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: 21 April 2022

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 tenancy agreements, and 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 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 four 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 April 2021

2. Update on progress in 2021-22

2.1 Information Governance and Information Assurance Successes since April 2021

- Surrey Councils' vulnerable persons systems Data Sharing Agreement finalised (March 2022)
- Freedom of Information performance figures improved from 80% in 2020 to 92% in 2021 (See FOI report to the 20 January 2022 Committee meeting for details).
- Data Protection Policy Update - extra section added to cover electronic card payments – Payment Compliance Industry Data Security Standards (PCI-DSS compliance) - and amendments made to reflect new protocol policies around ICT usage/security) - Approved by Executive on 24 August 2021
- First post-GDPR review of 2018 Information Asset Registers (IARs) successfully completed
- Data Sharing Agreement (DSA) and Privacy Impact Assessment (PIA) between Guildford and Waverley borough councils drawn up in consultation with Data Protection, Legal and ICT officers from each council - agreed and signed off by respective Senior Information Risk Owners (SIROs) on 8 November 2021 – to ensure compliance with data protection and privacy legislation in respect of the GBC-WBC joint management strategy/Inter-Authority Agreement
- Updated Freedom of Information publication scheme approved by CMT on 28 September 2021 and now live on GBC website
- New internal data sharing form to support all employees in ensuring compliance with data protection legislation and information security considerations when personal information is being shared internally between two or more service areas within the Council has been created and uploaded to intranet (May 2021)
- Data Protection/GDPR training for councillors provided by Surrey CC successfully rolled out in June and July 2021
- Virtual cybersecurity training session for service leaders took place on 18 November 2021, delivered by National Cyber Security Centre (NCSC), with emphasis on ransomware – with aim of eventually rolling out to all staff in 2022
- Data cleansing exercise (removal of outdated files from network drives) carried out across council network
- Windows 2003 legacy servers decommissioned from council network
- Continue to provide advice and guidance to staff in relation to spoofing*, phishing**, smishing*** and other 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.

2.2 Objectives for next six months

- Managing external and internal security penetration tests of council-wide systems.
- Complete removal of legacy systems currently in progress
- Release of Council wide Cyber Security Awareness Training for all Staff

- Migration of FOI logging system from eCase to Salesforce

3. Background Papers

None.

3. Appendices

None.

Definitions

*** 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.

**** 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.

*****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.