Findings from the ICO's consensual audits of 11 multi academy trusts

September 2018 to October 2019

Information Commissioner's Office

Table of contents

Introduction..3
Approach..3
Typical processing of personal data by MATs....................................3
Scope areas...4
Areas of good practice..4
Areas for improvement...5
Governance and accountability...5
Training and awareness..12
Data sharing..16
Resources...20

Introduction

The Information Commissioner's Office (the ICO) enforces and promotes compliance with the Data Protection Act 2018 (the DPA) and the General Data Protection Regulations 2018 (GDPR), which contains seven principles of good information handling.

Approach

The ICO carried out a programme of audits at multi academy trusts (MATs). This was to better understand how MATs process personal data and how this processing linked into the rights of the individual under the DPA and GDPR, as well as new provisions for children.

11 MATs participated in consensual audits. The MATs ranged in size and included nursery classes and pre-schools up to sixth form and post-16 education. In total the MATs audited have around 200,000 pupils. We conducted audits via telephone interviews and onsite visits between September 2018 and October 2019.

This report is based on these audits. It highlights our experience of governance and accountability, training and awareness and data sharing at these MATs. It is intended to help them and others in the sector to recognise where they can make improvements in these areas. No individual organisations are named in this report.

Typical processing of personal data by MATs

MATs process both paper and electronic records relating to pupils, parents and staff. The main lawful basis used for the processing of personal data is 'public task' for the delivery of pupil education.

The MATs involved process a significant amount of special category personal data, including data related to special educational needs, safeguarding of children, medical conditions of pupils and staff records.

Personal information is either held electronically in computer databases or manually in filing cabinets.

Scope areas

When conducting these audits, we made an assessment of the controls the 11 MATs had in place for three relevant scope areas and how effective those arrangements were. Where we identified information risks, we made recommendations to mitigate these and improve assurance against specific controls.

The relevant scope areas were:

- **Governance and accountability** – information governance accountability, policies and procedures, performance measurement controls and reporting mechanisms to monitor data protection compliance are in place and in operation throughout the organisation;
- **Training and awareness** - the provision and monitoring of staff data protection, records management, information security training and the awareness of data protection regulation requirements relating to their roles and responsibilities; and,
- **Data sharing** - the design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.

The examples identified within this report were not always consistent across all of the organisations we spoke to; however, they were evidenced in at least one participating MAT.

Areas of good practice

The audits identified a number of areas of good practice.

✓ 81% had a data protection officer (DPO) in place with designated responsibilities for data protection compliance.

✓ In 72% of cases the DPO had appropriate reporting mechanisms in place to senior management.

✓ 90% had an information governance steering group or equivalent in place, which was responsible for providing the general oversight for information governance and data protection compliance activity within the organisation.

- ✓ 81% have made their policies and procedures available to staff on the organisation's intranet site.

- ✓ 90% produced weekly or monthly bulletins or newsletters to help disseminate and inform staff of new information governance policies and subsequent updates.

- ✓ 81% had produced guidelines, posters or publications to promote awareness of staff responsibilities toward data protection compliance.

- ✓ 90% maintained records of when and how consent was obtained from individuals.

- ✓ In 90% of cases, awareness was raised across the organisation for information governance, data protection, information security and the associated policies or procedures using various media, including emails, team briefs, team meetings, posters and handouts on a regular basis.

- ✓ 100% of staff interviewed across all MATs were aware of who to contact within the organisation for any information governance related queries or advice. This would usually be the nominated data protection champion in the academy or the DPO.

Areas for improvement

Governance and accountability:

There were a number of areas where we felt that MATs should implement improvements to their governance and accountability.

Management structures and policies

- ✗ Over 70% of MATs had not clearly defined and documented operational roles and responsibilities for the day-to-day management of records management, information security and data sharing at Trust and academy level within data protection policies and relevant job descriptions. In some cases, these roles had not been assigned to appropriate staff.

