THE BLUE SCHOOL

CHURCH OF ENGLAND

Whatever you do in word or deed,
do everything in the name of the Lord Jesus,
giving thanks to God the Father through him.

Colossians 3:17

Policy	Right of Erasure request Procedure
Author	Headteacher
Ratified	December 2022
Review	December 2024

Subject Access Request Procedure

This procedure is based on guidance on Requests for Erasure (RFE) produced by the Information Commissioner's Office (ICO).

Requests for Erasure

Individuals have the right to invoke a request that their personal data be erased if:

- The personal data is no longer necessary for the purpose which you originally collected or processed it for;
- You are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- You are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- You are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- You have to do it to comply with a legal obligation; or
- You have processed the personal data to offer information society services to a child.

Neither the GDPR nor the DPA 2018 specify what constitutes a valid request, therefore;

- It can be in any format, verbal or written form (Letter, email, social media)
- Does not have to include the phrase "Request for Erasure" or "Article 17"
- Requester just needs to make it clear if they want their data erased, deleted anonymised or "to be forgotten"
- Can come from a 3rd party you share data with.

Key principles:

- **Anything you legally must retain do not and should not be erased i.e. Safeguarding files**
- **Cannot blanket withdraw consent, if you ask for it in a granular format, it needs to be withdrawn ina granular format,**
- **Clearly communicate the action you have taken on all the data which has been requested.**
- **Log and document everything you do for posterity.**

Rights of Children:

Regardless of their age, an individual has the right to control over their own data. This right supersedes the rights of parents or guardians.
This has implications for both requests by a child, or on behalf of a child, a child being an individual younger than the age of 18.

If the request for erasure comes from a child and you are confident that the child is mature enough to understand their rights then, you should respond directly to the child.
In this case then a Parent or Guardian would need the written permission of the child to act on their behalf (see 3rd party requests).
Alternatively, if it is clearly evident that the child is not mature enough then their parents/guardians can exercise their rights on their behalf.

In Scotland if someone is aged 12 years or over, they are presumed of sufficient age and maturity, however this does not apply in England, but it is a good indicator level of what could be reasonable.
For borderline cases then you can use the following to make an assessment;

- The child's level of maturity and their ability to make decisions like this;
- The nature of the personal data;
- Any court orders relating to parental access or responsibility that may apply;
- Any duty of confidence owed to the child or young person;
- Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- Any views the child or young person has on whether their parents should have access to information about them.

3rd Party Requests
An individual other than the data subject can submit a RFE most commonly this is utilised by solicitors working on behalf of an individual.
These 3rd parties would need written authorisation from the individual to act on their behalf. If there are any doubts regarding their authority, then contact the data subject directly to confirm.

Full Refusal to comply with a request:
You can refuse to comply with a request in full if it is:

a) Manifestly Unfounded

- the individual clearly has no intention to exercise their right of erasure for example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or

- the request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption. For example:
- the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
- the request makes unsubstantiated accusations against you or specific employees;
- the individual is targeting a particular employee against whom they have some personal grudge; or
- the individual systematically sends different requests to you as part of a campaign, e.g. once a week, with the intention of causing disruption.

There must be an obvious or clear quality to it being unfounded.
You should consider if you can prove if the individual genuinely wants to exercise their rights or not.

b) Excessive.

- It repeats the substance of previous requests and a reasonable interval has not elapsed; or
- It overlaps with other requests.

  However, it depends on the circumstances. It will **not necessarily** be excessive just because the individual:

- Requested a large amount of data be erased, even if you might find the request burdensome as they may have a legal right to do so.
- Made an overlapping request relating to a separate set of information; or
- Previously submitted requests which have been manifestly unfounded or excessive.

N.B Always consider when refusing a request you have to be able to demonstrate to the individual and ICO why you have made that decision.

<u>Receiving a Request for Erasure</u>

On receipt of a confirmed or potential RFE, the staff member or data processor must immediately notify the Office Manager at office@theblueschool.com
They will decide whether to refer the matter to the Data Protection Officer (DPO)
David Coy (contactable on david.coy@london.anglican.org, 07903 506531)

When an RFE is received it should be immediately entered onto the Request for Erasure log and given a reference number e.g. RFE2019001, in all future communications this reference number should be used to discuss the RFE.
The Log should record the, who, when, what, and why of the process.

Additionally, a folder should be created under the reference number and all associated documentation regarding the RFE be kept in the file for posterity.

Irrespective of whether the DPO is notified or not the response to the breach will follow the same path and be
be broken down into four distinct sections: **Acknowledgment, Search, Review & Erase, Response**

Timeframe of Response
The Data Protection Act 2018 gives a timeframe of one calendar month from the day after receipt for responding to an RFE. This is irrespective of the number of days in the month e.g. Received 17th July, Deadline 18th July.

Where this is not possible because the next month does not have a corresponding day, then the deadline is the last day of the month e.g. Received January 31st, Deadline 28th February.

