Primary Advantage

Data protection & retention policy

PRIMARY ADVANTAGE

SCHOOLS ACHIEVING MORE TOGETHER

Table of Contents

Revisions

Date	Summary of changes
April 2022	Adoption of the template policy from The Key for School Governors.

1. Aims

The Federation aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

It also reflects the Government's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation

TERM	DEFINITION
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

Our Federation and its schools process personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Federation is registered with the ICO, as legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our Federation and its schools, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The Central Governing Board has overall responsibility for ensuring that our schools comply with all relevant data protection obligations. Data protection is monitored by Business & Finance Committee.

5.2 Data protection officer

The data protection officer (DPO) is responsible for advising on the implementation of this policy, monitoring our compliance with data protection law, and advising on related policies and guidelines where applicable.

The DPO is also the first point of contact for the ICO.

Our DPO is Hassan Muzammal at Grow Education Partners: Hassan.Muzammal@london.anglican.org

5.3 Data protection lead

The Federation's Governance Manager is our data protection lead (DPL). They are responsible for the implementation of this policy, working with school staff in relation to compliance with data protection law, and developing related policies and guidelines where applicable in consultation with the DPO and school staff.

The DPL will provide an annual report on data protection to Business & Finance Committee and, where relevant, report to the Central Governing Board or Business & Finance Committee the advice and recommendations they have received on data protection issues.

The data protection lead will usually be the first point of contact for individuals whose data the Federation or its schools process.

You can contact the DPL via: governors@primaryadvantage.hackney.sch.uk

5.4 Headteachers
Headteachers act as the representative of the data controller on a day-to-day basis.

5.4 All staff
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing their school of any changes to their personal data, such as a change of address
- Contacting the DPL or DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles
The UK GDPR is based on data protection principles that our schools must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Federation aims to comply with these principles.

7. Collecting personal data
7.1 Lawfulness, fairness and transparency
We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school or Federation can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school or Federation can **comply with a legal obligation**

- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school or Federation, as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school or Federation (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school or Federation holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPL or DPO. We will respond in accordance with our subject access procedure, which is in appendix three.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase[1] or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPL or DPO. If staff receive such a request, they must immediately forward it to the DPL or DPO.

Our subject access and educational record procedure is in appendix 3.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

We use CCTV in various locations around school sites to ensure they remain safe. We will adhere to the Government's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the school's Business & Finance Manager.

Our use of CCTV is discussed in more detail in our CCTV policy.

[1] Our right of erasure procedure is in appendix 4.

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Following advice from our DPO, we will seek consent from parents at the following times:

- At the start of reception
- At the start of year three
- At the start of year six
- Whenever a child joins the school

This means that consent is refreshed at least every three years. In addition, when we ask for consent, we will state how long we will use the image for. This will usually be from three to seven years and may include a period after a child has left the school.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our child protection & safeguarding policy and our online safety & acceptable use policy for more information on our use of photographs and videos.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, who may be from outside the Federation, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section six)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our schools and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our online safety & acceptable use policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Our data retention schedule is set out in appendix 1.

16. Personal data breaches

The Federation will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 5.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. Training

All staff and governors are provided with this policy as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Federation's processes make it necessary.

18. Freedom of information

The ICO's Model Publication Scheme is in appendix two of this policy.

Our freedom of information request procedure is in appendix six.

19. Links with other policies

This data protection policy is linked to our:

- CCTV policy
- Child protection & safeguarding policy
- Online safety & acceptable use policy
- Social media & networking policy
- Use of internet & email policy

Appendix 1: Data retention schedule

The data retention schedule was provided by Grow Education Partners, who provide data protection support to the Federation. Some records may not be held.

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
Governors				
Agendas for Governing Body meetings	No		Date of meeting + 10 years	Secure disposal
Records relating to DBS checks carried out on clerk and the members of the governing body	Yes		Date of DBS check + 6 years	Secure disposal
Governor personal files	Yes		Date of appointment ceases + 6 years	Secure disposal
Records relating to the induction programme for new governors	No		Date of appointment ceases + 6 years	Secure disposal
Records relating to the training required and received by Governors	No		Date of appointment ceases + 6 years	Secure disposal
Records relating to the appointment of a clerk to the governing body	Yes		Date of appointment ceases + 6 years	Secure disposal
Records relating to governor declaration of disqualification criteria	No		Date of appointment ceases + 6 years	Secure disposal
Register of business interests	Yes		Date of appointment ceases + 6 years	Secure disposal
Records relating to the election of parent and staff governors not appointed by the governors	Yes		Date of election + 6 months	Secure disposal

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
Record of attendance at full governing Board Meetings	No		Date of Meeting + 6 years	Secure disposal
Correspondence sent and received by the governing body or head teacher	Maybe		Current year + 3 years	Secure disposal
Minutes of Governing Body meetings	Yes		Date of meeting + 10 years	Secure disposal
Principal Set (signed)	No		Permanent	Transfer to archives when the school has closed.
Inspection Copies[2]	No		Date of meeting + 3 years	Secure disposal
Reports presented to the Governing Body	No		Date of report + 6 years	Transfer to archives
Instruments of Government including Articles of Association	No		Permanent	Retain in school. Transfer to Archives when the school has closed.
Trusts and endowments managed by the Governing Body	No		Permanent	Retain in school whilst operationally required. Transfer to archives when the school has closed.
Action plans created and administered by the Governing Body	No		Until superseded or whilst relevant	Secure disposal. It may be appropriate to offer to the Archives.
Policy documents created and administered by the Governing Body	No		Until superseded	Retain in school whilst policy is operational then transfer to archives

[2] These are the copies which the clerk to the Governors may wish to retain so that requestors can view all the appropriate information without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
Records relating to complaints dealt with by the Governing Body	Yes		(i) Major Complaints: Date of resolution of complaint + 6 years (ii) Complaints involving allegations of Negligence: Date of resolution of complaint + 15 years (iii) Complaints involving allegations relating to safeguarding or child protection: Date of resolution of complaint + 40 years	Retain in school for the first six years. Review for further retention in the case of contentious disputes. Secure disposal routine complaints.
Annual Reports required by the Department for Education	No	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171	Date of report + 10 years	Transfer to Archives
Proposals for schools to become, or be established as Specialist Status schools	No		Current year + 3 years	Transfer to Archives
Executive Principal, Head Teachers and Senior Management Team				
Log books of activity in the school maintained by the Headteacher	Yes		Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the County Archives Service if appropriate