- ✗ 36% had an inadequate overarching policy framework. An information governance policy framework should incorporate policies for data protection, information security, records management and data sharing. The information governance framework should also be endorsed at board level and approval recorded in the document control area of the policy and within relevant meeting minutes. For further details see our guidance on accountability and governance.

- ✘ 18% had no formal sign-off process or contractual requirements to support the fact that employees should read and be aware of information governance policies and their responsibilities. In a further 36% of MATs, the sign-off process and contractual requirements were ineffective. For example, formal checks were not made to ensure that staff have read policies. We also found that the sign-off process was practiced on an informal basis at academy level, but it was not mandatory across the Trust.

- ✘ In 63% of MATs, information risks were not sufficiently managed throughout the organisation. For example, there was no specific information risk register in place identifying the key information risks (at both academy and Trust level) and no assigned risk or information asset owners. In some cases, there was no documented process outlining how information risks should be identified, assessed, treated and escalated to relevant governance groups and corporate risk registers.

Good practice case study - information risk management

An established and effective information risk management framework should be in place. In one MAT, we observed that information risk registers were in place, which provided a detailed breakdown of all the risks across the organisation at both academy and Trust level, and recorded any mitigating controls or safeguards in place. Risks had been assigned a rating based on likelihood and the impact. Responsibilities for reviewing and managing risks were allocated to named risk owners at academy level and Trust departmental level. Overall responsibility for risk was assigned to a senior information risk owner (SIRO) who sat on the Board and Information Governance Steering Group. High level risks were escalated to the SIRO and DPO by the local risk owners. Both local and Trust level risk registers were managed by the Information Governance Steering Group and any risks identified on the breach log or during internal audits fed into the risk registers.

Data Processors

- ✘ At 54% of MATs we found that data processor contracts did not include:
  - all the compulsory details and terms as outlined under Article 28 of the GDPR; and,
  - the technical and organisational security measures the data processor would adopt (including encryption, pseudonymisation, resilience of processing systems and backing up personal data in order to be able to reinstate the system) outlined under Article 28(3)(c) and Article 32 of the GDPR. For details see our guidance on contracts and what needs to be included in the contract.

- ✘ 72% did not have suitable procedures in place with all processors to ensure GDPR obligations in relation to:
  - the notification of personal data breaches,
  - complying with the rights of individuals; and,
  - data protection impact assessments (DPIAs) were met.

- ✘ The majority of the MATS did not complete sufficient periodic checks or audits on processors to provide assurances that:
  - data processors have procedures in place to comply with their specific legal obligations outlined under the GDPR (90%). This could include data breach notification, complying with or assisting with data subject requests and DPIAs;
  - data processor staff have completed information governance training, and that their staff were aware of and understood data protection policies and procedures (81%); and,
  - data processor data security arrangements were effective and complied with contractual agreements (81%).

- ✘ 36% carried out initial checks on data processors when entering into a contract but failed to carry out periodic checks or audits to ensure continued assurance. For further details see our guidance on responsibilities and liabilities of controllers

Good practice case study – compliance checks on data processors

It is important that organisations carry out checks on their data processors. One Trust had conducted an onsite audit with their IT providers to ensure that the processor had appropriate security safeguards in place and were adhering to contractual requirements in relation to data protection. The Trust IT Manager checked areas such as physical security, network security, information security, business continuity, compliance with the DPA and GDPR and contractual obligations.

Compliance and assurance

- ✘ Only 54% of MATs had an effective programme of risk-based internal audit in place covering information governance and data protection. Audits are an important tool in assessing, improving and providing assurances that the organisation's policies, procedures and safeguards are working in practice and is an important part of the accountability principle.

- ✘ A significant number of MATs had not carried out compliance checks or audits:

  - on manual and electronic files to assess adequacy and accuracy of records (54%) to ensure compliance with the data minimisation principle and accuracy principle; and,

  - to test staff awareness and understanding of data protection policies and procedures (72%).

