Final Internal Audit Report
GDPR in Schools
October 2018

Distribution: Executive Director (Interim) Children, Families & Education (Final only)

Director of Education and Youth Engagement

Assurance Level	Recommendations Made	
Limited	Priority 1	0
	Priority 2	8
	Priority 3	0

Contents

Page

Executive Summary

Detailed Report

Appendices

Executive Summary

1. Introduction

1.1 The Data Protection Act 2018 came into force on 25th May 2018 and enshrined the General Data Protection Regulations (GDPR) into UK law. The purpose of this audit was to assess how well prepared Schools in the London Borough of Croydon were for these changes.

1.2 A questionnaire was sent out to schools for the Head Teachers to complete and provide supporting evidence where applicable. Our findings are based on the responses and supporting evidence provided from 16 schools; 11 primary, two secondary schools and three academies.

1.3 It should be noted that although evidence was requested for the majority of questions asked, evidence to support responses was not always provided. Audit has noted instances where a nil response was given or actions are not yet complete / noted as being in progress.

1.4 This audit was undertaken as part of the agreed Internal Audit Plan for 2018/19 based on a risk assessment. The objectives, approach and scope are contained in the Audit Terms of Reference at Appendix 1.

2. Key Issues

Priority 2 Issues
For 11 out of the 16 schools sampled, it could not be verified whether an appropriate DPA 2018 / GDPR implementation plan had been developed and was being used for tracking activities, **(Issue 1).**
A number of schools were still in the process of updating their various policies and procedures for the DPA 2018 / GDPR, **(Issue 2).**
One out of the 16 schools sampled had not yet appointed a Data Protection Officer (DPO), **(Issue 3).**
One out of 16 schools sampled did not confirm whether regular checks were being undertaken to highlight areas of non-compliance with the DPA 2018, **(Issue 4).**
Two out of 16 schools sampled were still in the process of putting an Information Asset Register into place, **(Issue 5).**
It could not be verified for five out of the 16 schools sampled whether the data security and protection procedures in place were sufficient, **(Issue 6).**
None of the 16 schools had yet fully reviewed their third party contracts to ensure compliance with the DPA 2018 (and therefore GDPR), **(Issue 8).**
Five out of 16 schools sampled were still in the process or reviewing their use 'consent' and the procedures to manage this, while the rest of the schools sampled, although stating that these had been reviewed, did not provide copies. **(Issue 7).**

3. Actions and Key Findings/Rationale

Control Area 1: Preparation for GDPR

Priority	Action Proposed by Management	Detailed Finding/Rational – Issue 1
2	Following finalisation of this report the Education and Youth Engagement Team will send a copy of this report, with names of schools redacted, to all maintained schools to remind them of their responsibilities in order that they are compliant with DPA 2018. Subsequent compliance will be checked, following agreement with the Internal Audit team, as part of the usual audit process. Schools will also be reminded of the DfE toolkit available along with the appropriate link.	A DPA 2018 / GDPR plan should be developed and used to track the activities required to comply with DPA 2018 / GDPR. The plan should include where relevant: • Development of Information Asset Register; • Development of Privacy Notice; • Data Protection Officer (DPO) role assigned; • Reviewing use of consent; • Data Protection Impact Assessments; • Relevant policies and procedures; • 3rd Party Contract Reviews; • Information Security; and • Staff communication and training. In five out of the 16 schools sampled, a GDPR plan had been developed and evidence of this was provided. Examination of the five plans received confirmed that these covered the main points identified in the list above and the plans were being used to track actions taken and to record the status of each task. In 11 out 16 schools sampled, while the schools had confirmed having a GDPR plan (of which five were following the ICO 12 Steps), copies of these plans were not provided to confirm this and as a result we are unable to confirm if these were being used to track activities' progress. Where a GDPR plan has not been developed by the schools, there is a risk of non-compliance with The DPA 2018 and thus GDPR if important tasks are not identified, targeted, tracked and implemented.

