Chichester District Council
Internal Audit

Internal Audit Summary Report

General Data Protection Regulation (GDPR)
Ann Kirk & Julie Ball
Auditors
5th March 2019

Contents

Audit: **General Data Protection Regulation (GDPR)**
Auditors: Ann Kirk & Julie Ball

If viewing on-screen, please click on the links below or use the scrolling arrows

1 Introduction 3
2 Scope 3
3 Areas for Improvement 3

4 Agreed Actions 4
5 Action Plan – Appendix 1 5

1 Introduction

1.1 Internal Audit reviewed General Data Protection Regulation (GDPR) as part of the Annual Internal Audit Plan which is approved by Corporate Governance and Audit Committee each year.

1.2 All British and European organisations including the Council had to comply with its provisions from the 25 May 2018. The purpose of the legislation is to make it 'fit for the 21st Century' in line with advances in information technology and changes to the ways in which individuals and organisations communicate and share information.

1.3 The review was undertaken in accordance with the information provided by the Information Commissioner's Office regarding how to implement GDPR.

1.4 A position statement was presented to the Corporate Governance & Audit Committee in January 2019 highlighting the areas of completion and those that were outstanding.

1.5 A report had also been presented by the Data Protection Officer (DPO) to the Corporate Governance and Audit Committee on GDPR in 25 January 2018.

2 Scope

2.1 Internal Audit reviewed the processes to provide assurance that the Council is able to demonstrate GDPR compliance. All exceptions raised in this report have already been discussed and actions agreed with the Divisional Manager Democratic Services.

3 Areas for Improvement

3.1 IT Security Policies were reviewed and updated by IT in June 2018 to bring them in line with GDPR. A further review of the policies will be undertaken by Legal Services to make improvements and to ensure there are no duplications within the policies. Staff will be informed of the revised policy when completed. Internal Audit will also review the updated policies on completion.

3.2 The policy for Data Protection held in the Council's Staff Handbook and the Intranet was put in place in May 2000 and was written by the Data Protection Officer in post at that time. Testing found that this has not been updated or reviewed since 31st January 2007. The policy needs to be brought up to date to be in line with GDPR and staff need to be made aware of the changes in order to mitigate the risk of data breaches from non-compliance with the

policy. The policy also needs to be kept up to date with any future changes to the legislation.

3.3 The Council has had a Retention Policy in place for a number of years. The purpose of this document is to evidence a corporate policy framework to ensure particular documents are being retained and/or disposed of in the correct manner and timescale. This was last updated on 3rd July 2017 and is to be reviewed in line with the IT Security Policies.

3.4 A Register of Data has been compiled and published on the Council's website by the Data Protection Officer (DPO) as per GDPR requirements. The register shows the level of administration that is undertaken by all services for the collection, storage and processing of data. The DPO is carrying out an audit to ensure that the information provided by individual services for the Register of Data is accurate and correct. The DPO should keep a record of the results of these audits and any actions required so that they can be followed up to ensure that they have been completed.

3.5 The DPO was able to demonstrate in the main that the Council is able to show GDPR compliance in all areas and has made good progress in implementing the change in Data Protection Legislation. The DPO has followed guidelines that the Information Commissioners Office (ICO) provided prior to 25th May 2018 when carrying out compliance testing. This has been a major project and will continue to be an ongoing requirement to ensure that the Council continue to be compliant with current policies, staff training requirements, data protection audits, privacy impact assessments, maintaining the data processing register and contracts with data processors.

4 Agreed Actions

4.1 The agreed Action Plan can be seen at Appendix 1 to this report.

4.2 In order to prioritise actions required, a High, Medium and Low risk factor has been applied to identify issues raised as follows:

High – Significant areas of improvement to be addressed

Medium – Important areas of improvement to be addressed

Low – Minor areas of improvement to be addressed

5 Agreed Action Plan – Appendix 1

	Areas for Improvement	Priority	Agreed Actions	Responsible Officer	Target Date
Data Protection and policies	The Policy for Data Protection is updated and reviewed with a record of the next review date.	Medium	Yes	Divisional Manager Democratic Services.	September 2019
	Retention Policy is updated and reviewed with a record of the next review date.	Medium	Yes	Divisional Manager Democratic Service's	September 2019
Data Protection Audit & Reviews	A record of audits is completed including results and actions required and when they have been completed.	Low	Yes	Divisional Manager Democratic Services.	With immediate effect