- ✘ 36% carried out ad-hoc checks on records accuracy, staff awareness and information security (walk arounds, clear desk checks, records and equipment storage) but failed to carry out checks on a periodic basis, record the findings and report on them to information governance steering groups. Recording checks is important for evidencing compliance with the 'accountability principle'.

- ✘ 27% had no central action plan in place for data protection, information security and records management related audits. A further 27% of MATs' action plans did not record expected information such as owners, dates of follow up and completion or details of progress made.

- A large proportion of MATs either had no or limited key performance indicators (KPIs) in place to measure organisational performance on:
    - subject access request (SAR) performance, covering volume of requests and percentage completed within statutory timescales, complaints from the ICO and individuals (54%);
    - mandatory training covering data protection and information governance related topics (72%);
    - number of security breaches, incidents, near misses and results of security spot checks such as clear desk sweeps (45%); and,
    - records management, including file retrieval statistics, adherence to disposal schedules and the performance of systems in place to index and track paper files containing personal data (90%).
- 72% were found to have either no or limited assurance that performance to information governance or data protection KPIs was reported and reviewed regularly at senior management or board level. This means that there was no high-level view of organisational performance and compliance with data protection and information rights legislation.

Lawful basis for processing personal data

- 45% had not completed or had only partially completed an information flow mapping exercise to identify the various types of processing being carried out.

- 54% did not have internal records of all processing activities in line with the requirements set out in Article 30 of the GDPR. See our guidance on documentation and documentation template for controllers.

- 54% had not adequately identified and documented the lawful basis for processing personal data (from Article 6 of the GDPR) and additional lawful basis for special categories of personal data (Article 9 of the GDPR). For further details see our guidance on lawful basis, the lawful basis interactive tool, lawful basis resources and what do we need to consider when choosing a lawful basis for processing children's personal data?

- ✘ 63% of MATs failed to explain the lawful basis for processing personal data and special category data in their privacy information. They often failed to clearly explain which lawful basis applied to each processing activity and identify the type of personal data collected, shared or used in the activity. See our guidance on the right to be informed.

- ✘ In two MATs, we found that one-off surveys and collections of personal data were conducted, however privacy information used vague and high-level statements when explaining the purpose of the processing, e.g. to gain an understanding of the 'learner experience'. Privacy information should be provided in clear and granular fashion to explain to individuals what the data will be used for (Articles 12 and 13 of the GDPR). This is particularly important where processing may involve automated decision making, including profiling (Article 22 of the GDPR).

- ✘ Only 54% of MATs ensured that consents were regularly reviewed to check that the relationship, the processing and the purposes have not changed and there were processes in place to refresh consent at appropriate intervals. For further information see our guidance on What is valid consent.

- ✘ 36% did not adequately publicise (in privacy information) or explain how individuals exercise their right to withdraw their consent at any time. See what privacy information should we provide.

- ✘ We observed on a couple of occasions that schools had stated that the age of consent to the processing of personal data was 13 years old. The general rule in the UK is you should consider whether the individual child has competence to understand and consent for themselves (the Gillick competence test). The age limit only applies to the provision of consent for online services which are provided directly to children. For further details see what are the rules on children's consent?

- ✘ In at least one MAT, we noted that privacy information was too complex for a child to read and understand. Article 12 of the GDPR says that privacy information should be clear and transparent. For children, age appropriate language should be used. Other methods could involve using graphics to help children to understand why their information is collected and how it is used. Please see our guidance on the right to be informed. There is also some useful information on transparency and privacy information in our Age appropriate design: a code of practice for online services.

Data protection by design

- ✘ 72% of MATs had not documented in policy or explained what measures they had in place for data minimisation and pseudonymisation (Article 25 of the GDPR). Some organisations described a high-level approach to data minimisation and pseudonymisation but failed to provide staff with procedures on how to implement this in practice. For further information see data protection by design and default.

- ✘ 54% had not suitably integrated core privacy considerations into existing project management and risk management methodologies and policies. For example, some failed to reference when a DPIA might be required before undertaking a new project or taking on a new supplier or contractor.