Responsible officer	Deadline
Director of Education and Youth Engagement	2 November 2018

Control Area 2: Policies and Procedures

Priority	Action Proposed by Management	Detailed Finding/Rational – Issue 2
2	Following finalisation of this report the Education and Youth Engagement Team will send a copy of this report, with names of schools redacted, to all maintained schools to remind them of their responsibilities in order that they are compliant with DPA 2018. Subsequent compliance will be checked, following agreement with the Internal Audit team, as part of the usual audit process. Schools will also be reminded of the DfE toolkit available along with the appropriate link.	The Information Security and IT Usage Policy (or equivalent) should be updated to comply with the DPA 2018 / GDPR. This should include a Retention Policy and an updated Data Protection Policy. HR Practices and Procedures should have been reviewed and brought up-to-date to include the consequences of any breaches (written warning etc.). A Data Breach Procedure should also be in place. A sample of 16 schools were asked if they had the following policies and procedures in place: Information Security and IT Usage Policy, Data Retention Policy, an HR Policy and a Data Breach Procedure. The following exceptions were identified: • Six schools reported that they were in the process of updating their Information Security and IT Usage Policies. • Eight schools reported that they were in the process of updating their Data Retention Policy. • Six schools reported that they were in the process of updating their HR policies. • Three Schools reported they were awaiting on third parties for their HR policies to be updated. • Two Schools reported that their HR policies would be reviewed in July. These two schools were. • Five Schools had reported that they were still in the process of developing their Data Breach Procedures. Where policies and procedures have not been updated in line with the DPA 2018 /GDPR, there is a risk that employees may not follow appropriate processes that support DPA 2018 / GDPR compliance which could lead to fines being imposed on the schools.

Responsible officer	Deadline
Director of Education and Youth Engagement	2 November 2018

Control Area 3: Roles and Responsibilities

Priority	Action Proposed by Management	Detailed Finding/Rational – Issue 3
2	Following finalisation of this report the Education and Youth Engagement Team will send a copy of this report, with names of schools redacted, to all maintained schools to remind them of their responsibilities in order that they are compliant with DPA 2018. Subsequent compliance will be checked, following agreement with the Internal Audit team, as part of the usual audit process. Schools will also be reminded of the DfE toolkit available along with the appropriate link.	The 'Data Protection – a toolkit for schools', under section seven details that a '*school needs to appoint a named DPO in order to prepare for GDPR coming into force*'. It was identified that for one out of the 16 schools sampled, that the school was yet to appoint a DPO at the time of audit testing in July 2018. Where a DPO is not in place, the school is at risk of receiving fines for non-compliance with the DPA 2018. There is also a risk that without a DPO a data protection culture will not be embedded within the school.

Responsible officer	Deadline
Director of Education and Youth Engagement	2 November 2018

Control Area 4: Organisational Awareness and Training

Priority	Action Proposed by Management	Detailed Finding/Rational – Issue 4
2	Compliance will be checked, following agreement with the Internal Audit team, as part of the usual audit process.	Regular Data Protection spot checks should be undertaken to ensure compliance with the DPA 2018. For one out of the 16 schools no response was provided to verify whether any checks are currently undertaken to ensure compliance with the DPA 2018 and thus identify if the School is GDPR compliant. Where regular checks are not undertaken to identify potential areas of non-compliance, there is a risk that the school is in breach of the DPA 2018 and continues to be so which can eventually lead to fines and reputational damage for the school.

Responsible officer	Deadline
Director of Education and Youth Engagement/ Internal Audit Contract Manager	Current and ongoing

Control Area 5: Data Protection, Classification and Management

Priority	Action Proposed by Management	Detailed Finding/Rational – Issue 5
2	Following finalisation of this report the Education and Youth Engagement Team will send a copy of this report, with names of schools redacted, to all maintained schools to remind them of their responsibilities in order that they are compliant with DPA 2018. Subsequent compliance will be checked, following agreement with the Internal Audit team, as part of the usual audit process. Schools will also be reminded of the DfE toolkit available along with the appropriate link.	Each School should create an 'Information Asset Register' which details the key types of data and information held by the school. Two out of the 16 schools sampled were still in the process of creating an Information Asset Register. Where an Information Asset Register is not in place, there is a risk that the school is not managing its data appropriately, which could result in non-compliance with the DPA 2018 and cause reputational damage to the school with fines imposed due to non-compliance.

