

INDEPENDENT SCHOOLS INSPECTORATE

DATA SUBJECT ACCESS REQUEST POLICY

DATE OF LAST REVIEW:	July 2025
POLICY OWNER:	Director Legal, Regulation and Complaints
APPROVED BY:	Chief Executive Officer - Chief Inspector
DATE OF NEXT REVIEW:	July 2027

Contents

Policy statement	3
What information are individuals entitled to?	3
When must the information be provided?	3
Is a fee charged for dealing with a subject access request?	4
How can requests for large amounts of personal data be managed?	5
When can requests be refused?	5
Complaints	6
ISI's process in response to a subject access request	6
TABLE OF KEY CHANGES	7

Policy statement

1. Under the UK General Data Protection Regulation (UK GDPR) and relevant UK legislation, individuals (data subjects) have the right to obtain confirmation that their data is being processed, and to have access to their personal data and other supplementary information.
2. An individual can make a subject access request (SAR) verbally or in writing to any part of ISI's organisation. All ISI employees and inspectors must therefore be aware of potential subject access requests.
3. This policy provides information on how ISI manages Data Subject Access Requests and outlines key processes and responsibilities.
4. Any enquiries about the policy should be directed to dp@isi.net.

What information are individuals entitled to?

5. As part of a SAR, data subjects are entitled to a copy of their personal data as well as other supplementary information as set out in ISI's privacy notice and below:
 - i. confirmation that ISI is processing their personal data;
 - ii. a copy of their personal data in intelligible form with an explanation of any technical terms or jargon which might otherwise obscure its meaning to the reader;
 - iii. other supplementary information that relates to the information that the Information Commissioner's Office sets out on their website and to the information ISI provides in its privacy notice:
 - (a) the legal basis on which ISI is processing the data;
 - (b) the purpose of this processing;
 - (c) the categories (types) of personal data relating to the individual that ISI is processing;
 - (d) the recipients or categories of recipients to whom their personal data have been or will be disclosed (if applicable);
 - (e) the envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data are stored;
 - (f) the existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing;
 - (g) their right to lodge a complaint with ISI and/or the Information Commissioner's Office (ICO) – see [below](#);
 - (h) where the personal data are not collected from the individual, any available information as to their source; and
 - (i) details of the safeguards in place for any transfers of their personal data to countries outside of the UK, where applicable.

When must the information be provided?

4. ISI will provide the relevant personal information to the requesting individual without delay and at the latest within one month of receipt of the request. This period can be extended by a further two months where requests from a requesting individual are complex or numerous (i.e. ISI may respond up to three months from the receipt of the request). If this is the case, the

requesting individual must be informed within one month of the receipt of the request, along with an explanation of why the extension is necessary, and what the new deadline for responding will be.

Is a fee charged for dealing with a subject access request?

5. ISI will provide a copy of the relevant information free of charge. However, where requests are manifestly unfounded or excessive, in particular because they are repetitive, ISI may:
 - i. charge a reasonable fee taking into account the administrative costs of providing the information; or
 - ii. refuse to respond.

How should the request be provided?

6. Ideally requests should be made by email to dp@isi.net specifying clearly the personal data sought. This will help ISI to understand the request and to respond promptly.
7. It is helpful and will enable ISI to respond more quickly if the following information is included in a SAR:
 - i. a subject line or header that says "subject access request"
 - ii. the name of the requesting individual (and any other name under which ISI may have recorded information about the requesting individual)
 - iii. any other information that would help ISI identify the requesting individual e.g. relationship to ISI
 - iv. the requesting individual's email address, home address and phone number
 - v. what personal information is wanted (be specific about the information being requested, and where relevant say what information is not requested)
 - vi. details or dates that will help ISI find the information sought
 - vii. the reason for requesting the information (this is not a requirement, but it will help ISI to find what is requested) and
 - viii. if the requesting individual has any accessibility requirements (e.g., large fonts).
8. When asking for information, the requesting individual should be as specific as possible. This may help to get the fastest possible reply and more useful information back.
9. The requesting individual can ask for all the information that ISI holds about themselves, though ISI may sometimes refuse to provide some or all of the information requested. If all of the information held is requested, it may mean a lot of information is sent back that is not needed. It may also mean that it takes longer for ISI to send this information.
10. If a third party is submitting the request on the requesting individual's behalf, they should explain their relationship to the requesting individual, along with the requesting individual's full details.
11. The identity of the person making the request must be verified by 'reasonable means'. To avoid personal data being sent to another individual, either accidentally or as a result of deception, it may be necessary for ISI to confirm the requesting individual's identity. Examples of the information ISI may request in order to do this include: date of birth, other known names or aliases, confirmation of postal or email address, a copy of a passport or driving license. The

timescale for responding to a subject access request does not begin until ISI has confirmed identity where this is necessary.

12. When making a subject access request for information held about a child, consideration should be given to whether the child is mature enough to understand their rights. If the request is from a child and they can understand their rights, the child will be responded to directly by ISI. ISI may, however, allow parents or guardians to exercise the child's rights on their behalf if the child authorises this in writing.

How can requests for large amounts of personal data be managed?

