Findings from ICO reviews of subject access request handling within educational establishments

November 2020

Information Commissioner's Office

Introduction
Table of contents

Introduction

The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Under Article 15 of the GDPR individuals have the right to access their personal data. This is commonly referred to as subject access.

Post GDPR, the most common data protection complaint received by the ICO concerning schools was in relation to subject access requests (SARs). The ICO carried out a review of eight educational establishments (EEs) in relation to their compliance with data protection legislation, particularly their SAR handling. The reviewed EEs consisted of multi academy trusts (MATs), local authority maintained primary schools and independent schools. The reviews concluded in 2019.

This report is based on these reviews. It highlights our experience of how effective the controls in place were in relation to the handling of SARs and how embedded they were. It is intended to help them and others in the sector recognise where they can make improvements. No individual organisations are named in this report.

Typical processing of personal data by educational establishments

The reviewed EEs process both paper and electronic records relating to staff, pupils and volunteers. Most personal data is processed for educational purposes. EEs also process a large amount of special category data as defined by the GDPR, including information on staff and pupils' health, race, ethnic origin, religion and biometrics.

Most information is held electronically on management information systems (MIS), in relation to pupil records, and human resources (HR) records, portals and payroll systems. Some organisations held local paper copies, which included HR information, school admissions and consent forms. This also included some special category data relating to special educational needs and safeguarding information.

Control areas

When conducting the reviews, we assessed the controls that the EEs had in place for the handling of SARs and how effective those arrangements were. Where we identified risks, we made recommendations to mitigate these and improve assurance against specific controls.

The relevant control areas were:

Being ready for requests
Individuals are guided on how to make a request and staff are in place to handle those requests in line with policies and procedures.

Training
Staff receive training on how to recognise a SAR and what to do if a request is received. Staff who handle SARs have specialist training.

Recognising a request
Staff are made aware of how to identify and channel requests to the appropriate team or person.

Validating and managing a request
Procedures are implemented to safeguard individuals' privacy and ensure that requests are dealt with in a timely manner that meets expectations.

Finding and retrieving information
Processes are in place to locate information required in response to a request in good time.

Exemptions and redactions
Procedures are in place to consider whether personal and third party data should be removed on a case by case basis and to ensure a consistent approach.

Supplying information
Procedures are in place and are being followed to explain what has been provided, where information has been withheld and also provide direct access and support if required.

Monitoring and improving performance
The organisation monitors performance in handling requests and uses that intelligence to improve performance and procedures.

Areas of good practice

We identified examples of good practice during the review.

- ✓ One EE had a well-structured, high-level data protection policy in place, with an easy to follow SARs process diagram.
- ✓ 87% of EEs had a specific person, such as a data protection officer (DPO) or equivalent, who was responsible for managing and responding to requests. At MATs or groupings of independent schools, a DPO was supported by a data protection lead in each school.
- ✓ In 87% of EEs, the data protection leads in each school had received specialised SAR training. Training concentrated on the application of exemptions and redaction of information. DPOs or equivalents received formalised training on SARs from external organisations.
- ✓ 62% of EEs had a central SAR log in place to record all requests for personal data. The DPO or equivalent had oversight and management of the log.
- ✓ One EE used their SAR log to trigger the escalation process. When a SAR was identified as falling behind, they used a traffic light system to escalate discussions to the DPO and senior management.
- ✓ 75% of EEs had an information asset register or data map which listed all types of records and personal data held and the location of the information. This made it easier to locate information that may be required as part of a SAR.
- ✓ In at least two cases, information to be redacted or withheld completely was considered on a case by case basis. Approval was also provided by the DPO or by a senior manager before the source material was copied into redacted form.
- ✓ One EE had a formally documented internal escalation process in place for requesters to follow and who wished to have the response to the request reviewed. This procedure was available on the organisation’s website and was referenced within the SAR response letter.

