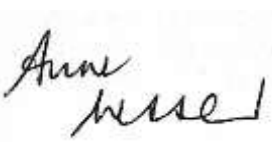
LDBS Academies Trust

Excellence and Equity for All Children in a Christian Context

Data Protection: Breach Management Procedure

ST RICHARD'S SCHOOL

INSPIRING BELIEF
in God and one another

DATE APPROVED BY THE LAT	May 2021
DATE APPROVED BY THE LAC	June 2021
REVIEW DATE	May 2023
Signed Headteacher	
Signed Chair of LAC	

LDBS Academies Trust

Vision Statement

Our schools aspire to provide 'excellence and equity in a Christian context', where every child is valued as a unique individual treasured by a loving God. 'I have inscribed you on the palms of my hands.' Isaiah 49.v16.

Our aim is that every child will have the opportunity to flourish and develop into a rounded adult who can live life to the full. 'I have come that they may have life and may have it in all its fullness'. John 10.v10.

Our schools are places where all are welcome and where we practise kindness and hospitality on a daily basis.

Our vision and our values are clearly displayed and while it is not a requirement that a child and their family have to be practising Christians we do expect all parts of the community, children, staff, parents and carers to support the values that we hold dear.

In our school we demonstrate how we support this vision through our values which are Friendship, Endurance, Trust and Hope and summed up in the following statement Inspiring belief in God and in one another.

The vision of St Richard's CE Primary School is for a thriving and outstanding school where children and adults have the opportunity to become the best they can be.

Inspiring belief…

- in ourselves – through progression and fulfilment
- in each other – through motivation and teamwork
- in the children – through showing them their potential
- in the parents – through building trust by results
- in God to all – through our whole lives.

- We believe in looking out for everyone
  We put safety first and we do all we can to ensure that all needs are met.
- We believe in working together
  We act like a family who support and motivate one another.
- We believe in aiming for the best
  We do all we can to ensure the highest quality in every area – our children deserve nothing less.
- We believe in looking to the future
  We are positive and seek opportunities to grow and improve, overcoming obstacles to achieve our goals.

We live out our values and vision through our key policies e.g. The LAT Behaviour policy is supported through the values described in the rewards and sanctions section of the policy demonstrating the importance of dignity and forgiveness.

The school admissions policy decided by the Local Academy Committee shows our inclusivity and the importance we place on service to our local community.

The breadth of the curriculum and the creative projects which we enjoy are key to providing opportunities for children to experience life in 'all its fullness', so that alongside learning and wisdom they also experience joy and delight in learning.
Care for the individual and their needs is crucial and the school's policies regarding inclusion and SEND are constant reminders that each of us is known to God and our names are 'inscribed on the palms of His hands'.

LAT HR policies are common in all schools and are created to ensure that individuals are treated fairly and with dignity. All HR policies have been scrutinised by the various unions to ensure that they contain acceptable procedures.

LDBS Academies Trust

Table of Contents

Definitions

Term	Definition
'Board'	Refers to the Board of Directors of the Trust.
'CCTV'	Refers to Closed Circuit Television.
'CEO'	Refers to the Chief Executive Officer of the Trust.
'Consent'	Freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
'Data Breach'	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.
'Data Controller'	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.
'Data Processor'	A natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller, following the Controller's instructions.
'Data Subject'	The identified or identifiable individual whose Personal Data is held or processed.
'DBS'	Refers to the Disclosure and Barring Service.
'DPL'	Refers to data protection law, including the EU's General Data Protection Regulation, the Data Protection Act (as revised from time to time), case law, regulations, and statutory guidance.
'DPO'	Refers to the Data Protection Officer.
'HMRC'	Refers to Her Majesty's Revenue and Customs Office.
'ICO'	Refers to the Information Commissioners' Office.
'LAC'	Refers to the Local Academy Committees of the Trust.

