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: Caroline Reeves

Tel: 07803 204433

Email: caroline.reeves@guildford.gov.uk

Date: 26 March 2020

Data Protection and Information Security Update Report

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 to Committee:

That the update report be noted.

<u>Reason for Recommendation:</u>
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 two years since the General Data Protection Regulation (GDPR) came into force. A number of positive advances have taken place within the Council since then.

1.2 This report will cover developments in data protection and information security within the Council since the Committee considered the last annual report in March 2019.

2. Update on progress in 2019

Information Governance Successes since March 2019

- During 2019, 94% of Freedom of Information (FOI) requests were completed within the 20 working day deadline - the highest performance figure since records began.
- The Council's FOI/EIR Disclosure log has been available online for over a year - https://guildford.disclosurelog.co.uk/ - and contains details of almost 400 Freedom of Information requests. Before submitting an online FOI request via the GBC website, members of the public are now required to tick a box to confirm they have checked the Disclosure Log to see if the information they require is already available online.
- The Transparency page on the public GBC website has recently been updated to a more user friendly format.
- Deployment of body-worn cameras (following approval of Privacy Impact Assessment and information security guarantee) by Civil Enforcement Officers has been a success in catching offenders (for example bogus disabled passes) and in establishing disputed facts
- The new intake of councillors received GDPR and cybersecurity training in May 2019
- We have been promoting paperless meetings, a key benefit of which is the reduction of the risk of data breaches.

Objectives for the next 6 months:

- Information Security Classification Policy currently in progress - sets out rules around sensitivity of information, encryption and forwarding of emails, internal and external data sharing, secure disposal of both electronic and hard copy information, intellectual property issues around data ownership
- Guidance on email encryption currently being updated to reflect organisational changes following migration of Council network to Office 365 – document to be uploaded to intranet
- Remove Personal Storage Table (PST) files from GBC devices
- Continue Disclosure Log with the aim of making it as detailed and comprehensive as possible

Information Assurance Successes since March 2019

- The Council achieved Payment Card Industry Data Secure Standards (PCI DSS) compliance in November 2019 - a certification on credit/debit card payments – which facilitates electronic payments (for example parking meters, council tax collection). If an organisation is not PCI DSS compliant it cannot take electronic card payments. The Council now takes in excess of 20,000 card transactions per year.

- Mandatory training for staff who deal with card payments took place in October 2019.

- The Council is currently looking into implementing 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[1] attacks, viruses, malicious sites and spyware at source - thus making the network more secure.

- The Council has procured a Security Information Event Management (SIEM) system, which provides real time analysis of security alerts, threat mitigation and incident response

- Considerable corporate due diligence has been conducted around new software systems to ensure they are GDPR compliant and have adequate cybersecurity measures in place when transferring, collecting and storing personal information

- Mitel softphone policy and Firewall policy completed and uploaded to internal Sharepoint system

- Information Assurance Officer has carried out work in conjunction with ignite around cloud-based systems

- KPMG auditors currently conducting GBC Cyber and GDPR review

Objectives for next six months

- Managing external and internal security penetration tests of council-wide systems

- New information security policies being drafted for Council

- Removal of legacy Windows 7 PC and Windows 2008 (r2) desktops currently in progress

- The Council is currently working on the implementation of DMARC (Domain-based Message Authentication, Reporting and Conformance), a

[1] **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.

system set up to tackle email spoofing[2]. 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.

3. Background Papers

None

4. Appendices

None

[2] **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.