Department
for Education

Data Protection ICO Audit Closure Summary

Version 1

Data Protection Office, Data Directorate

October 2023

Contents

ICO audit response

The ICO undertook an audit in February and March 2020. The Department for Education (DfE) extended the scope of the audit to include the sharing of data contained within the Learning Records Service (LRS) database. This was to assist an ICO investigation following a reported data breach.

The scope of the audit covered the following key control areas:

1. Governance & Accountability
2. Individual Rights
3. Training & Awareness
4. Information Risk
5. Data Sharing
6. Records Management
7. Information Security

A summary of the recommendations for each key control area is given below.

1. Governance and accountability

ICO Audit had 38 recommendations on governance and accountability

The ICO said:

DfE has internal cultural barriers and attitudes that are preventing the DfE from implementing an effective system of information governance. DfE has no oversight of information governance, including data protection, records management, risk management, data sharing and information security.

What DfE did:

- Developed a strategic approach to decision making about data, including:
    - Creating a new data protection team, the Office of the Data Protection Officer (ODPO).
    - Developing internal reporting on data protection compliance
    - Closer working with teams managing data/information.
    - Creation of new Governance Forums (including roles and responsibilities) to ensure robust policy development, incorporation & assurance measurement.
- Developed new data frameworks, policies and standards. These are easily available to all DfE staff through a new Intranet site. Roll-out was supported by communications and training to ensure integration.
- Used the ICO spreadsheet template to create a Record of Processing Activity (RoPA).

To develop this further DfE:

- Linked the RoPA to DfE's Information Asset Register (IAR). Data is now entered through a single Intranet-based form. Users are prompted to create a RoPA entry when they have an information asset that contains personal data.
- Identification of critical data across DfE and the creation of a Central Repository to support alignment, quality, approval of access/use and assurance of data.
- Developed a self-serve data protection dashboard for use by DfE staff from April 2023. The purpose of the dashboard is to identify any DP compliance issues with the RoPA entries. The dashboard will highlight the risks and issues relating to the personal data we process. This will enable timely rectification of issues.

The impact on service users:

- Linking the RoPA to the IAR means Information Asset Owners (IAOs) can update their records in one place, making it is easy for IAOs to record their processing activities. It also enables ODPO to identify and follow up in a timely way any gaps in our RoPA.

Next Steps:

- Implement improvements to the internal audit process for assessing DP compliance.
- DfE are reviewing our privacy information to improve usability and ensure the information is user/child-friendly and suitable for all DfE's audiences/stakeholders.
- Alignment of data governance activity across various teams and portfolio areas with proactive, rather than reactive, engagement.

2. Information rights

ICO Audit had 13 recommendations on Information Rights

The ICO told us:

DfE has an ineffective system of managing information rights requests.

What DfE did in response:

- Created and formally trained a centralised team to actively overview/manage DfE's information rights requests as well as provide expert support and advice to DfE colleagues in responding to information rights requests.
- Created a bespoke Subject Access Request (SAR) option on our DfE Contact Us form resulting in a one stage process that makes it easier for people to raise information rights requests.
- Incorporated an information rights section into DfE's mandatory data protection training, ensuring DfE colleagues can: recognise information rights requests, understand our legal obligations, and know where to direct requests when received via channels other than the Contact Us route.

To develop this further DfE:

- Developed closer working relationships with the educational sector to ensure children's information rights and wellbeing are considered in requests that the department receives from parent/guardians.
- Actively sought user feedback to use as a basis for improvement.
- Developed quality measures to ensure decision making and responses are of a consistent standard and meet UK GDPR requirements.
- Identified and supported teams to improve their internal processes and procedures to strengthen data protection compliance.

The impact on service users:

- DfE resource and value for money saving:
    - Creation of the new information rights team working closely with the service, delivered a value for money saving of five Full Time Equivalent (FTE) staff.