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	Yes		Date of the meeting + 3 years then review	Secure Disposal. These could be of permanent historical value and should be offered to the County Archives Service if appropriate
Reports created by the Head Teacher or the Management Team	Yes		Date of the report + a minimum of 3 years then review	Secure Disposal. These could be of permanent historical value and should be offered to the County Archives Service if appropriate
Records created by EP, head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes		Current academic year + 6 years then review	Secure Disposal
Correspondence created by EP, head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes		Date of correspondence + 3 years then review	Secure Disposal
Professional Development Plans	Yes		Life of the plan + 6 years	Secure Disposal
Federation/School Development Plans	No		Life of the plan + 3 years	Secure Disposal
School Privacy notice which is sent to parents and pupils	Yes		Until superseded + 6 years	

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
Admissions Process				
All records relating to the creation and implementation of the School Admissions Policy	No		Life of the policy + 3 years then review	Secure Disposal
Admissions – if the admission is successful	Yes		Date of Admission + 1 Year	Secure Disposal
Admissions – if the appeal is unsuccessful	Yes		Resolution of case + 1 year	Secure Disposal
Admissions – Secondary Schools – Casual – if offer is accepted	Yes		Current Year + 1 Year	Secure Disposal
Admissions – Secondary Schools – Casual – if offer is declined	Yes		Retain for 3 months	Secure Disposal
Proof of address supplied by parents as part of the admissions process	Yes		Current year + 1 year	Secure Disposal
Supplementary Information form including additional information such as religion, medical conditions etc.	Yes		Current year + 1 year	Secure Disposal
Register of Admissions	Yes		Every entry must be preserved for 3 years from the point of entry.	Secure Disposal
For successful admissions	Yes		This information should be added to the pupil file	Secure Disposal
For unsuccessful admissions	Yes		Until appeals process completed.	Secure Disposal

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
Operational Administration				
General file series	No		Current year + 5 years then review	Secure disposal
Google Forms used to attain data from pupils or staff.	No		6 months then Review	Secure disposal
Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	Standard disposal
Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	Standard disposal
Newsletters and other items with a short operational use	No		Current year + 1 year	Standard disposal
Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	Secure disposal
Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	Secure disposal
Recruitment				
All records leading up to the appointment of a new EP/headteacher	Yes		Date of appointment + 6 years	Secure disposal
All records leading up to the appointment of a new member of	Yes		Date of appointment of successful candidate + 6 months	Secure disposal

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
staff – unsuccessful candidates				
All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	Secure disposal
Pre-employment vetting information – DBS checks for successful candidates	No	DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education) Sections 73, 74	Application forms and references and other documents for the duration of the employees employment + 6 years	Secure disposal
Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file	Secure disposal
Pre-employment vetting information – Evidence proving the right to work in the United Kingdom	Yes	An employer's guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that	Secure disposal

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
			the documents are kept for termination of Employment plus not less than 2 years	
Operational Staff Management				
Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	Secure Disposal
Timesheets	Yes		Current year + 6 years	Secure Disposal
Annual appraisal/assessment records	Yes		Current year + 6 years	Secure Disposal
Staff Training-where training related to children (e.g. safeguarding or other child related training)	Yes		Date of Training + 40 years	Secure disposal
Staff Training-where training leads to continuing professional development	Yes		Length of time required by the professional body	Secure disposal
Sickness and absence monitoring	Yes		Current Year + 3 Years	Secure disposal
Management of Disciplinary and Grievance Processes				
Allegation of a child protection nature against a member of staff including where the allegation is unfounded	Yes	"Keeping children safe in education 2021"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children 2018"	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then review. Note allegations that are found to be malicious should be removed from personnel	Secure disposal

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
			files. If found they are to be kept on the file and a copy provided to the person concerned	
Disciplinary Proceedings				
Oral warning	Yes		Date of warning + 6 months	Secure disposal
Written warning – level 1	Yes		Date of warning + 6 months	Secure disposal
Written warning – level 2	Yes		Date of warning + 12 months	Secure disposal
Final warning	Yes		Date of warning + 18 months	Secure disposal
Case not found	Yes		If the incident is child protection related then see above, otherwise dispose of at the conclusion of the case	Secure disposal
Health and Safety				
Health and Safety Policy Statements	No		Life of policy + 3 years	Secure disposal
Health and Safety Risk Assessments	No		Life of risk assessment + 3 years	Secure disposal
Accident reporting records relating to those under/over the age of 18	Yes		Accident book: 3 years after the last entry of the book.	Secure disposal
Records relating to any reportable death injury, disease or dangerous occurrence.	Yes		Date of Incident +3 years	Secure disposal
Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11;	Date of Incident + 40 years	Secure disposal

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
		Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)		
Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	Secure disposal
Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	Secure disposal
Fire Precautions log books	No		Current year + 3 years	Secure disposal
Payroll and Pensions				
Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	Secure disposal
National Insurance schedule of payments	Yes		Current Year + 6 years	Secure disposal
Income tax form P60	Yes		Current year + 6 years	Secure disposal
Absence Record	Yes		Current year + 3 years	Secure disposal
Records held under Retirement Benefits	Yes		Current year + 6 years	Secure disposal

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
Schemes (Information Powers) Regulations 1995				
Risk Management and Insurance				
Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	Secure disposal
Asset Management				
Inventories of furniture and equipment	No		Current year + 6 years	Secure disposal
Burglary, theft and vandalism report forms	No		Current year + 6 years	Secure disposal
Accounts and statements including budget management				
Annual Accounts	No		Current year + 6 years	Secure disposal
Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then review	Secure disposal
Student Grant applications	Yes		Current year + 3 years	Secure disposal
All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No		Life of the budget + 3 years	Secure disposal
Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	Secure disposal
Records relating to the collection and banking of monies	No		Current financial year + 6 years	Secure disposal