Areas for improvement

During the review a number of areas for improvement were identified. We made recommendations to assist the individual EEs to address these areas. Some of the key recommendations are outlined in the grey boxes below, particularly where they address areas for improvement identified in multiple EEs or where we feel it would be beneficial for other organisations in the sector to consider implementing them.

Being ready for requests

- ✘ Some EEs had no version control or document control table in place for the SAR procedures or data protection policies.

- ✘ Not all EEs included a section within the data protection policy and SAR procedures detailing how compliance with the policy was governed and monitored.

Recommendation

Policies should include a document control table, which records:

- version number,
- date of approval,
- date for review,
- approval by an appropriate governance group or senior management, and
- annual review date.

Policies should also include a section on how they will be governed and monitored. Responsibilities for handling of SARs should be assigned to appropriate staff and recorded in data protection policies or SAR procedures. Organisations need to demonstrate how they ensure compliance with Article 12 and Article 15 of the GDPR.

- ✘ In some cases we found that the SAR guidance provided in data protection policies was too high level and there were no detailed operational procedures for all stages of the SAR handling process.

- ✘ In one instance we found that there was no staff information on how they should deal with requests which are 'manifestly unfounded' or 'excessive' as referred to in Article 12(5) of the GDPR.

- ✘ Over a third of EEs did not action a SAR received in school holidays, incorrectly delaying the request until the new school term. This had also been incorrectly referred to in policies and procedures. The statutory timeframe outlined in Article 12(3) of the GDPR still applies during school holidays or closures.

Recommendation

Organisations should create detailed operational procedures for the SARs, including:

- each stage of the process and the key information that should be considered,
- guidance on ‘manifestly unfounded’ or ‘manifestly excessive’ requests and how these should be handled. For further details please see What does manifestly unfounded mean? and What does manifestly excessive mean?, and
- the SAR response timescales and the fact that requests received in school holidays or closures should still be responded to within the normal statutory timescales. For further details see How long do we have to comply?

✘ Over 60% of EEs did not provide sufficient guidance on how to make a SAR on the organisation’s website. Also, the equivalent information was not provided in paper format in public areas. In some cases, privacy notices also lacked details about individual rights under the GDPR, including the right of access and details on how individuals can exercise these rights as required by Article 13(2)(b) of the GDPR. Please see our guidance on the right to be informed.

Recommendation

Organisations should ensure that they provide guidance on their websites and in public information points, such as reception areas, on how they can make a SAR. It is good practice to provide a SAR form on the organisation’s website, although you must make it clear that completion of a SAR form is not compulsory.

A form can act as a guide for requesters and staff and help to ensure that all relevant information is captured at the outset. This helps to minimise the need to ask for further clarification, ID or proof of consent from the requester further into the process. It can also help staff to capture all relevant information if a request is made verbally and help the organisation to expedite requests within the statutory timescale of one calendar month (Article 12(3) of the GDPR). For further details please see Should we provide a specially designed form?

- ✘ Around a quarter of EEs only had one person responsible for processing SARs. This means that there was no resilience against staff absence, to mitigate against any backlogs or failures to meet statutory response timeframes.

Recommendation

Organisations need to consider nominating and training extra staff who can help to cover the SAR workload if the main SAR handler is absent. This will assist in meeting the statutory timescales.

- ✘ 75% of EEs did not ensure that all data processors who collected, stored or processed personal data on behalf of the EE understood their obligations in relation to requests for personal data as required under Article 28(1) of the GDPR. Not all data processor contracts included a clause outlining these responsibilities.

Recommendation

Data processor contracts should include clauses that require the data processor to:

- notify the controller of any requests for personal data received as soon as possible or within a stated timeframe, and
- to provide personal data to the controller in the event of a request within a specified timescale as required by Article 28(3)(e) of the GDPR.

For further details see our guidance on what needs to be included in the contract.

Training

- ✘ Most EEs included information about SARs within their mandatory staff data protection training; however some EEs did not annually refresh training.