    - Continually improved/streamlined information rights processes.
    - Developed a suite of tailored and plain English response templates.
- Positive feedback received from internal users about the support from the newly created team and processes:
    - "I don't know what we would do without your support".
    - "Clear, tailored, and instant responses to queries followed up with written advice. Thank you so much".
    - "New response templates make life so much easier, thank you".
    - "I feel less panicked by SARs now you have taken the helm".
- Feedback from external user:
    - "Information received was clear and what I asked for. Response was received within the required timeframe".
- 100% of responses were made on time within the prescribed timeframe of one-three calendar months, for quarter ending December 2022.

Next Steps

- Produce a Subject Access Requests Guide for use by education establishments, after user testing in Quarter 4 2023.
- Undertake percentage check of requests where responses are being made within business-as-usual processes to ensure full compliance with ICO guidance.

3. Training & Awareness

ICO Audit had 13 recommendations on training and awareness

The ICO told us:

DfE are providing very limited training to staff about information governance, data protection, records management, risk management, data sharing, information security and individual rights.

What DfE did in response:

- Created a new Data Protection Hub which provides a one stop shop for DfE staff to easily find and navigate data protection support and guidance.
- Created a specific Microsoft Teams channel and email newsletters to update DfE staff on data protection and all aspects of data/information management.
- Developed and delivered mandatory DfE specific data protection training.
- Developed additional training material covering specific aspects of data protection to ensure departmental compliance.
- Analysed training needs for different staff, e.g. data protection training for Subject Access Requests (SAR) handlers and commercial colleagues.

To develop this further DfE:

- Developed chatbots to enable DfE staff to easily access the right information. The chatbots are hosted on our intranet pages to provide a single gateway to our data protection, information management and records management.
- As the first government department to launch a data protection specific chatbot, we share updates across government to support OGDs in their consideration of adopting their own chatbot.
- Developed bespoke DPIA training for teams with plans to roll out drop-in surgeries to support teams.

The impact on service users:

- 35% of DfE staff have completed the data protection awareness training. DfE gained approval for this course to be made mandatory in September 2022, to achieve a significant increase in completion rates in 2023
- Feedback from staff about the course:
    - 79% of people were satisfied or very satisfied with the training.
    - 85% of people's expectations were met.
- All DfE staff who handle Subject Access Requests (SARs) have completed the Individual Data Rights and Subject Access Requests module. This is a voluntary module for all staff to complete and mandatory for the centralised SAR team.

Next Steps

- Develop further training modules are in development and will be launched during 2023. These will include:
    - Data Protection Contract Clauses
    - Data Protection Risks & Data Protection Impact Assessments (DPIAs)
    - Data Sharing
    - Retention of Information (in collaboration with DfE Knowledge and Information Management Team (KIM))
    - Additional bitesize videos and resources will also be available.
    - Additional guidance and provide training for all DfE staff so they are aware of their responsibilities for maintaining a Record of Processing Activities (RoPA).
- Existing training modules are under content review and will be updated as part required.
- The DfE specific data protection training module is now part of the mandatory learning programme and will be part of the annual roll out managed by HR.
- We continue to work closely with HR to make improvements to the existing training including access to new software to develop and host content.
- We continue to develop and deliver communication activity quarterly on a particular data protection theme. This ensures we are continuously raising awareness of data protection within DfE and encourage completion of available training.
- In 2023, we will start developing:
    - An Education Privacy Assurance Scheme. This will provide data protection guidance to education settings to help them make informed decisions to improve compliance with Data Protection legislation.

    - A ‘Data Protection Portal’ aimed at learners; parents/carers; and education staff. The portal will contain data protection learning & training materials, deep dives on the use of data in DfE projects, a comprehensive index of data protection information for data subjects and more. This will be hosted online for anyone to access – including DfE staff so there is a consistent understanding across DfE and the sector. We will promote is widely to the sector and DfE users.

