Corporate Governance and Standards Committee Report

Ward(s) affected: n/a

Report of Director of Strategic Services

Author: Ciaran Ward

Tel: 01483 444072

Email: ciaran.ward@guildford.gov.uk

Lead Councillor responsible: Joss Bigmore

Tel: 07974 979369

Email: joss.bigmore@guildford.gov.uk

Date: 22 April 2021

Data Protection and Information Security Update

Executive Summary

The transactions and interactions customers, residents, and staff make with the Council often involves the sharing of personal data, for example, in relation to council tax accounts, housing agreements, employment contracts.

It is therefore important that this data is used only in ways reasonably expected, and that it stays safe. Similarly, the secure collection, storage, and transfer must be executed with regard to sound cybersecurity practices.

Recommendation

That the Committee notes this report.

Reason for Recommendation:
To keep the Committee informed of progress with various data protection and information security initiatives that have taken place since the last annual report.

Is the report (or part of it) exempt from publication? No

1. Background

1.1 It is now almost three years since the General Data Protection Regulation (GDPR) came into force. Although the UK has left the European Union since then, the basic principles of the GDPR continue to apply. A number of positive advances have taken place within the Council during this time.

1.2 This report will cover developments in data protection and information security within the Council since the last annual report of March 2020.

2. Update on progress in 2020

2.1 Information Governance and Information Assurance Successes since March 2020

- Policy page on intranet updated, encompassing release of new cloud-based suite of GBC branded information security and ICT-related policies/procedures, and guidance on email encryption (updated to reflect organisational changes following migration of Council network to Office 365) – including guidance on acceptable use of ICT systems, access control, anti-virus measures, business continuity, use of mobile devices, cybersecurity, password/authentication and related areas.
- Phasing out of old Sharepoint system and replacement with new and more efficient cloud-based Office 365 version for the storage of folders and documents.
- Successful take-up of Office 365, especially the use of Microsoft Teams for virtual meetings out of necessity due to large scale working at home during the Covid-19 lockdown period over the past 12 months which has coincided with the allocation of laptops to office-based staff.
- New GDPR online training for all new starters – included as part of a suite of online training programmes provided by Workrite.
- Implementation of DMARC (Domain-based Message Authentication, Reporting and Conformance), a system set up to tackle email spoofing[1]. DMARC aims to reduce email spam by approximately 80% to 90%. Examples of fraudulent spam messages in the past have included fake emails purporting to be from GBC's council tax department which tell the recipient they owe a sum of unpaid council taxes.
- PDNS (Protective Domain Name System), a system created by government agency the National Cyber Security Centre (NCSC). PDNS scans the network for suspicious emails by mapping IP addresses to names, thereby hampering the use of domain name systems for malware distribution and preventing access to malware, ransomware, phishing[2] attacks, viruses, malicious sites and spyware at source - thus making the network more secure.
- Removal of legacy Government Connect Secure Extranet (GCSx) email infrastructure, as traffic within "gov.uk" email domains now recognised as being secure.
- Information Assurance Officer has carried out work in conjunction with Ignite around cloud-based systems and mandated internal and external penetration tests of all new systems.

---

[1] **Spoofing** - The creation of email messages with a forged sender address often designed to trick the receiver into believing they come from a legitimate source (e.g. a bank or utility supplier) for the purposes of unlawful financial gain. Spoof emails often have the intention of spreading malicious viruses.

[2] **Phishing** – a fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication – e.g. emails or text messages - which often direct users to enter personal data at a fake website which matches the look and feel of the legitimate site.

- Information Assurance Officer managed KPMG auditors to complete a Cyber Security and Privacy Report – which has resulted in the new suite of policies as referenced above.
- Continue to provide advice and guidance to staff in relation to Covid related phishing, and smishing[3] related social engineering scams – a number of all-staff emails have been sent out urging employees to be vigilant and to report any suspicious-looking emails or text messages to ICT.
- Roll-out of remote data protection training sessions via Microsoft Teams offered as refresher training to all staff as well as part of induction process for new starters – a consequence of staff largely working from home during lockdown.

2.2 Objectives for next six months

- Managing external and internal security penetration tests of council-wide systems.
- Removal of legacy systems currently in progress
- Release of Council wide Cyber Security Awareness Training for all Staff.
- Review and update of Information Asset Registers (IARs) held by each service area (it is now almost three years since the implementation of the GDPR which made it compulsory for organisations to document their information assets. There have been various changes within the Council since then, including organisational restructuring, adoption of new policies and procedures, etc. – so the Council's IARs will require updating).

3. Background Papers

None.

3. Appendices

None.

[3] **Smishing** – a form of phishing which involves the scammer attempting to trick the victim into giving them private information via a text or SMS message.