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
Pupil Premium Fund Record	Yes	Limitations Act 1980	Date the pupil leaves the provision + 6 years	Secure disposal
Records relating to the identification and collection of debt	No		Current financial year + 6 years	Secure disposal
Records Related to Gift Aid	No		Current financial year + 6 years	Secure disposal
Contract Management				
All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	Secure Disposal
All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	Secure disposal
Records relating to the monitoring of contracts	No		Current year + 6 years or 12 years	Secure disposal
School Fund				
School Fund - Cheque books	No		Current year + 6 years	Secure disposal
School Fund - Paying in books	No		Current year + 6 years	Secure disposal
School Fund – Ledger	No		Current year + 6 years	Secure disposal
School Fund – Invoices	No		Current year + 6 years	Secure disposal
School Fund – Receipts	No		Current year + 6 years	Secure disposal
School Fund – Bank Statements	No		Current year + 6 years	Secure disposal
School Fund – Journey Books	No		Current year + 6 years	Secure disposal
School Meals Management				
Free School Meals Registers	Yes		Current year + 6 years	Secure disposal
School Meals Registers	Yes		Current year + 3 years	Secure disposal

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
School Meals Summary Sheets	No		Current year + 3 years	Secure disposal
Property Management				
Title deeds of properties belonging to the Federation/school	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry	NA
Plans of property belong to the Federation/school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold	NA
Leases of property leased by or to the school	No		Expiry of lease + 6 years	Secure disposal
Records relating to the letting of Federation/school premises	No		Current financial year + 6 years	Secure disposal
Maintenance				
All records relating to the maintenance of the school carried out by contractors	No		These should be retained whilst the building belongs to the school and should be passed to any new owners of the building is leased or sold.	Secure disposal
All records relating to the maintenance of the school carried out by school employees including maintenance log books	No		These should be retained whilst the building belongs to the school and should be passed to any new owners of the building is leased or sold.	Secure disposal

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
Pupil's Educational Record				
Pupil's Educational Record	Yes	The Education (Pupil information) (England) Regulations 2005 SI 2005 No. 1437	NA – transfer to new school	NA
Secondary	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	Secure disposal
Examination Results – Pupil Copies: Public	Yes		This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
Examination Results – Pupil Copies: Internal	Yes		This information should be added to the pupil file	Secure disposal
Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	Secure disposal
Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of	Secure disposal

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
		welfare of children March 2015"	this information will be found on the Local Authority Social Services record	
Attendance				
Attendance Registers	Yes		Date of register + 3 years	Secure disposal
Correspondence relating to authorized absence	Yes	Education Act 1996 Section 7	Current academic year + 2 years	Secure disposal
Special Educational Needs				
Special Educational Needs files, reviews and Individual Education Plans	Yes	Children and Family's Act 2014 Special Educational Needs	Date of birth of the pupil + 31 years	NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.
Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 31 years [This would normally be retained on the pupil file]	Secure disposal unless the document is subject to a legal hold

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 31years [This would normally be retained on the pupil file]	Secure disposal unless the document is subject to a legal hold
Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 31 years [This would normally be retained on the pupil file]	Secure disposal unless the document is subject to a legal hold
Statistics and Management Information				
Curriculum Returns	No		Current year + 3 years	Secure disposal
Examination Results (Schools Copy)	Yes		Current year + 6 years	Secure disposal
Published Admission Number (PAN) Reports	Yes		Current year + 6 years	Secure disposal
Value Added and Contextual Data	Yes		Current year + 6 years	Secure disposal
Self Evaluation Forms	Yes		Current year + 6 years	Secure disposal
Implementation of Curriculum				
Schemes of Work	No		Current year + 1 years	It may be appropriate to review these records at the end of each year and allocate a further retention period or Secure Disposal
Timetable	No		Current year + 1 years	Standard disposal
Class Record Books	No		Current year + 1 years	Standard disposal
Mark Books	No		Current year + 1 years	Standard disposal
Record of homework set	No		Current year + 1 years	Standard disposal

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	Secure disposal
Educational Visits outside the Classroom				
Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	Secure disposal
Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.
Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that	Secure disposal

Basic file description	Personal information	Statutory Provisions (if any)	Retention period	Action at the end of the administrative life of the record
			the rules had been followed for all pupils	
Walking Bus				
Walking Bus Register	Yes		Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	Secure disposal [If these records are retained electronically any backup copies should be destroyed at the same time]
Local Authority				
Attendance Returns	Yes		Current year + 1 year	Secure disposal
School Census Returns	No		Current year + 5 years	Secure disposal
Circulars and other information sent from the Local Authority	No		Operational use	Secure disposal
Central Government				
OFSTED reports and papers	No		Life of the report then review	Secure disposal
Returns made to central government	No		Current year + 6 years	Secure disposal
Circulars and other information sent from central government	No		Operational use	Secure disposal

Information Commissioner's Office

Appendix 2: ICO model publication scheme

Model publication scheme

Freedom of Information Act

This model publication scheme has been prepared and approved by the Information Commissioner. It may be adopted without modification by any public authority without further approval and will be valid until further notice.

This publication scheme commits an authority to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by the authority. Additional assistance is provided to the definition of these classes in sector specific guidance manuals issued by the Information Commissioner.

The scheme commits an authority:

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the authority and falls within the classifications below.
- To specify the information which is held by the authority and falls within the classifications below.
- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.
- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- To review and update on a regular basis the information the authority makes available under this scheme.
- To produce a schedule of any fees charged for access to information which is made proactively available.
- To make this publication scheme available to the public.
- To publish any dataset held by the authority that has been requested, and any updated versions it holds, unless the authority is satisfied that it is not appropriate to do so; to publish the dataset, where reasonably practicable, in an electronic form that is capable of re-use; and, if any information in the dataset is a relevant copyright work and the public

authority is the only owner, to make the information available for re-use under the terms of the Re-use of Public Sector Information Regulations 2015, if they apply, and otherwise under the terms of the Freedom of Information Act section 19.
The term 'dataset' is defined in section 11(5) of the Freedom of Information Act. The term 'relevant copyright work' is defined in section 19(8) of that Act.

Classes of information

Who we are and what we do.
Organisational information, locations and contacts, constitutional and legal governance.

What we spend and how we spend it.
Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.

What our priorities are and how we are doing.
Strategy and performance information, plans, assessments, inspections and reviews.

How we make decisions.
Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.