- ✘ The same number again did not carry out DPIAs or failed to adequately document DPIAs with all the information required under Article 35 of the GDPR. Furthermore, they did not evidence who signed off the DPIA nor show how any residual risks identified were managed or mitigated by the organisation (as part of the risk management process). Some organisations did not have a DPIA procedure in place and did not reference DPIAs within training. For further details see our guidance on DPIAs.

- ✘ In at least one instance it was found that a DPIA had not been carried out before the introduction of a new cashless system which used pupil fingerprints (biometric data). We require a DPIA to be completed if you plan to process biometric data. For a list of criteria please see When do we need a DPIA?

Good practice case study - DPIAs

An effective and embedded DPIA process should be in place. One of the organisation’s procurement policy stated that either the DPO or IT Director be involved in all new IT projects, apps, projects which included the use of personal data and contractors (processors) who had access to or carried out processing of personal data. An initial assessment of information security and data protection risks was carried out by the business manager or head teachers to gauge whether a full DPIA may be required. A DPIA procedure and template form was in place which explained how to complete the DPIA.

Training and awareness:

There were a number of areas where we felt that MATs should implement improvements to their programmes of information governance training and awareness raising.

Training programmes:

- ✘ In 70% of MATs, the overall information governance information governance induction and refresher training programme did not include training for all staff on the following key areas:
    - Data protection or GDPR;
    - information security (including data breaches);
    - records management;
    - data sharing; and,
    - requests for personal data.
- ✘ Only 40% had an information governance training programme which incorporated sector-specific requirements (tailored to schools and the education sector) and which was approved by senior management. Training should include examples specific to school or Trust working environments to make it more meaningful for staff.
- ✘ In 80% of MATs, information governance training needs were not regularly assessed for all staff groups (including temporary and contract staff) who have access to or handle personal data. Training

needs should be documented within a training needs analysis and reviewed annually.

- ✘ 60% of MATs' training plans or strategies were either not documented or had not detailed how information governance training needs would be met within agreed timescales and what resources may be required to deliver training.

- ✘ 40% had either not allocated adequate resources to deliver information governance training or staff had not received appropriate training in information governance in order to deliver the training required to other staff.

- ✘ 50% had assigned responsibilities for managing and coordinating information governance training across the organisation but had not sufficiently documented these responsibilities within training or information governance policies and in job descriptions.

Induction and refresher training

- ✘ In 60% of MATs we found that information governance induction training was not completed within one month of an employee's start date and no assessment or minimum pass rate was set to ensure effective understanding of content and training. In some cases, appropriate records of training completion were not retained or followed up. In other instances, it was found that the requirement that induction training be completed within one calendar month was not documented in policy.

- ✘ 70% were found to not have delivered information governance induction training to all staff. Gaps were observed particularly in relation to temporary and contract staff. In some circumstances, whilst induction training was mandatory for all staff, this requirement had not been documented in policy or enforced in practice.

- ✘ In 50% of induction training and 40% of refresher training, the training material was not reviewed on an annual basis to ensure it remained up to date with current legislative requirements and reflected current information governance practice within the organisation. Training content should also be updated to include key lessons learned from data breaches and near misses.

- ✗ Only 50% of MATs had induction training which was written by the DPO, or content which was approved and overseen by the DPO. The responsibility for writing or approving training content should be documented in policy and job descriptions. Training content should also be approved by an information governance steering group or equivalent, and any approvals should be recorded in any relevant information governance steering group minutes.

- ✗ 90% had either not provided refresher information governance training to staff or did not have documented plans in place to refresh training on an annual basis.

- ✗ In 50% of cases we found that there was insufficient provision of alternative information governance training to staff who may not have access to online training (e.g. facilities staff and catering staff). Alternatives could include training videos, face to face training and briefings. Training content should be role appropriate and reflect the nature of the personal data they have access to, handle or process. For example, catering staff may handle special category data in the form of health-related personal data (food allergies and other health conditions).