Responsible officer	Deadline
Director of Education and Youth Engagement	2 November 2018

Control Area 6: Confidentiality, Integrity and Availability of Data

Priority	Action Proposed by Management	Detailed Finding/Rational – Issue 6
2	Following finalisation of this report the Education and Youth Engagement Team will send a copy of this report, with names of schools redacted, to all maintained schools to remind them of their responsibilities in order that they are compliant with DPA 2018. Subsequent compliance will be checked, following agreement with the Internal Audit team, as part of the usual audit process. Schools will also be reminded of the DfE toolkit available along with the appropriate link.	Schools are required take appropriate steps to ensure personal data is adequately protected. Examples include: • Username and password is required for users to access the system; • System prompts users to change passwords on a regular basis; • Users have access formally authorised; • Access rights for leavers are disabled; • Encryption of any device that stores the school's data; • Physical security; • Up-to-date antivirus and patching; and • Attack from the internet protection. Testing of the documentation held for a sample of 16 schools tested identified that: • In four schools, the schools had provided some detail regarding procedures in place for data security, however it could not be verified that the key areas above were covered. • One school provided no details on their current procedures for data security. Where schools have not taken adequate steps to ensure their data is appropriately protected, there is a risk of unauthorised access to data which may have implications if the schools are found to not be compliant with the DPA 2018.

Responsible officer	Deadline
Director of Education and Youth Engagement	2 November 2018

Control Area 7:Third Parties

Priority	Action Proposed by Management	Detailed Finding/Rational – Issue 7
2	Following finalisation of this report the Education and Youth Engagement Team will send a copy of this report, with names of schools redacted, to all maintained schools to remind them of their responsibilities in order that they are compliant with DPA 2018. Subsequent compliance will be checked, following agreement with the Internal Audit team, as part of the usual audit process. Schools will also be reminded of the DfE toolkit available along with the appropriate link.	Contracts with third parties should be reviewed to ensure compliance with the DPA 2018. Contracts that will need reviewing, but are not exclusive, are the following: school meal caterers, third party IT providers who host or have access to personal data, such as cloud service providers or IT helpdesks, payroll, after school clubs, alternative education (counsellors, play therapists, ASD support) etc. Any contracts that involve the use of the school's personal data (staff info, pupil info etc.) should include a data sharing agreement covering responsibilities on complying with the DPA 2018 / GDPR, keeping info secure and confidential etc. The following was identified for the 16 schools: <u>Lists of contracts currently in place</u> Two schools didn't respond. Five Schools provided the lists of their contracts held but explained they are in the process of updating information and or chasing suppliers. <u>Third party contracts reviewed in line with DPA 2018 / GDPR</u> Three schools didn't respond. All 12 remaining schools were in the process of updating their 3rd party contracts. Where schools have not reviewed their contracts with third parties, there is a risk that data shared with third parties is not handled in line with the DPA 2018

Responsible officer	Deadline
Director of Education and Youth Engagement	2 November 2018