Our policies and procedures.
Current written protocols for delivering our functions and responsibilities.

Lists and registers.
Information held in registers required by law and other lists and registers relating to the functions of the authority.

The services we offer.
Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

The method by which information published under this scheme will be made available

The authority will indicate clearly to the public what information is covered by this scheme and how it can be obtained.

Where it is within the capability of a public authority, information will be provided on a website. Where it is impracticable to make information available on a website or when an individual does not wish to access the information by the website, a public authority will indicate how information can be obtained by other means and provide it by those means.

In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where an authority is legally required to translate any information, it will do so.

Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

Charges which may be made for information publishedunder this scheme

The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by the authority for routinely published material will be justified and transparent and kept to a minimum.

Material which is published and accessed on a website will be provided free of charge.

Charges may be made for information subject to a charging regime specified by Parliament.

Charges may be made for actual disbursements incurred such as:

- photocopying
- postage and packaging
- the costs directly incurred as a result of viewing information

Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public.

Charges may also be made for making datasets (or parts of datasets) that arerelevant copyright works available for re-use. These charges will be in accordance with the terms of the Re-use of Public Sector Information Regulations 2015, where they apply, or with regulations made under section 11B of the Freedom of Information Act, or with other statutory powers of the public authority.

If a charge is to be made, confirmation of the payment due will be given beforethe information is provided. Payment may be requested prior to provision of the information.

Written requests

Information held by a public authority that is not published under this schemecan be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.

Appendix 3: Subject access & education record request procedure

This procedure is based on guidance on Subject Access Requests (SAR) produced by the Information Commissioner's Office (ICO). We have also used resources from The Key Support Services Limited and Grow Education Partners.

1. Subject access requests and education record requests

SARs should not be confused with educational record requests. The latter give those with parental authority the right to request access to their child's education record. People are entitled to a much wider range of material under a SAR, which is why the bulk of this procedure is devoted to that. It is highly likely that a SAR for all of a child's personal data would include everything in their education record.

The procedure for educational record requests is set out in section 8.

2. Subject Access Request Rights

Individuals have the right to obtain:

- Confirmation that their data is being processed
- A copy of their personal data.

Neither the General Data Protection Regulation 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 "subject access request" or "Article 15".
- Requester just needs to make it clear they want a copy of their personal data.
- Can come from a third party on behalf of the data subject.
- Can come from a joint controller or outsourced processor that you work with.

Key Principles:

- Communicate with the requester to establish what they want, especially with "all data access request".
- Log and document the process for posterity.
- Present the data as clearly as possible which shows how you have responded to the request.

Rights of Children:

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at the Federation and its schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

3. Third Party Requests

An individual other than the data subject can submit a SAR. Staff should note that most commonly this is utilised by solicitors working on behalf of an individual.

These third parties would need written authorisation from the individual to act on their behalf.
If there are any doubts regarding their authority, then we will contact the data subject directly to confirm.

4. Full refusal to comply with a request

We 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 access. 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 the organisation with no real purposes other than to cause disruption. For example:
    I. The individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
    II. The request makes unsubstantiated accusations against the Federation or its schools or specific employees;
    III. The individual is targeting a particular employee against whom they have some personal grudge; or
    IV. The individual systematically sends different requests to the Federation or its schools 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 manifestly unfounded. We should consider if we 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 information, even if we might find the request burdensome. Instead, we should consider asking them for more information to help them locate what they want.
- Wanted to receive a further copy of information they have requested previously. In this situation we can charge a reasonable fee for the administrative costs of providing this information again and it is unlikely that this would be an excessive request;
- Made an overlapping request relating to a separate set of information; or
- Previously submitted requests which have been manifestly unfounded or excessive.

When deciding whether a reasonable interval has elapsed we will consider:

- The nature of the data – this could include whether it is particularly sensitive;
- The purposes of the processing – these could include whether the processing is likely to cause detriment (harm) to the requester if disclosed; and
- How often the data is altered – if information is unlikely to have changed between requests, we may decide you do not need to respond to the same request twice. However, if we have deleted information since the last request we will inform the individual of this.

Always consider when refusing data that we will have to be able to demonstrate to the individual and ICO why we have made that decision.

5. Receiving a Subject Access Request

On receipt of a confirmed or potential SAR, the staff member or data processor must immediately notify the finance & admin manager or the cluster finance & admin at their school and the Federation's governance manager. They will make a decision whether to refer the matter to the Data Protection Officer (DPO), who is Hassan Muzammal at Grow Education Partners (Hassan.Muzammal@london.anglican.org).

When a SAR is received it will be immediately entered onto the subject access request log and given a reference number, which will be used to discuss the SAR. The log will record the who, when, what, and why of the process. A central log for the Federation will be held by the governance manager so that we are able to monitor requests that come to multiple schools and respond in a consistent fashion. Schools may keep their own logs as well.

Additionally, a folder will be created under the reference number and all associated documentation regarding the SAR 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 broken down into four distinct sections: acknowledgment, collection, review, response.

No data should be deleted to pre-emptively prevent it from being released, this is illegal. In all likelihood it can be reviewed.

6. Timeframe of Response

The Data Protection Act 2018 gives a timeframe of one calendar month from the date of receipt, for responding to a SAR. 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.

Schools cannot claim additional time to complete a SAR just because it arrives or is due during the school holidays, although it may be necessary to extend the response period. This is in accordance with article 12(3) of the GDPR and will be the case where the request is complex, for example, where we need multiple staff to collect the data. Individual schools should put in place processes for dealing with this. Requests made to the Federation centrally will be dealt with by staff who are on 52-week contracts.

7. Stage 1: Acknowledgment:

We will send a formal acknowledgement to confirm that:

- A SAR has been received.
- The date of receipt.
- What we believe the SAR is regarding.
- Whether anything further is needed from the data subject i.e. clarification or refinement of the SAR, ID for verification.
- The timeframe for a response.
- How the requester would like to/will receive the data i.e. paper pick up, paper posting, electronic sending.

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

A template acknowledgement response is attached at appendix 2.

Content of SAR

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”, we should ask for further refinement to allow us to respond efficiently to the request within the timeframe.

ID Verification

It is important that you are satisfied that the request is genuine, and the individual is who they say they 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 the acknowledgment.