4. Information Risk

ICO Audit had 24 recommendations on information risk

The ICO told us:

- Information risks are not managed consistently. Risks are not assessed regularly or in enough detail to provide meaningful control and monitoring.
- Data Protection Impact Assessments (DPIAs) are not being carried out at a stage of the project early enough to influence the outcome.
- Lawful basis is assigned at too high a level. Lawful basis is DfE’s legal justification for processing your personal data.

What DfE did in response:

- Introduced a new approach to engage with Information Asset Owners (IAOs) to highlight information risks relating to their information assets.
- Introduced a quarterly review of information asset risks. This enables these risks to be managed consistently and the detail kept up to date.
- Updated DfE Information Risk Management Policy to ensure that information asset risks are managed consistently.
- Updated DPIA processes, procedures, guidance and templates to make them easier to follow. Working with DfE stakeholders and across government to ensure best practice.
- Established a quarterly DPIA process review to respond to feedback, review and update guidance and amend as appropriate.
- Guidance is now held within the central DPIA portal as well as links within the DPIA documents directly.
- Introduced clearer acceptance of risks and recommendations by IAO’s to the DPIA process to encourage engagement and ownership.
- Implemented an annual DPIA review. ODPO contacts the IAO/SRO to identify if the data processing is ongoing. If data processing is:
    - Ongoing the DPIA will be reviewed and updated with any changes to the data processing, ensuring risks are identified and mitigated against.
    - If the data processing has ceased the DPIA will be closed and Record of Processing Activity (RoPA) updated.
- Reviewed the lawful basis for each processing activity.
- Developed risk management training, available for all DfE’s Central risk team.

To develop this further DfE:

- Updated the Legitimate Interest Assessment (LIA) process and templates

The impact on service users:

- By engaging with stakeholders and actively seeking feedback users have confirmed the process and guidance is far more straightforward and easier to engage with. Any gaps or clarifications are responded to and incorporated into the quarterly process review.
- Users have reported that the Confidentiality / Integrity / Availability (CIA) method of recording risks is confusing.
- We have strengthened our signposting and guidance to DfE Risk Management and the Risk Management Framework, making it easier to manage risks.

Next Steps

- Continue to report performance for compliance with data protection requirements up to board level. To ensure that risks and issues are visible and can be addressed in a timely way.
- Improve the DPIA processes based on user feedback to ensure DPIA and RoPA processes are aligned.

5. Data Sharing

ICO Audit had 26 recommendations on data sharing

The ICO told us:

- The Data Sharing Approvals Panel (DSAP) has limited oversight and consistency around how data is shared externally.
- There is no requirement for a DPIA to be carried out for all sharing applications.
- There is an over reliance on using public task as the lawful basis for sharing.
- There is limited understanding of the requirements of legitimate interest to assess the application and legalities of it prior to sharing taking place.
- DfE must improve transparency around the processing and access to the Learning Records Service (LRS) database.

What DfE did in response:

- A DPIA is now completed, and assessed by ODPO, for all third-party data shares.
- Implemented the new DfE (& Executive Agencies) Data Sharing Service with clearer roles and responsibilities, more effective principles, processes and procedures and a new suite of forms and guidance documents.

- The Data Sharing Service and Office of DPO work tirelessly to support each other to ensure Data Sharing Approval Panel (DSAP) is a robust, effective and transparent board.
- DfE has improved its communication through GOV.uk and now publishes all external data shares quarterly.
- DfE has significantly strengthened its relationship with the Office for National Statistics (ONS) in order to ensure the majority of all new data shares are via the ONS Secure Research Service under their Five Safes framework.
- DfE implemented the onward sharing of the Longitudinal Education Outcomes (LEO) with researchers through ONS SRS using the Digital Economy Act and will continue to build on this secure method of data sharing for other DfE data assets.
- As part of the new Data Sharing Service, DfE overhauled its Data Sharing Agreement (DSA) templates, its Application Forms and its Data Protection Impact Assessment (DPIA) for third party requests (including new questions around lawful basis and legitimate interests).
- Reviewed the data collected in LRS to ensure all fields were aligned to a lawful basis, removing fields and the underlying data where it was deemed not required.
- Reviewed and updated the retention period for LRS data.
- Implemented new security and access control measures for LRS.