Control Area 8:Legal Basis

Priority	Action Proposed by Management	Detailed Finding/Rational – Issue 8
2	Following finalisation of this report the Education and Youth Engagement Team will send a copy of this report, with names of schools redacted, to all maintained schools to remind them of their responsibilities in order that they are compliant with DPA 2018. Subsequent compliance will be checked, following agreement with the Internal Audit team, as part of the usual audit process. Schools will also be reminded of the DfE toolkit available along with the appropriate link.	Each school should have reviewed the use of consent and the procedures to manage that consents are in place. These include topics such as storage, periodic review, expiry and refresh. The DPA 2018 / GDPR strengthens the rules regarding how to get and record consent. Each school should make it completely clear what individuals are consenting to, their consent must be unambiguous (positively opting-in) and they must be made them aware they can withdraw their consent at any time. Testing of 16 schools identified that: ▪ For five schools, the use of consent and the procedures to manage these was still under review and partly completed. Only photo consent forms were evidenced (the five schools were identified as not having up to date GDPR policies in place yet, which we would expect to include this information). ▪ For the remainder of the schools the robustness of the processes in place could not be verified, due to lack of details/evidence being provided. Where the schools have not established how they will manage consent, data subjects could subsequently challenge whether consent was provided, what this included and if the School does not have records to support their processing a Data Protection breach would occur.

Responsible officer	Deadline
Director of Education and Youth Engagement	2 November 2018

Appendix 1

INTERNAL AUDIT TERMS OF REFERENCE

GDPR in Schools

1. INTRODUCTION

1.1 The law relating to data protection is going to change on 25 May 2018, with the Data Protection Act 2018 (and the General Data Protection Regulation (GDPR)) replacing the Data Protection Act 1998. This regulates the way in which Schools handle personal data. Although many of the principles will remain the same as the DPA 1998, there will be some important changes which will affect schools.

1.2 In general terms, the GDPR places more emphasis on transparency, accountability and record keeping and will introduce a number of changes that will affect Schools.

1.3 It is important that personal data is handled correctly as the Information Commissioner's Office (ICO), can issue fines to organisations who breach GDPR (up to €20 million or 4% of annual turnover, whichever is higher).

1.4 The purpose of this audit is to assess how well prepared Schools in the London Borough of Croydon are for these changes.

2. OBJECTIVES AND METHOD

2.1 The overall audit objective is to provide an objective independent opinion on the adequacy and effectiveness of controls / processes.

2.2 The audit will for each controls / process being considered:

- Walkthrough the processes to consider the key controls;
- Conduct sample testing of the identified key controls, and
- Report on these accordingly.

3. SCOPE

3.1 This audit examined the School's arrangements in preparing for GDPR and included the following areas (and number of recommendations made):

Control Areas/Risks	Recommendations Made		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Preparation for GDPR	0	1	0
Policies and Procedures	0	1	0
Roles and Responsibilities	0	1	0
Organisational Awareness and Training	0	1	0
Data Documentation, Classification and Management	0	1	0
Confidentiality, Integrity and Availability of Data	0	1	0

Third Parties	0	1	0
Legal Basis / Consents;	0	1	0
Total	**0**	**8**	**0**

Appendix 2

DEFINITIONS FOR AUDIT OPINIONS AND RECOMMENDATIONS

In order to assist management in using our reports:

We categorise our **audit assurance opinion** according to our overall assessment of the risk management system, effectiveness of the controls in place and the level of compliance with these controls and the action being taken to remedy significant findings or weaknesses.

	Full Assurance	There is a sound system of control designed to achieve the system objectives and the controls are consistently applied.
	Substantial Assurance	While there is basically a sound system of control to achieve the system objectives, there are weaknesses in the design or level of non-compliance which may put this achievement at risk.
	Limited Assurance	There are significant weaknesses in key areas of system controls and/or non-compliance that puts achieving the system objectives at risk.
	No Assurance	Controls are non-existent or weak and/or there are high levels of non-compliance, leaving the system open to the high risk of error or abuse which could result in financial loss and/or reputational damage.

Priorities assigned to recommendations are based on the following criteria:

Priority 1 (High)	Fundamental control weaknesses that require the immediate attention of management to mitigate significant exposure to risk.
Priority 2 (Medium)	Control weakness that represent an exposure to risk and require timely action.
Priority 3 (Low)	Although control weaknesses are considered to be relatively minor and low risk, action to address still provides an opportunity for improvement. May also apply to areas considered to be of best practice.

Appendix 3

STATEMENT OF RESPONSIBILITY

We take responsibility to the London Borough of Croydon for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

Registered office: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom.
Registered in England and Wales No 0C308299.