If we believe we cannot respond within the one calendar month timeframe, then we 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 Federation or school.

8. Stage 2 Collection
This is where the data that has been requested is collated and stored ready for review, this can be done in either an electronic or paper format. Which is more efficient will vary depending on what has been requested and how it has been requested it. i.e. what format the original copy of the data is in and how it is to be sent.

Using the confirmed requested content of the SAR, you should work down the list and point for point collect the data.

It is recommended that someone who has an appropriate level of authority is selected to collect the data requested.

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 etc.
c) What outsourced processors need to be contacted.

Contacting Outsourced processors
If the some of the requested data is being held by an outsourced processor, then they would need to be contacted to inform them of the SAR and that their assistance is needed. If they are a joint controller, such as the council or social services, it may be applicable to inform them that you have had a SAR and they may expect one shortly as well, as you cannot make the decision yourself to release the data.

Collection of Emails
If the request involves emails and their contents i.e. all emails which contain my name Jo Bloggs. Then we will either:
a) Contact all staff to ask for them to forward these emails; or
b) Use IT support to run a mass email search remotely.

In either case, we will advise staff beforehand so they can pre-emptively contact the person putting the SAR response together if they think the emails may present a problem.

During the collection and review 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.

9. Stage 3 Review
It is recommended this part of the process is undertaken by the Headteacher and or DPO as this is where the collected data is reviewed, and items are removed or redacted. Therefore, the person making the decision should have the authority to do so.

The DPA 2018 states you need not have to comply with a request in full or aspects if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

Items would include:
- Names of other data subjects.
- Email addresses of other data subjects.
- Data relating to other data subjects i.e. where the individual forms part of a bigger data set; exam results, class lists.
- Items which could cause emotional or physical harm or distress to the data subject or other data subjects.

This is not an exhaustive list and it is very much a case by case basis of what could and should be released. This should not be done remotely without seeing the item. It is worth noting that anything which is removed needs to be justified in the response. In addition, if names and emails are redacted for one individual because consent is not given and others are, this may create a disparity which will need explaining.

How the redaction occurs is dependent on the format it is presented in, paper redaction can be done by marker pen, tippex and then photocopying. If the items are in an electronic format, then you can highlight in black and print them out or use the Acrobat Reader Pro redaction function. Please note, if you are sending the information electronically, then don't redact the document in a way that can be reversed.

A copy of both what is and what is not supplied in the response should be kept in the file for posterity.

10. Stage 4: Response

This is where in a formal correspondence you explain the process and result of collection and review process to the data subject and present them with the information. It should include:
- What and where was searched to comply with the request, e.g. paper records, SIMS, emails, CPOMS.
- Reconfirm what was asked for.
- What is being supplied.
- What is not being supplied and why.
- Why items have been redacted e.g. removing any information which would identify any data subjects other than themselves.
- Ability to discuss this further with the school.
- Right to refer to the ICO and contact details.

N.B. When supplying the data, it must be in an understandable format. Therefore, it is recommended to explain what is what and why. Go point for point with what was requested and what has and has not been supplied. We will label what the individual items are so a layman could understand it.

A template response is attached at appendix 3.

11. Education record requests

Those with parental authority have the right to request to view their child's education record under The Education (Pupil Information) (England) Regulations 2005. Unlike an SAR, this right sits with parents rather than children.

What is the education record?

The ICO defines the education record as:
"An education record covers information that comes from a teacher or other employee of a local authority or school, the pupil or you as a parent, and is processed by or for the school's governing body or teacher. This is likely to cover information such as; the records of the pupil's academic achievements as well as correspondence from teachers, local education authority employees and educational psychologists engaged

by the school's governing body. It may also include information from the child and from you, as a parent, carer or guardian. Information provided by the parent of another child or information created by a teacher solely for their own use would not form part of a child's education record."[3]

Processing requests

Requests will be processed in the same way as SARs, following the procedure set out above, with the following exceptions:

- Requests can only be made by those with parental authority for the records of their own children. We may not fulfil a parent's request for these records if there is a court order in place which limits their exercise of parental responsibility.
- The deadline for responding is 15 school days.
- We can refuse to provide anything that we couldn't lawfully be given under the Data Protection Act 1998. This includes material which may cause serious harm to the physical or mental health or condition of the pupil or someone else. We will also withhold anything where it would mean releasing examination marks before they are officially announced.
- References to the ICO should not be included in any correspondence as it does not regulate education record requests. Any complaints about how we have processed an education record request will be dealt with under the Federation's complaints procedure.

[3] https://ico.org.uk/your-data-matters/schools/pupils-info/

Appendix 1 of the subject access request & education record request procedure: Subject access request template

Dear sir/ madam,

Please provide me with the information about me that I am entitled to under the UK General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing. Here is the necessary information:

Your name:	
Name of the school:	
Your relationship with the school:	*Please select:* *Pupil / parent / employee / governor / volunteer* *Other (please specify):*
Correspondence address:	
Contact number:	
Email address:	
Details of the information requested:	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* › *My personnel file.* › *My child's medical records.* › *My child's behaviour record and who it's held by.* › *Emails between specific people and the dates involved.*

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that, in most cases, you must supply me with the information within one month and free of charge.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,

Please return this request to your school office or email it to governors@primaryadvantage.hackney.sch.uk

Appendix 2 of the subject access request & education record request procedure: acknowledgement template

This is a simple template for acknowledging SARs that can be put in a letter or emailed.

Dear [name],

Re: your subject access request

I can confirm that [school name] received your request on [date] to see the following data that we hold about you:
[Summarise the data requested]

[Please ask for any clarification that you need.]

I am proposing to provide the information by [insert method: email/ paper etc.]. Please let me know if that will cause you any difficulties.

If you expect to respond within 1 month, insert:
We will respond to your request within one month, as required under the UK General Data Protection Regulation (UK GDPR).

We don't think we will need to extend the response time, which we're able to do when requests are complex. However, if it becomes clear that we do need to extend the response period by up to two months, we will let you know by [date – this will be 1 month from when you received the request].

If you think the request is too complex to respond within 1 month, insert:
In most cases, we will respond to subject access requests within one month, as required under the UK General Data Protection Regulation (UK GDPR). However, under article 12 (3), we are able to extend this period by up to 2 months for complex requests.