<u>Stage 1: Acknowledgment:</u>
Sending a formal acknowledgement to confirm that:

- An RFE has been received.
- The date of receipt.
- What you believe the RFE is regarding.
- Whether anything further is needed from the Data subject i.e. clarification or refinement of the RFE, ID for verification.
- The timeframe for a final response*.

The acknowledgement can be sent electronically or in paper format, it is **not** recommended that this is undertaken verbally.

What the RFE is regarding:
It is important that you state verbatim what the individual has requested and give them the opportunity to confirm that you have understood the request correctly. This will save wasted time collecting data which is not required.

Clarification or Refinement:
If a request is received with asks for “All Data”, it is highly recommended that you seek further refinement to allow you to efficiently respond to the request within the timeframe.

ID Verification:
It is important that you are satisfied that the request is genuine, and the individual is are who they say there are. You don’t want to release information to an incorrect recipient. Therefore, if you are unsure request a copy of photo ID to confirm the identity of the requester.
.

Timeframe for Response:
Although the official process stated that there is a timeframe of one calendar month from the day after receipt.
This can be delayed or extended.

If you have requested further clarification or ID verification, the clock does not start until this is received. This should be explained in your acknowledgment.
If you believe you cannot respond within the one calendar month timeframe, then you can extend the deadline for up to two months. Most commonly this extension is used if the request is complex or extensive.
“All Data” requests commonly fall into this category.
Hence refining the “All Data” request is beneficial for both the requester and the school.

Stage 2 Search and Review.
Using the confirmed requested erasure of the RFE, you should work down the list and point for point and make a note of;

- Where data is held.
- What the format it is held in, paper or electronic.
- The Lawful basis for processing the data e.g. legitimate interest, consent, legal obligation.
- If there is a mandatory retention period for the data.
- Whether the data can be completely erased or anonymised.
- If it is held elsewhere in the form of system backups.

A way to store this information is in a spreadsheet or table.

Data Type	Location	Format	Lawful Basis	Retention Period	Erase/ Anonymise	Backup?

It is recommended that someone who has an appropriate level of authority is selected to search for the disputed data.

Record of Data Processing:
This can be used as an assistance tool to

a) Understand what data is being held on individuals
b) Where it is being held; Management software, filing cabinets.
c) What third party processors need to be contacted.

Contacting Third Party processors.
You are required to inform your third-party data processors or joint controllers of the request for erasure if:

- The personal data has been disclosed to others; or
- The personal data has been made public in an online environment (for example on social networks, forums or websites).

If the data has been disclosed to the third parties you must contact each one to inform them of the erasure request, if there are too many of them, then you just need to inform the requester who they are and what has been shared.

Erasure?

The DPA 2018 states you need not have to comply with a request for erasure in full if the data is required:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation;
- For the performance of a task carried out in the public interest or in the exercise of official authority;
- For archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- For the establishment, exercise or defence of legal claims.

This is not an exhaustive list and it is very much a case by case basis of what could and should be not be erased

N.B. During the Search and Review & Delete stages it can help that data is grouped together which respond to specific aspects of the request or which form narratives. E.g. all internal emails, Pupil file, exam results.

Stage 3 Collect and Erase:

It is recommended this part of the process be undertaken under the supervision of the Headteacher and or DPO as this is where the act of erasing items may occur.
Therefore, the person making the decision should have the requisite authority and knowledge to undertake the task

Using a version of the table or spreadsheet created in the Search and Review stage, pare down the information and add in the justification of why the decision was made.
This should be as it should be as granular as necessary to fully illustrate how you have responded to the request.
For example:

Request Item	Location Held/Format	Decision	Justification
Full Name	SIMS (Electronic)	Erase/Anonymise/Retain	Legal Obligation to hold for DOB + 25 years
Email Address	Parent Pay	**Erase**/~~Anonymise/Retain~~	School no longer needs to contact parent

Erase/Anonymise?

Whilst going through and creating your justification table it is recommended that carry out the collection and erasure/anonymisiation of any data you have selected

Stage 4: Final Response.

This is where in a formal correspondence you explain the process and result of the Search and Review & Erase stages to the data subject and present them with the conclusion.

It should include:

- What and where was searched to comply with the request, e.g. paper records, SIMS, emails, CPOMS
- Reconfirm what was asked to be erased
- The third parties where data has been disclosed and you have contacted to inform of the erasure request.
- What has been erased and why.
- What has been retained and why.
- Ability to discuss this further with the school.
- Right to refer to the ICO and contact details.

To save duplication of work, the table of decisions made in the Collect and Erase phase can be used.

Request Item	**Location Held/Format**	**Decision**	**Justification**
Full Name	SIMS (Electronic)	~~Erase/Anonymise/~~**Retain**	Legal Obligation to hold for DOB + 25 years
Email Address	Parent Pay	**Erase**/~~Anonymise/Retain~~	School no longer needs to contact parent

This should be easy to read and understand without using jargon.

N.B. You will also be retaining some data on the individual in your Request for Erasure Log and Associated file. This should be mentioned in the response.