter Bryant, Head of Democratic and Legal Services
Email: peter.bryant@woking.gov.uk, Extn: 3030

Contact Person: Peter Bryant, Head of Democratic and Legal Services
Email: peter.bryant@woking.gov.uk, Extn: 3030

Adele Devon, ICT Manager
Email: adele.devon@woking.gov.uk, Extn: 3279

Portfolio Holder: Councillor Ayesha Azad
Email: cllrayesha.azad@woking.gov.uk

Shadow Portfolio Holder: Councillor Ann-Marie Barker
Email: cllrann-marie.barker@woking.gov.uk

Date Published: 15 November 2019

1.0 Introduction

1.1 This report deals with two matters. First, the Council's compliance with the requirements of the General Data Protection Regulation (GDPR). Second, cyber security issues affecting the Council.

2.0 General Data Protection Regulation (GDPR)

2.1 The General Data Protection Regulation (GDPR) came into effect on 25 May 2018. Together with the related Data Protection Act 2018, the GDPR introduced stronger data protection rights and controls.

2.2 At its meeting on 22 March 2018, the Executive was advised of the action taken, and to be taken, to ensure that the Council was GDPR compliant on 25 May 2018.

2.3 As part of the internal audit plan for 2018/19 agreed by the Standards and Audit Committee, the Council's Internal Auditor undertook an internal audit of the GDPR at the Council. The internal audit report was published in July 2019. Under the Council's Constitution, the Standards and Audit Committee is responsible for overseeing the internal audit service and monitoring compliance with internal audit recommendations. However, it is appropriate that the Executive is advised of the internal audit findings as part of this report on GDPR compliance.

2.4 The overall assurance opinion of the internal auditors, based on their assessment of (i) the controls in place and (ii) the level of compliance with those controls, was that the position was "satisfactory". This assessment was made against four possible descriptors, i.e. "nil", "limited", "satisfactory" and "substantial".

2.5 The internal auditors made three recommendations. Two were of medium priority, and one of low priority. The two medium priority recommendations related to (i) documenting more fully the basis on which some processing activities are carried out by the Council and (ii) ensuring that all relevant third-party contractors to the Council had signed up to having GDPR compliant processes in place. The low priority recommendation concerned ensuring that all staff received the on-line GDPR training (this related to new starters and staff on long-term leave). Steps have been/are being taken to address these recommendations.

2.6 The GDPR introduced an obligation on organisations to report some data breaches to the Information Commissioner's Office (ICO). A breach is reportable if it is likely to result in a risk to a person's rights and freedoms. Whether this is the case is assessed against guidelines issued by the European Union Agency for Cyber Security (ENISA). There have been eighteen data breaches since May 2018, of which three have been reported to the ICO. The most common breaches relate to emails being sent, or cc'd, to the wrong persons. Additional guidance has been issued to minimise the chances of this happening. The reportable cases concerned:-

(i) Confidential information was circulated outside the Council by an agency employee, allegedly on social media.

(ii) Brookwood Cemetery was the subject of a cyber security incident in respect of a fraudulent invoice.

(iii) Email sent to wrong person, containing sensitive personal information

In the case of incidents (i) and (ii) above, appropriate remedial action was taken as part of the reporting process. Incident (iii) has only recently occurred and the ICO has not completed its investigation.

3.0 Cyber Security

3.1 The Council was assessed by the Local Government Association (LGA) and given a rating to identify the areas where there was considered most risk. The rating was assessed as a RAG flag. The detail below summarises the LAG assessment and actions the Council is taking to address high risk areas. Following the assessment, a program to address areas for improvement was produced.

<u>Leadership, reporting and ownership</u>

3.2 LGA Assessed as Green.

3.3 The Council has a Cyber Security Board consisting of the Head of Democratic and Legal Services (the Council's Data Protection Officer) and the ICT Manager as standing members. Other Officers attend when appropriate. The Board meets monthly to discuss the improvement program resulting from the LGA stocktake and any other relevant data or cyber security issues. A quarterly report is presented to CMG.

