

Official Departmental Response to the 2020 ICO Audit of the DfE

The department is rightly always under scrutiny about how it processes children's data, especially in the National Pupil Database (NPD).

On 19 December 2019 The Information Commissioner's Office (ICO) issued an assessment notice due to the risks associated with the volume and types of personal data processed within the National Pupil Database, as well as the ages of the individuals whose data is processed.

The Commissioner decided that a wide-ranging audit of the department would be the best approach to help us identify how we can improve our data protection processes. This would allow the Commissioner to fully understand the risks associated with the data processed and implications for the individual rights of our data subjects.

The DfE agreed to extend the scope of the audit to include the sharing of data contained within the Learning Records Service (LRS) database to assist an ICO investigation following a reported data breach.

The audit field work was undertaken at DfE Offices in London, Coventry, and Sheffield between 24 February and 4 March.

The purpose of the audit was to provide the Commissioner with an assurance of the extent to which DfE, within the scope of the audit, is complying with data protection legislation.

Whilst the department accepts the findings in the report, we also acknowledge that the challenges with resources, training, and recording personal data processes are faced across the public sector. However, the audit sets out a gold standard in data protection that we are aiming for.

The ICO identified that there are some cultural issues that the Data Protection Officer (DPO) faced, these included:

- The lack of importance placed on data protection in the development of policy and ways of working. It was felt that this was reflected by the lack of resourcing afforded to the DPO and the impact this has had on what is achievable.

- The light touch approaches the department has taken when providing advice and guidance on data protection matters.

Moves to address these issues have included the provision of sufficient resources to the DPO to enable a much more proactive approach. This has benefitted many of the COVID workstreams the DPO's team have been engaged in, allowing them to work much more closely with both schools and teams within the department. As the DPO office grows in maturity, so will the provision of the full range of data protection services including compliance and training.

Prior to the audit taking place we initiated an ambitious reform of the organisational structure relative to data protection functions. This was supported by the additional resources provided to the DPO office which was also relocated to within the Chief Data Officer's (CDO) Data Directorate. The Privacy and Information Rights Advisory Service (PIRAS) was brought into the DPO office. The legislative requirement for the DPO to inform and advise the controller is clearly defined within this structure with the Permanent Secretary regularly briefed with clear lines of communication in situ.

The DPO has led a programme to develop a comprehensive framework of data protection policies. This refresh will see an overarching Data Protection Policy incorporating a comprehensive set of supporting policies. Information Security policies are also under review and stakeholder engagement is advanced. The policy framework ties in with developments across other areas in the department, notably information security but also knowledge information management, commercial, and data operations. A full review of live contracts is also underway to ensure GDPR compliance.

To ensure consistency across the various work strands there is close alignment between the information security and data protection teams. The creation of strong governance frameworks is being co-ordinated within the work being done to address the report recommendations. This, along with the structural changes that have been implemented, has addressed the cultural barriers identified by the ICO auditors during their visit. The close collaboration of many teams across the department is being reflected in the work carried out to meet the ICO recommendations.

The 'light touch' approach that has traditionally been the approach the department has taken when providing advice and guidance on data protection matters has been

discontinued. With additional resources and working in a collaborative environment the DPO is now much more proactive. This has benefitted many of the COVID-19 workstreams the DPO team have been engaged in, allowing them to work much more closely with both schools and teams across the department. The DPO team supported Department of Health and Social Care colleagues and schools in a range of COVID-19 testing pilots, working closely with the ICO to enable progress toward a wider roll out of the programme.

The ICO raised concerns around privacy notices and data sharing that the DPO has worked very closely with colleagues from ESFA and Data Directorate to address through the development of a data sharing policy and data sharing strategy. Building on lessons learned during the early period of the COVID-19 pandemic, steps have been taken to improve how we share privacy information with schools as well as simplifying the information they pass on to parents about what we in the DfE do with their data. A key strand of this work will be to make the service efficient and user-centred and the DPO began to implement improved ways of talking to parents about how we process their data in response to COVID-19 by changing the format of privacy notices to a question-and-answer configuration. This was exemplified in the free school meals voucher scheme. The changes have been welcomed by schools and a review of all our privacy notices is being undertaken.

The review into all personal data processing activities within the department is well under way and nearing completion. We are conducting a full audit across the department to identify what personal data we use and that we are using it legally. Additional work is also taking place to address ICO concerns around information risk. The DPO and Knowledge and Information Management (KIM) teams are engaging with colleagues across the department to fulfil these important obligations. We are also using the information from the review to support work on the COVID-19 response. This information was further utilised by the DPO team when working with respective policy teams to ensure the continued processing of personal data should an adequacy agreement not be in place as part of the UK exit from the EU.

To support these activities more training and awareness will be delivered to those with information governance, data protection, records management, risk management, data sharing, information security, and individual rights

responsibilities. The DPO team are working toward the completion of formal qualifications and this has also been rolled out to colleagues in strategically key positions. Bespoke training is in development, blending with the comprehensive training offer developed by KIM, and this will be rolled out with compulsory elements and on demand offers. It is our aim to deliver gold standard data protection by design throughout the department.

The DPO continues to work with the ICO to deliver against the recommendations identified within the audit report. The department is committed to this programme of work and will publish a further update in June 2021.