- ✗ In 20% of cases, refresher training was not delivered to all staff (including temporary and contract staff). In a further 30% of cases, we found that that policies did not reference the fact that refresher information governance training was mandatory for all staff and did not document or implement a timescale in which training must be completed.

Good practice case study - training provided to temporary and contract staff

Organisations should satisfy themselves that temporary and contract staff have been provided with an adequate level of information governance training. Temporary and contract staff should also be aware of the organisation’s key data protection procedures before being allowed to access or process personal data. One method of ensuring this is to provide the training to temporary or contract staff directly. At one organisation we observed that a training video was provided to contractors and supply teachers. This provided assurance that these staff have had an adequate level of data protection training and were aware of the organisation’s key information governance policies and procedures.

Specialist training

- ✘ Just under a third of MATs had not delivered enhanced or specialist training to identified staff, based on job role requirements. For example, this could include the DPO, data champions, business managers, head teachers or staff who may be required to deal with data breaches, subject access requests, data protection impact assessments or data sharing.

- ✘ In 30% of cases, specialised training content was not written by, approved or overseen by the DPO, Information Governance Manager or equivalent. Some MATs did not have an assessment and minimum pass rate to ensure understanding of content and delivery of the specialist training was effective.

Follow up and reporting

- ✘ 30% of MATs had not clearly allocated or documented the responsibility for training follow-up, and in some cases, the follow-up process had not been documented.

- ✘ 50% had not provided sufficient assurances that staff at all levels across the Trust who had not attended information governance training were identified and required to complete it. In some instances, MATs were found to not have adequate mechanisms in place to identify untrained staff. Where training follow-up procedures were in place, they did not include a timeframe in which training should be completed once a reminder has been sent and the consequences for staff in not completing the training (unless there was good reason).

- ✘ In 40% of MATs we found that information governance training completion reports were not reported to and reviewed by appropriate steering groups and to senior management.

- ✘ 40% did not monitor information governance or data protection related training objectives as part of the annual appraisal process. The same number again did not provide staff with adequate feedback mechanisms on information governance training content and methods of delivery.

Good Practice case study - training reports and follow ups

Staff training completion should be monitored and followed up. One MAT had a training system in place which provided visibility of staff training completion across the organisation. Staff which had not completed training were chased up via Data Champions in each school. The DPO sent regular reports to Data Champions and training completion statistics to members of the Information Governance Steering Group. Training completion statistics was a standing agenda item of the Information Governance Steering Group. Training completion was discussed at the weekly senior management meetings at academy level.

Data sharing:

There were a number of areas where we felt that MATs should implement improvements to their programmes of data sharing in relation to controller to controller sharing of personal data.

Fair processing information

- ✘ Around half of MATs had not clearly documented in privacy information the purpose of the data sharing and the legal basis. There were also some inconsistencies in the privacy notices relating to the lawful basis. For example, one MAT's privacy information stated that data was shared under legal obligation, but in another section said that sharing was on the basis of consent. There is an ICO Draft Data Sharing Code of Practice (closed to public consultation in September 2019). A finalised version of the Data Sharing Code of Practice will be published in due course. Also see our data sharing and subject access checklist.

Informed decision making

- ✘ 70% of MATs had not maintained an adequate record or log of all data sharing decisions for audit, monitoring and investigation purposes. In some instances, there was no documented process detailing how data sharing decisions should be managed and recorded.

- ✘ In 60% of MATs we found that policies, procedures and guidance did not clearly set out who had the authority to make decisions about systematic sharing or one-off disclosures, and when it was appropriate to do so.

- ✘ In 80% of cases, generic and role-based data sharing training needs were not adequately identified and documented on a training needs analysis. It was commonly found that training provided to staff in sharing information was not sufficient, as it only provided an overview and did not cover data sharing in any detail.

Assessing legality, risks and benefits (DPIA)

- ✘ 70% of MATs had not documented their approach to applying exemptions from the non-disclosure provisions within data protection legislation in relation to data sharing. Staff should be provided with guidance on common exemptions and when these should be used. A record on any exemptions cited when disclosing information should be recorded on a data sharing log or the data subject's record. For further details see our guidance on exemptions.