<u>Governance structures and policies</u>

3.4 LGA Assessed as Amber.

3.5 The areas which were identified for improvement were around the risk registers, business continuity and emergency planning, responsibilities for Security Policies and the testing of ICT disaster recovery plans.

3.6 Although the Council has the procedures in place to manage risk, business continuity, emergency planning and ICT disaster recovery, there is no specific cyber security risk register which has resulting risks identified within the business continuity, ICT Disaster recovery or emergency planning. A risk register will be completed this year for cyber security, and incorporated into the associated plans as detailed.

3.7 Although the ICT Disaster recovery procedures have been partially tested, there is a requirement to undertake a full test. This is currently being planned, but due to the inherent risk of instigating such a test, key processing dates and events must be avoided to ensure there is minimum risk to the business.

<u>Partnership, information, advice and guidance</u>

3.8 LGA Assessed as Amber.

3.9 There are a number of organisations which provide advice and guidance on cyber security matters and although we had engaged with some of them, we were not members of a Warning, Advice and Reporting Point (WARP) organisation. The Council is now a member of the South East WARP (SEGWARP) and attends the regular meetings. We have also engaged with the National Cyber Security Centre (NCSC), using their website as a source of information to assist with the improvement plan.

<u>Technology, standards and compliance</u>

3.10 LGA Assessed as Red.

3.11 The Council has not certified against ISO27001 or any other recognised standard, although we are formally assessed for PSN compliance every year and maintain the security standards required for accreditation.

3.12 There are a number of standards for compliance which are being discussed at the SEGWARP meetings. As the PSN is being decommissioned, the Council will review, with other Local Authorities, appropriate security standards to begin a program of compliance over the next year.

<u>Technology and standards – Identification</u>

3.13 LGA Assessed as Green.

3.14 The Council has identified key operational services, technologies and suppliers.

<u>Technology and standards – Protect</u>

3.15 LGA Assessed as Amber.

3.16 The Council was identified as needing to take action on two key points, holding sensitive data in an encrypted format and segregating servers containing sensitive data. Further advice is required in this area as the Council holds sensitive data in all areas of the business and this data can be accessed across business areas as appropriate and managed by permissions. The whole of the Council's data network is therefore secured to an appropriate level for sensitive data. Action may need to be taken following further investigation.

<u>Technology and standards – Detect</u>

3.17 LGA Assessed as Red.

3.18 Since the stocktake, additional monitoring has been put in place on the network perimeter and internal firewalls to detect and prevent intrusion. Monitoring was also increased to report on system events but this has not proved to be a sustainable option to volumes and specific software may be required to undertake these checks.

<u>Technology and standards – Respond</u>

3.19 LGA Assessed as Amber.

3.20 Further work is required to update the incident response policy to take account of different scenarios and ensure that resources are sufficient to enact the policy.

<u>Technology and standards – Recover</u>

3.21 LGA Assessed as Green.

3.22 The Cyber Security Board reviews incidents to improve processes and update risk registers and policies.

<u>Training and Awareness</u>

3.23 LGA Assessed as Red.

3.24 The Council is currently reviewing options for on-line training, and also updating all the Council's security policies, to increase awareness and mitigate against cyber-attacks. Training will be rolled out to all officers, Councillors and relevant partners using the Council's data network.

4.0 Conclusions

4.1 The results of the internal audit report on GDPR and the LGA stocktake on cyber security have not raised any issues of particular concern. The Council's approach to both matters is good, although improvements can be made. Issues raised in the internal audit report and the LGA stocktake are being addressed.

4.2 It is good practice for there to be Member oversight of data breaches and cyber security. An annual report will, therefore, be presented to the Executive. Further reports will be presented if, and when, it is appropriate to do so.

5.0 Implications

Financial

5.1 None arising from this report.

Human Resource/Training and Development

5.2 Cyber security training is to be delivered to all officers, Councillors and relevant partners on the data network and Councillors.

Community Safety

5.3 None arising from this report.

Risk Management

5.4 Cyber Security Risk Assessment to be undertaken.

Sustainability

5.5 None arising from this report.

Equalities

5.6 None arising from this report.

Safeguarding

5.7 None arising from this report.

6.0 Consultations

6.1 None.

REPORT ENDS