- ✘ In other instances, we found that the DPO or equivalent did not have oversight of training content and training completion reports. Line managers did not chase up staff who hadn’t completed the training.

✘ Training content and other guidance did not always provide sufficient information about SARs.

Recommendation

All staff who handle personal data should complete data protection training and refresh this training on an annual basis.

Training content and relevant procedures should cover:

- what is a SAR,
- the fact that SARs can be made in writing, as well as verbally or via social media,
- what to do if a SAR is received,
- who is entitled to make a SAR, and
- what to do if a request for personal data is made by a third party either on behalf of the individual or for other reasons, for example a police officer.

Reports on training completion should be provided to the DPO or equivalent and to relevant line managers. Staff who have not completed training should be chased up and required to complete the training. See our guidance on the right of access.

✘ Not all staff responsible for the handling of SARs had received specialist training.

Recommendation

Staff who handle or process SARs should receive additional training which includes:

- the SAR process,
- how to apply exemptions,
- third party personal data, and
- how to redact information safely and securely.

This training should be refreshed on an annual basis.

Recognising a request

✘ In 50% of cases, only written SAR requests were recognised and this was incorrectly documented in policies and procedures. The GDPR does not specify how to make a valid request. This means that an individual can make a SAR to an organisation either verbally or in writing, including via social media. We also found a lack of guidance detailing how verbal SARs should be handled and recorded. For further details please How do we recognise a request?

Recommendation

Data protection policies and SAR guidance should state that requests can be made verbally and in writing, including via social media. Organisations should create a procedure for dealing with verbal requests, detailing how these should be recorded, responded to and processed.

- ✗ Half of EEs did not have a documented process for verifying the identity and the address of the requester, including stating when ID checks are required. We also found that some EEs did not keep adequate records of the ID and address checks undertaken.
- ✗ In approximately a quarter of cases, we found that where requests were made on an individual’s behalf, request handlers checked to ensure that a written authority or power of attorney was in place. However, no record of checks made were retained.

Recommendation

Article 12(6) of the GDPR says that where the controller has reasonable doubt regarding the identity of the requester, they may request further information to confirm the identity of that person. There should be a documented process in place for verifying the identity of the requester, where there is reasonable doubt. This should specify what sort of ID is requested and the circumstances where this may be required. Addresses should be checked to ensure that information is sent to the correct postal or email address. A record of the checks should also be maintained to ensure adequate checks have been made and to minimise the risk of an inappropriate disclosure of the information to the wrong person or address. For further information see Can we ask for ID?

The procedure should also state that checks for either a written authority or power of attorney should be made where a requester is acting on behalf of another individual. A record of any checks made should be maintained. For further details see What about requests made on behalf of others?

✘ In some cases there were inadequate records kept detailing checks on parental responsibility, where requests were made on a child’s behalf.

Recommendation

The right of access to the personal data belongs to the child and consideration should be given to whether the child has the maturity and ability to understand their rights. Where an organisation is confident that the child has the ability to understand their rights, the response should be directed to the child rather than their parents or guardian. An organisation may allow the parent to exercise the child’s rights on their behalf if the child authorises this, or if it is in the best interests of the child.

A record of any assessments made regarding the child’s capacity, checks on parental responsibility or if the child has provided consent for the individual to request their personal data, should be recorded. For further information please see What about requests for information about children?

✘ In around a third of EEs there was no written process for dealing with requests which required further clarification, such as where there was insufficient information to locate the data or the nature of the request was unclear. In one instance, guidance stated that the request would not be responded to if the request was unclear.

Recommendation

Organisations should clarify a request as soon as possible. Organisations cannot refuse to provide a response which they believe is not clear. However, Recital 63 of the GDPR states that “where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates”. Guidance for clarifying requests should be included in SAR procedures. This may help organisations locate what information is required. For further information please see What should we consider when responding to a request?