- ✘ 70% had not carried out or documented a data protection impact assessment (DPIA) in respect of data sharing decisions. DPIAs help organisations decide whether to proceed with sharing personal data, to consider the risks involved and how data can be securely shared (minimising personal data where possible and considering if anonymised data can be used instead). For further details see our guidance on DPIAs.

Information sharing agreements and logs

- ✘ 40% of MATs did not have any high-level data sharing agreements (DSAs) in place which set out the common rules to be followed by all data sharing partners.

- ✘ In 30% of MATs we found that statements of compliance or DSAs were not signed by the senior management of each organisation, committing them to comply with the terms of the agreement.

- ✘ In 60% of cases there was no review process in place to ensure partner organisations were removed from or added to agreements when required, and to regularly examine the working of the agreement. There was also no supporting review checklist or procedure.

- ✘ 60% had no supporting procedures or guidance in place for operational staff detailing the DSAs with each organisation.

- ✘ 50% had no central log of DSAs. In a further 40%, data sharing logs had not provided enough details such as the nature of the sharing, the lawful basis, the partners, details of sign off and review.

Data quality and retention

- ✘ 50% of MATs did not have detailed common retention and disposal arrangements in place between data sharing partner organisations. Details should be documented in the DSA and on each organisation’s retention schedule and supporting procedures.

- ✘ 60% had not ensured that they had procedures in place to explain to staff to only share agreed information (authorised by DSAs or by appropriate managers), how to redact information (which shouldn’t be disclosed) and how to clearly explain when sharing information what is factual and what is opinion. For further details see our guidance on data minimisation and The National Archives Redaction toolkit.

- ✘ 80% did not seek guarantees or assurances that recipient organisations or individuals had deleted, destroyed or returned shared data once the purpose was served or any relevant retention period expired. We found that some MATs had not asked for evidence of disposal or audited partner organisations to check that data had been deleted in line with agreed retention periods.

Good practice case study - data quality and retention

Organisations should ensure that data retention periods are agreed and recorded in DSAs. One organisation had documented common retention periods in DSAs along with details of destruction methods. Agreements either allowed the organisation to audit the partner organisation to check records had been destroyed or stated that a destruction certificate would be provided as evidence.

Disclosures

- ✘ At 70% of MATs there was insufficient evidence recorded on the data subject file, spreadsheets or monitoring documents to show quality assessment or approval regarding the validity of any disclosures. In some cases, there was no documented requirement that disclosures should be quality checked or approved and that evidence of checks should be recorded.

Good practice case study – quality checks on disclosures

Organisations are expected to make sure that appropriate checks are in place before sharing personal data with third parties. One example of good practice we observed at a MAT, the data protection officer (DPO) was notified of any ad-hoc third party requests for personal data by the person handling the request. The DPO authorised any disclosures. A record of the request, who made the request and the reason for the request, the information requested, any ID checks and the DPO advice provided was documented on the pupil’s CPOMs record.

Resources

We have produced guidance for organisations to consult in regard to their information security incident management. This information can be found on our website www.ico.org.uk:

- Guide to Data Protection,
- Overview of the GDPR,
- Personal data breaches,
- Data protection breach notification form,
- Accountability and governance,
- Contracts,
- What needs to be included in the contract?,
- Responsibilities and liabilities of controllers ,
- Accountability principle;
- Data minimisation principle,
- Accuracy principle,
- Documentation,
- Documentation template for controllers,
- Lawful basis interactive tool,
- Lawful basis resources,
- What do we need to consider when choosing a lawful basis for processing children's personal data?,
- The right to be informed,
- Automated decision making, including profiling,
- What is valid consent?,
- What are the rules on children's consent?,
- What privacy information should we provide?,
- Age appropriate design: a code of practice for online services,
- Data protection by design and default,
- DPIAs,
- Draft data sharing code of practice,
- Data sharing and subject access checklist,
- Exemptions, and
- The National Archives Redaction toolkit.