

RIGHTS OF DATA SUBJECTS



Understanding Individual Rights under the UK GDPR

Every individual has legal rights over how their personal information is collected, used and shared. Schools and academy trusts must recognise requests promptly, respond within statutory timescales and demonstrate accountability under the UK GDPR and Data Protection Act 2018.

REMEMBER

A request does not need to mention "UK GDPR" or "Subject Access Request" to be valid. If somebody asks about personal data held by the school or trust, treat it seriously, log it promptly and seek DPO advice where needed.



Respecting individual rights strengthens trust, transparency and good information governance.

INDIVIDUAL RIGHTS

1

RIGHT TO BE INFORMED



Provide clear privacy notices. Explain what data is collected, why it is used, who it is shared with and how long it is retained.

Be transparent.

2

RIGHT OF ACCESS



Recognise Subject Access Requests made verbally or in writing. Verify identity and respond within one month.

Respond promptly

3

RIGHT TO RECTIFICATION



Correct inaccurate personal data and complete incomplete records. Notify others where appropriate.

Keep records accurate.

4

RIGHT TO ERASURE



Consider requests carefully alongside safeguarding, legal, financial and retention obligations. Record the decision.

Not an absolute right.



4

RESTRICT PROCESSING



Pause or limit processing while concerns are investigated. Mark restricted records clearly

Protect individual rights.

5

RIGHT TO DATA PORTABILITY



Receive personal data in a structured, commonly used and machine-readable format.

Provide data securely.

6

RIGHT TO OBJECT



Individuals can object to certain types of processing, particularly where personal data is processed.

Consider every request.

IOIO
IOIO



PRACTICAL GUIDANCE



Good practice is based on recognising requests early, verifying identity, applying exemptions carefully and keeping a clear audit trail.

1

PRACTICAL GUIDANCE



- Requests can be verbal or written.
- Check identity before disclosure.
- Clarify scope where needed.



Keep it lawful and evidenced.

2

COMMON MISTAKES



- Missing informal requests.
- Disclosing third-party information.
- Failing to monitor deadlines.



Avoid preventable risk.

3

GOOD PRACTICE



- Use a central request log.
- Escalate complex cases to the DPO.
- Review lessons learned.



Embed what good looks like.

THE 5 KEY ACTIONS



1

IDNETIFY

Recognise requests immediately.



2

LOG

Record date, scope and deadline.



3

VERIFY

Confirm identity before disclosure.



4

RESPOND

Apply exemptions and meet deadlines.



5

REVIEW

Update procedures and training.

SELF-ASSESSMENT CHECKLIST

	Yes	No	N/A
Staff can recognise data subject rights requests.	☐	☐	☐
Requests are logged with dates, scope and deadline.	☐	☐	☐
Identity checks are completed before disclosure.	☐	☐	☐
Exemptions and third-party data are considered.	☐	☐	☐
Responses are reviewed by the DPO where required.	☐	☐	☐
Lessons learned are recorded and acted upon.	☐	☐	☐

EXAMPLES OF DATA SUBJECT REQUESTS

01

A parent asks for a copy of their child's records.

02

A staff member asks to see information held in HR files.

03

A former pupil asks whether data can be deleted.

04

An employee asks for inaccurate information to be corrected.

05

An individual objects to the use of their photograph.



office@shardbusinessservices.co.uk



Part of the SBS Insight Hub
Professional Guidance Series



Produced by Shard Business Services
Helping you do more with less.