Validating and managing a request

- ✘ A number of EEs confirmed that it was customary to send an email or letter to the requester acknowledging receipt of a request. However, there was no written procedure which detailed the requirement to acknowledge receipt.

Recommendation

It is good practice to acknowledge receipt of a SAR. Organisations should consider creating a template acknowledgement letter for SARs. This should inform the requester that the request has been received and the expected deadline for completion. This provides assurance that the request has been received and is being dealt with within the timescale of any expected response.

- ✘ A significant proportion of EEs did not keep accurate records outlining the reasons for extending the timeframe of a request. In addition, some did not have written procedures explaining when the response timeframe of a request can be extended and how these requests should be processed.
- ✘ In over a third of cases we found that there were no standard procedures or template letters in place for contacting the requester when a request is delayed or where the organisation has applied an extension to the timescale. Article 12(3) requires that where an extension has been applied "the controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay".

Recommendation

Article 12(3) of the GDPR states that requests should be responded to within a calendar month. However, it also allows for an extension of the response timeframe by a further two months, in some circumstances, considering the complexity and number of requests. Organisations should create SAR guidance explaining when the timescale for SARs can be extended. A record of the reason why the timescale has been extended should be maintained. If there will be a delay in providing a response to the request outside of statutory timescales, the reason for the delay should also be recorded. Guidance should also explain that the requester be notified as soon as possible about any extension of the timescales or delay in dealing with the request and the reasons for this and the expected date of the response. Template response letters should be created to reflect this procedure.

For further information please see How long do we have to comply?

✘ A number of EEs did not record key headings on the SAR log, such as the due dates for requests, a brief explanation of information withheld and the reasons for withholding it under a relevant exemption or exception within the GDPR.

Recommendation

Organisations should include on the SAR log:

- due date of request,
- brief explanation of the information withheld, and
- reasons for withholding the information under an exemption or exception.

This information should be recorded so that the organisation can monitor when requests are due and ensure that they are completed within statutory timescales set out under Article 12(3) of the GDPR. Records of exemptions applied and the reasons behind these should be recorded to ensure that there is an audit trail of any decisions made to withhold information and in the event that this is queried by the requester or the ICO.

✘ In 50% of cases we found that there was no formal checklist or that checklists in place did not record all key stages of the SAR, such as, identity and address verification, systems or departments searched, redaction of third party and exempt data, as well as any quality assessments carried out.

Recommendation

Organisations may wish to create a formal checklist listing the various stages that the individual processing the SAR must complete. This could include:

- identity and address verification,
- systems and departments checked for information,
- review of information,
- redaction of third party or exempt data, and
- quality assessments carried out.

Checklists can assist organisations dealing with requests in line with their own procedures and the GDPR.

✘ Around half of EEs hold informal meetings in order to escalate SARs that are complex or may be delayed. However, a significant number of EEs had not formally documented the escalation process.

Recommendation

Organisations should have a documented process in place for escalating SARs which are complex or delayed to suitable senior management or a forum. This helps organisations to demonstrate compliance with Article 5(2) of the GDPR, the accountability principle and the timescales outlined under Article 12(3) of the GDPR.

✘ Not all EEs referenced in their SAR Procedure the fact that it is an offence under Section 173 of the DPA 2018 for a controller, employee of the controller or a person acting under the direction of the controller to alter, deface, block, erase, destroy or conceal information in relation to a SAR.

Recommendation

Organisations should highlight in procedures the provisions set out in Section 173 of the DPA 2018 to ensure that information in relation to a SAR is not unlawfully altered, defaced, blocked, erased, destroyed or concealed.

Finding and retrieving information

✘ Around a quarter of EEs did not have written procedures in place to advise staff how to find and retrieve archived paper records that may be required as part of a SAR. We also found that not all EEs had formal written procedures detailing the process for finding and retrieving personal data that has been stored electronically, archived or backed up (including emails).