13. If the scope of the request is unclear, or where large quantities of information about an individual are processed, the requesting individual can be asked to specify the information the request relates to or narrow the scope of their request, for example by specifying the date from when the data is sought, in order to facilitate ISI's response. The time limit for responding is paused until ISI receives clarification. ISI will confirm this to the requesting individual when requesting clarification.
14. However, requesting individuals are not required to narrow their requests. Where requests are particularly voluminous, ISI is only required to carry out a 'reasonable search' for the information, taking into account staff time, cost, the volume of data records, any potential exemptions, seeking legal advice, etc.
15. If, following a response to a request, the requesting individual makes repeat requests for information that has been previously provided, ISI may consider a request excessive.

When can requests be refused?

16. ISI may refuse to comply with a SAR if it is 'manifestly unfounded' or 'manifestly excessive'.
17. Factors that may indicate a **manifestly unfounded** request include where:
 - i. the requesting individual clearly has no intention to exercise their right of access, for example an individual makes a request, but then offers to withdraw it in return for some form of benefit
 - ii. the request is malicious in intent and is being used to harass ISI with no real purpose other than to cause disruption. For example, the requesting individual explicitly states, in the request itself or in other communications, that they intend to cause disruption; makes unsubstantiated accusations against ISI or specific employees which are clearly prompted by malice; targets a particular employee against whom they have some personal grudge; or systematically sends different requests to ISI as part of a campaign with the intention of causing disruption.
18. To determine whether a request is **manifestly excessive** ISI will consider:
 - i. the nature of the requested information;
 - ii. the context of the request, and the relationship between ISI and the requesting individual;
 - iii. ISI's available resources;
 - iv. whether the request largely repeats previous requests and a reasonable interval has not elapsed;
 - v. whether it overlaps with other requests;

- vi. where ISI has already provided a copy of the information to the requesting individual by alternative means.
19. Access to personal data may also be restricted in instances where an exemption under the Data Protection Act 2018 applies, for example, the relevant information identifies a third party, is covered by legal advice privilege or information sharing may place the requesting individual at risk of significant harm or jeopardise police investigations into any alleged offence(s). The application of any exemptions will be determined on a case-by-case basis. ISI will justify and document its reasons for relying on an exemption. In some situations, ISI's response may be more general and may not include details of which exemptions it has relied on, for example, where telling a requesting individual that ISI has applied a particular exemption would prejudice the purpose of that exemption.
 20. Where ISI refuses to respond to a request, ISI will notify the requesting individual that their subject access request has been refused within one calendar month from the date they made the request. ISI will explain why it is refusing to respond, informing the requesting individual of their right to have their case reviewed by way of ISI's non-inspections complaints procedure available on ISI's website [here](#), the right to complain to the Information Commissioners Office (ICO) following the arrangements set out on the ICO's website [here](#), or their ability to seek to enforce this right through a judicial remedy.

Complaints

21. If the requesting individual is unhappy with ISI's response to their request, they can submit a complaint to ISI within two months of receiving ISI's response. In exceptional circumstances ISI may be able to extend the time limit to make a complaint.
22. ISI will respond to the complaint without delay and in line with ISI's non-inspection complaints policy, available on ISI's website [here](#). If the requesting individual is still unhappy with ISI's response, they have the right to make a complaint to the Information Commissioners Office (ICO), the UK supervisory authority for data protection issues. Arrangements for doing so are set out on the ICO's website [here](#).

ISI's process in response to a subject access request

23. Any requests sent to any employee other than by way of dp@isi.net, should be forwarded by the receiving employee immediately to the Director Legal, Regulation and Complaints, copying in data@isi.net and complaints@isi.net.
24. A member of the Complaints and Legal Team will respond to the data subject to: (i) verify identity; and (ii) where necessary, ask for the request to be clarified or narrowed.
25. The Head of Information Technology will coordinate the search of online records, as instructed by the Director Legal, Regulation and Complaints.
18. The Head of the relevant function, as instructed by a member of the Complaints and Legal team, will coordinate a search of paper documents, if needed, and the conversion of these into electronic versions.

19. The Complaints and Legal Team will review relevant documents and manage redaction if necessary.
20. The Chief Operating Officer, if appropriate to the subject matter, will approve documents to be sent to the data subject.
21. The Complaints and Legal Team will coordinate the transfer of relevant documents to the data subject, under cover of letter (which may be sent electronically).
22. Any response sent to the requesting individual must comply with the requirements of the UK GDPR and must include all of the information the requesting individual is entitled to (see [above](#)).
23. Director Legal, Regulation and Complaints records details in relation to the request received and the actions taken in the relevant folder in the dedicated GDPR site.

TABLE OF KEY CHANGES

Date of review	Paragraph	Amendments
July 2025	All	Rewritten to provide clarity regarding: <ul style="list-style-type: none"> • What information individuals are entitled to • How requests should be provided • How ISI may verify identity of requesting individual • How ISI treats SARS requesting information about a child • When ISI may refuse a SAR • How to complain
May 2023	Cover	Change name of policy to 'Data' Subject Access Request policy
	1	Update all references to GDPR to UK GDPR
	3	New paragraphs outlining the information to which individuals are entitled
	4	Updated reference to deadlines
	9-14	New paragraphs outlining management of requests
	15-23	Updated process to reflect current management structure