We anticipate that your request will be too complex for us to fulfil within one month.
In particular, [insert more details to explain why you have judged that this request is too complex].

We will respond to your request by [date – which will be 3 months from the date the request was received] at the latest.

If you disagree with this decision, you can contact the Information Commissioner's Office by calling 0303 123 1113, or going to the following webpage: https://ico.org.uk/global/contact-us/

We are sorry for any inconvenience this may cause you.

If we have asked you to prove your identity, the time period for fulfilling the subject access request doesn't start until we have seen this.

Yours sincerely,

[Name]

Appendix 3 of the subject access request & education record request procedure: response template

Dear [insert the name of the individual who submitted the subject access request]
Please find enclosed the information that you requested under the UK General Data Protection Regulation (UK GDPR).

Your name	[Insert requester's name]
Your relationship with the school	[Pupil / parent / employee / governor / volunteer / other (specify)]
Details of the information you requested/enclosed and, where applicable, the reasons for refusing to provide it	[Insert details of the specific information requested, such as: › *My personnel file.* › *My child's medical records.* › *My child's behaviour record and who it's held by.* › *Emails between specific people and the dates involved.*
Date you requested the information	[Insert date]
Date we supplied the information	[This must be within one month of the above date, except in the case of an extension or delay, e.g. in receiving ID]
Format we supplied the information	[For example, encrypted USB stick accompanying this letter]

If you need any further advice relating to your subject access request, you can contact the Federation's governance manager via: governors@primaryadvantage.hackney.sch.uk or the school finance & admin manager via [email address]

Yours sincerely,

[Name]

Appendix 4: Right of erasure request procedure

This procedure is based on guidance on requests for erasure (RFE) produced by the Information Commissioner's Office (ICO). We have also used resources from The Key Support Services Limited.

1. Requests for Erasure

Individuals have the right to invoke a request that their personal data is 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 (i.e. in breach of the lawfulness requirement of the first principle).
- You have to do it to comply with a legal obligation.
- You have processed the personal data to offer information society services to a child.

Neither the General Data Protection Regulation (GDPR) nor the Data Protection Act (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".
- The requester just needs to make it clear if they want their data erased, deleted, anonymised or "to be forgotten".
- It can come from a third party you share data with.

2. Key principles

Anything you legally must retain, do not and should not be erased, such as safeguarding files.

Someone cannot blanket withdraw consent. If you ask for it in a granular format, it needs to be withdrawn in a 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.

3. 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 third 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. Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of an erasure request. Therefore, most requests from parents or carers of pupils at the Federation and its schools may be granted without the express

permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

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.
- Any views the child or young person has on whether their parents should have access to information about them.

4. Third party requests

An individual other than the data subject can submit a request for erasure (RFE). Most commonly this is utilised by solicitors working on behalf of an individual. These third 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.

5. Full refusal to comply with a request

There are some situations when we can refuse to comply with a request in full.

Manifestly unfounded

This is where:

- 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.
- 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 the Federation, one or more of its schools or specific employees.
- The individual is targeting a particular employee against whom they have some personal grudge.
- The individual systematically sends different requests 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.

We must consider if we can prove if the individual genuinely wants to exercise their rights or not.

Excessive

This is where:

- The RFE repeats the substance of previous requests and a reasonable interval has not elapsed.
- 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.
- Previously submitted requests which have been manifestly unfounded or excessive.

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

6. Receiving a request for erasure

On receipt of a confirmed or potential RFE, the staff member or data processor must immediately notify the finance & admin manager or the cluster finance & admin at their school and the Federation's governance manager. They will make a decision whether to refer the matter to the Data Protection Officer (DPO), who is Hassan Muzammal at the LDBS (Hassan.Muzammal@london.anglican.org).

When an RFE is received it will be entered onto the freedom of information log and given a reference number. In all future communications this reference number should be used to discuss the RFE. The log will record the who, when, what, and why of the process.

Additionally, a folder will 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 broken down into four distinct sections: acknowledgment, search, review & erase, response.

7. 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 17 July, deadline 17 August.

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 31 January, deadline 28 February.

8. Stage 1: Acknowledgment

We will send a formal acknowledgement to confirm that:

- An RFE has been received.
- The date of receipt.
- What we 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 will generally be sent electronically.

What the RFE is regarding

It is important to state verbatim what the individual has requested and give them the opportunity to confirm that we 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 to seek further refinement to allow us to respond efficiently to the request within the timeframe.

ID verification

It is important that we are satisfied that the request is genuine, and the individual is who they say there are, as we must not release information to an incorrect recipient. Therefore, if we are unsure, we will 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 we have requested further clarification or ID verification, the clock does not start until this is received. This will be explained in our acknowledgment.

If we believe we cannot respond within the one calendar month timeframe, then we 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, which is why refining “all data” requests is beneficial for both the requester and the school.

9. Stage 2: Search & review

Using the confirmed requested erasure of the RFE, we will work down the list 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:

- Understand what data is being held on individuals.
- Where it is being held: management software, filing cabinets etc.
- What third party processors need to be contacted.

Contacting third party processors

We are required to inform our 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, we must contact each one to inform them of the erasure request. If there are too many of them, then we just need to inform the requester who they are and what has been shared.

Erasure

The DPA 2018 states we 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.

- 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

During the search & review and 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.

10. Stage 3: Collect and erase

It is recommended this part of the process is done 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 we 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 the justification table, it is recommended to carry out the collection and erasure/anonymisiation of any data selected.

11. Stage 4: Final response

This is where in a formal correspondence we explain the process and result of the Search & review and 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 is not 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.

We 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.

Appendix 5: Data protection breach procedure

This procedure is based on guidance on Freedom of Information Requests (FOI) produced by the Information Commissioner's Office (ICO). We have also used resources from The Key Support Services Limited and Grow Education Partners.

1. Breach notification

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the finance & admin manager or the cluster finance & admin at their school and the Federation's governance manager. They will make a decision whether to refer the matter to the Data Protection Officer (DPO), who is Hassan Muzammal at Grow Education Partners (Hassan.Muzammal@london.anglican.org).