Recommendation

Organisations should ensure that they have formally documented procedures for the retrieval of electronic records, (including those stored in archive or back-up systems) and archived paper records. It is important that formal procedures are in place so that organisations can evidence compliance with Article 24(1) (‘appropriate technical and organisational measures’). For further information see the ‘How should we prepare?’ section of our detailed guidance on the Right of Access.

✘ In one case, emails were stored indefinitely and were not being automatically deleted.

Recommendation

It is important that information such as emails are not kept for longer than is necessary. Organisations should have measures in place to manage this and to ensure compliance with Article 5(2)(e) of the GDPR (storage limitation principle). Emails which are required for evidential purposes should be kept in properly indexed and managed filing system or database. Organisations should consider whether email client systems could be set to auto delete email after a set period of time. The time period should be documented within the retention policy. This will help organisations to cut down on the amount of information that may need to be searched for, checked and provided as part of a SAR. Please see our guidance on storage limitation.

Exemptions and redactions

✘ At some EEs there was no documented sign off process for checking the information prior to it being withheld or redacted.

Recommendation

Organisations should ensure that there is a formally documented process for checking information prior to it being withheld or redacted. Sign off for the SAR should be carried out by someone who is independent of the SAR processing. This can be the DPO or someone with adequate authority, for example the head teacher or safeguarding lead. This is to ensure that information is correctly withheld from the requester in accordance with an exemption or exception under the GDPR and DPA18. A record of sign off should be recorded on the SAR log, SAR file or on a checklist. For further details please see 'What other exemptions are there?' and 'What should we do if the request involves information about other individuals?' sections in our Right of access detailed guidance.

✘ We found that the majority of EEs followed expected practice by carrying out redactions on the information to be provided where appropriate. Redactions were either carried out manually using a black marker pen or electronically using redaction software; however there was no documented process explaining to staff how this should be carried out.

Recommendation

A formally documented process should be in place to ensure that redactions are dealt with consistently and to provide resilience in case staff who have knowledge of the redaction process are absent or leave the organisation. For further information please see The National Archives Redaction Toolkit.

✘ A significant number of EEs did not carry out an independent quality review to confirm that all data has been appropriately withheld. Around 75% of EEs had not formally documented their quality review process.

Recommendation

Organisations should formally implement and document an independent quality review process for SARs. The review should be carried out by someone who was independent of the SAR processing. The quality review should be recorded on the SAR log, SAR file or checklist (who by and the date).

✘ Three quarters of EEs did not carry out routine sample cold case quality reviews on completed SARs.

Recommendation

It is good practice to carry out cold case quality reviews. The quality review should be carried out by the DPO or suitable manager to ensure that information has been redacted appropriately and exemptions are applied consistently. The cold case assessment process should be documented.

✘ In some cases, a copy of the information disclosed to the requestor, showing the redactions and / or exemptions, and the reasons behind them was not kept. This should be retained for reference purposes to assist with quality reviews and complaints.

Recommendation

A full record of the redactions and exemptions should be retained in case the requester or the ICO request a review of the decision to withhold the information. This information can also be used in quality reviews to ensure staff are consistently applying redactions and exemptions. These records should be retained in line with the organisation's retention schedule. This requirement should be be recorded in the SAR procedure.

Supplying information

✘ A significant number of EEs did not explain in the covering letter sent in response to a SAR, what searches had been made to deal with the request and the information revealed by those searches. Including these details in the covering letter will help the requester understand whether they have received all the information they are entitled to.

✘ Some EEs did not explain in their SAR response letters, what information had been withheld and the reasons why.

✘ Some EEs did not include reference to the individual’s right to appeal to the ICO under Article 15(1)(f) in the response letter sent to the requester.