To develop this further DfE:

- The Find and Explore tool provides a public-facing transparency tool for anyone wishing to know what the department holds on their children. It focuses on data we hold on the NPD. This is used in the DfE Personal Information Charter, the newly published NPD Privacy Notice and for many Subject Access Requests.

The impact on service users:

- The new Data Sharing Service and more effective DSAP has been widely welcomed across the research community and is now used across government as a model of good practice in its Data Sharing Governance Framework.

Next Steps

- DfE is continually improving the service to support its users in accordance with UK GDPR

6. Records Management

ICO Audit had 10 recommendations on records management

The ICO told us:

The DfE Knowledge and Information Management Team (KIM) have no active involvement with the National Pupil Database (NPD). This means there has been no expert involvement in developing procedures for the creation, storage and retention of records.

What DfE did in response:

Reviewed the National Pupil Database (NPD) retention period. This has led to an updated NPD weeding policy and NPD retention policy.

To develop this further DfE:

- Reviewed all retention periods of our data collections.
- Published an updated privacy notice for the NPD on gov.uk.
- Published its data protection policy on gov.uk in quarter 3 of 2023

The impact on service users:

- The new ways of working between Knowledge and Information Management Team (KIM) and National Pupil Database (NPD) teams will ensure full oversight of all data retention policies.
- The NPD retention policy will be published online alongside the NPD privacy notice ensuring transparency for both internal and external users of NPD data, along with data subjects.

Next Steps

- To improve transparency on data retention, DfE will publish its records management policy and retention and disposal schedule in quarter 4 of 2023.
- DfE is currently reviewing the retention of back-up data to ensure it meets legal requirements.
- DfE is instigating review periods for all Privacy Notices of between 6 months and one year

7. Information Security

ICO Audit had 14 recommendations on information security

The ICO told us:

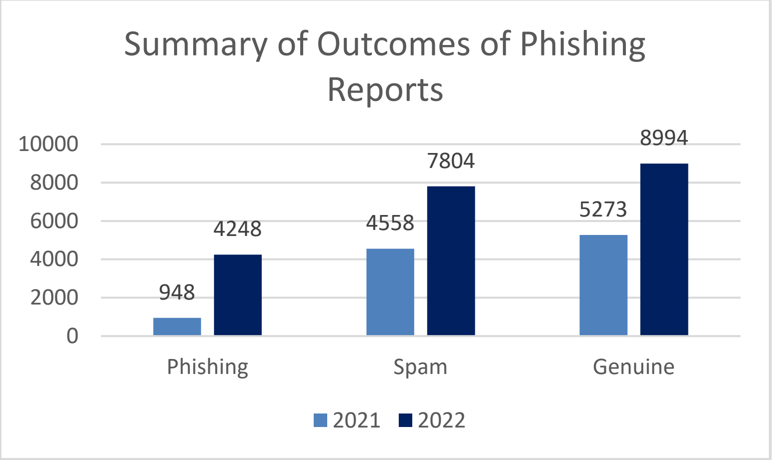
- DfE should review all internal security procedures to identify any additional preventative measures that can be implemented.
- DfE has no oversight of information security and is providing very limited training to staff about information security.

What DfE did in response:

- Formalised the information security policies so that they are in an Information Security Management System on the DfE Intranet.
- Updated processes around access to the Learning Records Service (LRS) system, including the Awarding Organisations Agreement and LRS User agreement.
- Developed mandatory security training for all staff which is delivered via a new training portal. In 2021-22, 5809 hours of training were completed by staff on the cyber security and data protection training modules.
    - 20 foundation and advanced learning campaigns to improve staff security awareness and security knowledge.
    - Cyber security awareness proficiency assessment (SAPA) carried out with a random sample of 2000 users. This showed that DfE staff had an above average knowledge of security topics against comparable industry data in all 7 assessment criteria. This represents a 0.5% increase over the figure achieved in the same exercise conducted in 2021.
    - Annual Benchmarking campaign carried out for LocatED & IfATE staff.
    - Specific campaigns targeting non-compliant staff i.e. non-reporters, never signed in.
    - Office for Children's Commissioner targeted phishing campaign organised.
    - Psychological variant phishing campaigns introduced to target specific behaviours including need & greed; scarcity & limited edition; authority & officials; likes; and reciprocity.
    - Pre & Post Induction training phishing campaigns to compare staff knowledge and performance before and after their initial induction training.
- Cyber Security Escape Room education event rolled out across 5 DfE sites to 70 teams comprising 266 staff during October Cyber Security Awareness month.

To develop this further DfE:

- Introduced a one click reporting button so staff can quickly report email staff suspect are phishing.
- Installed auto email analysis and triage software so we can respond automatically and train staff on what emails are spam and phishing.
- The chart below shows the outcome of phishing alerts in 2020 and 2022. This is a significant increase from 450 reports in 2019.



- Introduced a new form for reporting security incidents, making it easier for DfE staff to report incidents.
- Ensure activity on LRS accounts is monitored routinely and inactive accounts removed.

The impact on service users:

The new ‘phishing’ App allows us to identify staff that need specific training, if they don’t identify some of the test phishing emails.

Next Steps

In 2023/24, DfE will deliver:

- Pre & Post Induction training phishing campaigns to compare staff knowledge and performance before and after their initial induction training.
- Tailored behaviour change campaigns to all staff targeting our prioritised Cyber & Information security risks.
- Behaviour Bootcamps to all DfE sites, to educate staff and psychologically strengthen them against attacks.
- Quarterly campaign targeting senior leadership, educating on specific threats to them, how to protect themselves and how to support development of a positive security culture in the department.

ICO reprimand – in response to the investigation into a data breach for the Learner Records Service

ICO reprimand had 5 recommendations

The ICO told us:

- Improve transparency on processing on the Learning Record Service (LRS).
- DfE should continue to review all internal security procedures on a regular basis to identify any additional preventative measures that can be implemented.

- DfE should ensure all relevant staff are made aware of any changes to processes as a result of this incident, by effective communication and by providing clear guidance.
- DfE should complete a thorough and detailed Data Protection Impact Assessment (DPIA), which adequately assesses the risk posed by that processing.
- DfE should continue to ensure sufficient data protection training is provided to all staff.

What DfE did in response:

- Updated processes around access to the Learning Records Service (LRS) system, including a more robust application process and better in-application audit processes to monitor usage of the service and remove users when required.
- Safeguards have been put in place to strengthen the controls around legitimate access to the LRS system.
- The LRS DPIA was thoroughly refreshed and updated.
- An updated, clearer, privacy notice for the LRS was published.
- Staff involved with the operation of the LRS have been thoroughly briefed and made aware of the specific changes made as a result of the incident.
- DfE has implemented data protection training for all staff.

To develop this further DfE:

- Ensured activity on LRS accounts is monitored routinely and inactive accounts removed.
- Removed fields and data no longer required from LRS.
- DfE has introduced privacy notices focussed on data subjects, e.g. privacy notices for learners in Early Years Foundation Stage and Key Stages 1-3 and for learners in Key Stages 4-5/adult.

The impact on service users:

- We have identified where there are non-compliant behaviours and resolved them.
- Undertaken lessons learned to improve the process for DfE and for users.

Next Steps

- To improve transparency, DfE is reviewing our privacy information to improve usability and ensure they are user/child friendly.
- Work continues across the DfE to further develop and enhance the LRS, including looking at ways of putting data subjects more in control of their data through the use of the new system, Titan.

Department
for Education

About this publication:

enquiries www.education.gov.uk/contactus
download www.gov.uk/government/publications

Follow us on Twitter:
@educationgovuk

Like us on Facebook:
facebook.com/educationgovuk