Irrespective of whether the DPO is notified or not, the response to the breach will follow the same path and be broken down into four distinct sections: investigation, recovery, reporting, remedial action.

Investigation, recovery and reporting must be done within 72 hours of breach realisation. This is the period of time which Data Protection Act 2018 allows for referral to the ICO or data subjects.

2. Stage 1: Investigation

This is an investigation into the breach report to determine whether a breach has occurred by deciding if personal data has been accidentally or unlawfully mishandled. This will be done by assessing whether the data has been:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

Once a breach has been confirmed then the severity of it will be assessed by considering:

- Data subject affected and their vulnerability
- Number of data subjects affected.
- Data type lost, personal identifying/ special category
- Specific data sets lost
- Number of data sets
- Format of data, electronic/paper

Once a breach has been confirmed, it will be entered onto the data breach log and assigned a unique reference number. All subsequent information will then be recorded on this log.

In addition, a file should be opened named after the unique reference number. All articles relating to the investigation, recovery and reporting should be stored within this file.

Staff and governors must cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

3. Stage 2: Recovery

The next stage is to contain and minimise the impact of the breach. This will be assisted by relevant staff members or data processors where necessary.

This may include but not be limited to:

- Contacting parties who may have received the data.

- Email Recovery.
- Backup file restoration.
- Requesting deletion of data.

If the data has been sent to the wrong individual and it has been requested to be deleted, confirmation of deletion should be attained in a written format for posterity.

The success or failure of the recovery must be recorded and will inform the action in the next stage.

4. Stage 3: Reporting

The investigator must decide who should be informed about the breach: affected data subjects and/or the ICO. Depending on the result of the containment efforts, the investigator will review the potential consequences, assess their seriousness and likelihood then make a decision about who needs to be informed.

If the risk of damage is high, the data subjects will be promptly informed, in writing. This means all individuals whose personal data has been breached. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach.
- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

The decision on whether to contact individuals will be documented.

Whether the breach must be reported to the ICO will be judged on a case-by-case basis.

To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorized reversal of pseudonymization (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The decision will be documented either way in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the GDPR section of Fedshare.

Where the ICO must be notified, this will be done via the report a breach page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO will set out:

- If all the above details are not yet known, then as much as is known should be reported to the ICO within 72 hours. The report will explain if there is a delay, the reasons why, and when the further information is expected to be known. Then the remaining information will be submitted as soon as possible

5. Stage 4: Remedial Action

Finally, the breach will be assessed and potential future actions considered on how to prevent a similar breach reoccurring.

Such actions include, but are not limited to:

- Anonymising and minimising data
- Encrypted drives
- Secure access servers
- Strong password setting
- Training and support for staff and governors
- Encrypted email

All data breaches will be reported to governors via a written report to Business & Finance Committee to brief them the outcome and propose ways it can be prevented from occurring again. This is to allow governors to hold the Federation and its schools accountable as per the GDPR Principle of accountability.

Data breach procedure appendix 1: Remedial action when sensitive information has been disclosed via email (including safeguarding records)

Staff should take the following actions when sensitive information has been disclosed via email:

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the school's IT support provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence).
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its three local safeguarding partners.

Appendix 6: Freedom of information request procedure

This procedure is based on guidance on Freedom of Information Requests (FOI) produced by the Information Commissioner's Office (ICO). We have also used resources from The Key Support Services Limited and Grow Education Partners.

Freedom of Information Request Rights

Members of the public have the right to attain any recorded information held by public authorities through:

- Publishing of certain information about their activities.
- Requesting specific information.

The reasoning behind this is that they spend money collected from taxpayers and make decisions that can significantly affect many people's lives.

Being able to access information helps the public hold authorities accountable for their actions and allows public debate to be better informed and more productive.

This guide will focus only on the specific information requests, guidance on what information should be published can be found in the ICO's model publication scheme.

What is a valid request?

The Freedom of Information Act defines what constitutes a valid request.

- Must be in written format.
- Does not have to include the phrase "Freedom of Information Act".
- Requester needs to include their real name.
- Must contain an address for correspondence either electronic or paper i.e. email address is fine.
- Describe the information they have requested.

If the request is made incorrectly, then we will follow good practice by drawing it to their attention how to make a valid request.

Key principles

We will follow four key principles:

- Everybody has the right to access official information, disclosure should be the default. Be as open with information as much as possible.
- Requesters do not need to justify why they want the information, but we have to justify why we are refusing a request.
- All requests should be treated equally, regardless of the requester be it journalists, parents, local residents, foreign nationals.
- If we have released information, treat it like we have told the world.

Public authorities

As state schools such as those in the Federation receive money from the central government and the local authority they are regarded as public authorities who are required to comply with FOIs.

Requesters

Anyone can make a request. They don't have to be UK citizens or residents. They also do not need to be an individual. Organisations like a company, newspaper or campaign group can make a request.

Repeated Requests:
Section 14(2) of the Freedom of Information Act (FOIA) advises that authorities can refuse a request that is "identical" or "substantially similar" to a previous request to the same individual. This is why we will ascertain the identity of the individuals who make request. We will consider:

- When we previously provided the requester with the information or confirmed that it was held.
- Identical means “scope and wording precisely match”
- Substantially similar “wording is different but the scope is the same or “wording is different but the scope does not differ significantly.”
- The length of interval between the requests can affect the scope, has the information changed since the last request?

Vexatious/manifestly unreasonable requests

Section 14(1) of the Freedom of Information Act (FOIA) advises that authorities can refuse a request as being vexatious or manifestly unreasonable. We will take the following into account when considering whether to refuse a request on these grounds:

- This should only be used in the most extreme of circumstances.
- If the request is “patently unreasonable” or “objectionable.”
- Is it likely to cause disproportionate or unjustified levels of disruption, irritation or distress.
- Objectively value impact on authority vs purpose & value of request.
- Take into account the history of the request or requests.

Staff must consider when refusing a request that they have to be able to demonstrate to the individual and ICO why they have made that decision.

2. Receiving a Freedom of Information Request

On receipt of a confirmed or potential FOI, the staff member or data processor must immediately notify the finance & admin manager or the cluster finance & admin at their school and the Federation’s governance manager. They will make a decision whether to refer the matter to the Data Protection Officer (DPO), who is Hassan Muzammal at Grow Education Partners (Hassan.Muzammal@london.anglican.org).