Recommendation

Organisations should consider creating a template covering letter to ensure that all key information is provided to the requester. The template letter should include:

- the various types of information that should be provided as Article 15 of the GDPR does not only require organisations to provide copies of personal data requested. See other information for a full list,
- where information has been withheld, provide an explanation (as far as is possible) to the requester of why any information has been withheld and the exemption or exception which is being relied upon to withhold the information. The explanation provided should be in plain English and should do more than simply state that a particular exemption has been applied. For further information see ‘What other exemptions are there?’?’ section of our Right of access details guidance.
- advice on how the requester can raise a complaint with the organisation to review the response to the request, and
- how requesters can complain to the ICO if they are not happy with the outcome of the request. The right to complain to the ICO should also be referenced within privacy notices. See our guidance on the right to be informed.

✘ It is good practice to allow requesters to view the requested information onsite. Over half of EEs did not have documented procedures in place for requesters to view the requested information on the premises (where appropriate).

Recommendation

Organisations may wish to document a procedure for allowing requesters to view the requested information onsite. A documented process should cover under what circumstances a requester is allowed to see their records on site. It should also explain when a requester can take away copies of their personal data (unless an exemption applies). For further guidance see 'How should we supply information to the requester?' in our Right of access detailed guidance.

✘ 75% of EEs did not mark the information disclosed to the requestor as 'individual's copy' before releasing the information to the requester.

Recommendation

Organisations should consider marking or labelling the information provided to the requestor with the identity of the requestor before release, such as, 'individual's copy'. This may help identify the source of any further disclosure of the information, should the need arise, such as breach reporting under the GDPR Article 33.

Monitoring and improving performance

✘ Some EEs did not report adequate management information about SARs to senior managers or steering groups. For example some reported on the number of requests received, but not how many were completed or outstanding within statutory timescales.

Recommendation

Organisations should report key information about SARs to senior managers or steering groups. It is advisable to set KPIs for SARs so that performance can be monitored by senior management or IG steering groups. KPIs could include the number of SARs received, the number completed within and outside statutory timescales, the number still outstanding and the number that have exceeded the statutory timescales. This will enable an organisation to demonstrate that it has oversight of data protection responsibilities and is actively managing compliance in line with the accountability principle under Article 5(2) of the GDPR and obligations under Articles 12 and 15 of the GDPR.

✘ 50% of EEs did not formally document an internal review process within the SAR procedure to deal with cases where requesters were dissatisfied with the initial response to the SAR.

Recommendation

It is good practice for organisations to have a documented process for dealing with complaints about SARs. Organisations should consider creating and documenting an internal review process for SARs. The procedure should be made available on the organisation’s website and referenced within the SAR response letter. The review should be carried out by a senior member of staff who was not involved in the original request.

✘ We observed that in one case, complaints to the ICO were combined with other general complaint figures and there was no categorisation of different types of complaint. This meant that statistics and trend analysis could not be reported on.

✘ In some cases, complaints about SARs were not analysed and feedback on lessons learned was not provided to relevant staff, senior management or steering groups. Reporting on complaints helps organisations to demonstrate that they are actively improving their compliance with the GDPR and DPA18.

Recommendation

Organisations should record and report on the number and type of complaints made to them and to the ICO. The outcomes of such complaints should be considered and any lessons learned implemented. This will help organisations to demonstrate that they are actively improving their compliance with the GDPR and DPA 2018.

ICO Resources

The ICO has produced SARs handling guidance for organisations to consult. This information can be found on our website www.ico.org.uk:

- Guide to Data Protection
- Guide to the GDPR
- Right of access
- Exemptions
- Right of access detailed guidance
- How do we recognise a subject access request (SAR)?
- What does manifestly unfounded mean?
- What does manifestly excessive mean?
- Should we provide a standard form?
- What needs to be included in the contract?
- Can we ask for ID?
- What about requests made on behalf of others?
- What about requests for information about children?
- What should we consider when responding to a request?
- How long do we have to comply?
- Can we extend the time for a response?
- Storage limitation
- The National Archives Redaction toolkit, and
- Right to be informed