When a FOI is received it will be entered onto the freedom of information log and given a reference number. In all future communications this reference number should be used to discuss the FOI. The log will record the who, when, what, and why of the process.

Additionally, a folder will be created under the reference number and all associated documentation regarding the FOI 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 broken down into four distinct sections: acknowledge, assess, collate, response

3. Timeframe of Response

The Freedom of Information Act 2000 gives a timeframe of 20 school days or 60 working days, whichever is shorter. Working days being any day other than Saturday, Sunday or Public Holidays.

Individual schools should put in place processes for dealing with FOIs received during the holidays. Requests made to the Federation centrally will be dealt with by staff who are on 52-week contracts.

4. Stage 1: Acknowledgment

We will send a formal acknowledgement to confirm that:

- An FOI has been received.
- The date of receipt.
- What we believe the FOI is regarding.
- Whether anything further is needed from the data subject, such as clarification or refinement of the FOI or their real name.
- The timeframe for a response.
- How we are proposing to send the data in response.

The acknowledgement will be sent electronically or in paper format.

Content of FOI
It is important that we state verbatim what the individual has requested and give them the opportunity to confirm that we have understood the request correctly. This will save wasted time collecting information which is not required.

Clarification or refinement
If a request is received which asks for a large amount of information, we will usually seek further refinement to allow us to respond efficiently to the request within the timeframe.

Timeframe for response
We will explain how we have calculated the deadline for the response, especially if it is affected by the school holidays.

5. Stage 2: Assess

We will assess whether we practically or legally can respond to the request through five tests. Some of these tests are best undertaken by the school, others by someone objective to the situation.

Test 1: Do you hold the information?
We cannot supply something we don't have. Therefore, we will work out if this is information that we hold.

Test 2: Is the information an absolute exemption?
There are several categories of information which a public authority does not need to supply from a FOI because they are an absolute exemption.

Therefore, we will assess whether the information requested falls under one of these exemptions, the most common being:

- Section 21: Information reasonably accessible to the applicant by other means e.g. an Ofsted report which is already on the website.
- Section 32: Court, Inquiry or arbitration records e.g. Results of a recent court case.
- Section 40 (1): Personal information where the requester is a data subject e.g. request for their own data.
- Section 40 (2) Personal information where the applicant is a third party e.g. request for someone else's data.

If the individual is asking for their own personal data, then we will treat this as a subject access request under the Data Protection Act 2018 and inform the requester of the change.

Test 3: Public Interest Test
The next test is to see if the information is falls under an exemption which requires a follow up public interest test. In this case we will assess whether the information requested falls under one of these exemptions, and if it does, undertake a public interest test. The most common will be:

- Section 22: Information intended for future publication and research information. E.g. We are working with a researcher who will be publishing the information as part of a report.
- Section 30(1): Criminal investigations and proceedings. E.g. Information law enforcement are using as part of a criminal investigation.
- Section 38: Endangering health and safety. E.g. Complying would endanger someone's physical or mental health.
- Section 42: Legal professional privilege. E.g. Advice given by a solicitor.
- Section 43: Commercial interests. E.g. Information which could be considered a "trade secret" or that affect a business dealing.

If the information falls under one of the above exemptions, then the public interest test will be applied.

1) Would this information interest the public at large? E.g. Is there, or has there been any media coverage surrounding it.
2) If there any benefit to this information coming out to the public at large or just the individual requester?
3) What benefits will there be to disclose the information?
4) Is this the best time to disclose the information, or would a later date be beneficial?

We will explain why we have reached our decision.

Test 4: Prejudice Test

If there is a chance that the release of this information could cause harm in some way, we need to consider any potential negatives of releasing the information.

1) Identify the potential negative consequence of the disclosure, these consequences should be graded as either trivial, medium or significant.
2) Demonstrate a link between the disclosure) and the negative consequences, showing how one would cause the other.
3) Indicate how there is a real possibility of the negative consequences happening, and grade it on a not likely, likely, very likely scale.

Test 5: Time/Cost Test:

Section 12 of the Freedom of Information Act (FOIA) advises that authorities can refuse a request if estimates that would exceed the appropriate cost limit of £450 to comply with the request;

- Cost estimates should include the time taken:
  (i) determining whether the information is held;
  (ii) locating it;
  (iii) retrieving it;
  (iv) extracting it.
- Time spent is calculated on a flat rate of £25 per person per hour.
- Therefore, the appropriate limit would be met after 18 hours of work.
- The cost estimate should be “sensible, realistic and supported by cogent evidence”.

If Section 12 is invoked, we will try to assist the requestor to refine the request so it comes under the limit.

6. Stage 3 Collate:

Once the decision has been made whether or not we can respond or not, then comes collating the information and presenting it in a readable format.

This can vary greatly as the request could be for a policy or for specific figures.

7. Stage 4: Response

We will explain the process and result of the assess stage to the requester and present them with the information. Our response will include:

- Reconfirming what was asked for.
- What is being supplied.
- What is not being supplied and why.
- Ability to discuss this further with the school or Federation.
- Right to refer to the ICO and contact details.

When supplying the data, it must be in an understandable format. It is recommended that we explain clearly what we have provided and why. We will also explain why we have not provided any information requested.

8. Stage 5: Review

If the requester asks for an internal review this will be carried out by a different and more senior person to the one who considered the original request. This will usually be the Federation's Finance & Business Director.

The review will be a fresh decision made on all the evidence that's relevant and available, rather than just a review of the first decision.

We will aim to complete internal reviews within 20 school days of their receipt.

Our response will include informing the requester of their right to refer their request to the ICO and the ICO's contact details.

Policy written:	June 2020
Amended/Updated:	April 2022
Adopted by Central Governing Board:	April 2022
Review date:	April 2023

The Central Governing Board have reviewed this policy with careful consideration of our approach to equalities as outlined in the Equalities Policy, January 2020.

We would like to acknowledge the work of other colleagues in drafting this policy. We have drawn on a range of sources including policies from other schools, good practice guides, published schemes and LA and Statutory guidelines where appropriate.

PRIMARY ADVANTAGE
SCHOOLS ACHIEVING MORE TOGETHER