'Personal Data'	Any information relating to an identified or identifiable natural or legal person (e.g. a Data Subject); an identifiable natural or legal person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as: • A name; • An identification number; • Location Data; • An online identifier; and / or • One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural or legal person.
'Processing'	Any operation, or set of operations, which is performed on Personal Data, or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing can be automated or manual.
'Special Categories of Personal Data'	Personal Data which is more sensitive and so needs more protection. Such data includes information about an individual's: • Racial or ethnic origin; • Political opinions; • Religious or philosophical beliefs; • Trade union memberships; • Genetics; • Biometrics (i.e. fingerprints, retinal or iris patterns), where used for identification purposes; • Health (including physical and mental); • Sexual history or sexual orientation; and / or • History of offences, convictions or cautions*. * Whilst criminal offences are not classified as 'sensitive data' within the Data Protection Act 2018, the Trust has included it within this policy as acknowledgement of the care needed with this data set.
'Trust'	Refers collectively to the LDBS Academies Trust and the LDBS Academies Trust 2.

1. Aim

1.1. The Trust aims to have a robust procedure in place to deal with any breaches of Personal Data. The Procedure is based on guidance released by the ICO and is in compliance with the Data Protection Act 2018.

1.2. This Procedure must be read in conjunction with the Trust's other Data Protection Policies.

2. Reporting a data breach

2.1. On finding or causing a breach of Personal Data, or a potential breach, the staff or data controller must immediately notify the (Executive) Headteacher. The (Executive) Headteacher will inform the CEO and make a decision as to whether the matter should be reported to the Trust's Data Protection Officer.

2.2. As a public body, the Trust has appointed the Grow Education Partners Ltd as its Data Protection Officer, the responsible person is David Coy, who can be contacted via email at david.coy@london.anglican.org or via mobile on 079 0350 6531.

3. Procedure to investigate data breaches

3.1. Irrespective of whether the DPO is notified the response to the breach should require (1) investigation, (2) recovery, (3) reporting and remedial action. Steps (1) to (3) must be completed within 72 hours of the breach, as per the guidance contained within the Data Protection Act 2018.

3.2. Investigation

3.2.1. The investigation should determine whether the Personal Data was accidentally or unlawfully handled. Reaching a conclusion will require determination of whether the data has been lost, stolen, destroyed, altered, disclosed or made available when it should not have been, and / or whether it was made available to unauthorised persons.

3.2.2. Once a breach has been confirmed, the investigating officer should consider whether the vulnerability of the Data Subjects, the type of Personal Data lost, the specific sets of Personal Data lost, the number of sets of Personal Data lost and the format of Personal Data lost.

3.2.3. Additionally, all confirmed breaches should be logged into the Data Breach Log and assigned a unique reference number. All subsequent information concerning the data breach should be recorded into this log.

3.3. Recovery

3.3.1. The second step of the Procedure concerns containment and minimisation of the impact from the data breach. The investigating officer should seek assistance from relevant staff members or other Data Processors as necessary.

3.3.2. The recovery process may include contacting persons whom may have received the data, email recovery, back-up file restoration and / or request to delete the data. If deletion of data has been requested, then a written confirmation should be attained.

3.3.3. The Data Breach Log must record the success or failure of the recovery.

3.4. Reporting

3.4.1. Depending on the result of the recovery and containment efforts, the investigating officer must review the potential consequences, and assess their seriousness and likelihood, to decide who should be informed about the data breach, the affected Data Subjects and / or the ICO.

3.4.2. In the report, the investigating officer must set out a description of the data breach, the name and contact details of the DPO, a description of the likely consequences of the data breach, and a description of the measures that have been, or will be, taken to deal with the data breach and mitigate adverse effects. The decision on whether to contact the affected Data Subjects individually must be documented.

3.4.3. The decision to report a breach to the ICO must include consideration of whether there might be any negative effects on the rights of the affected Data Subject's freedoms, cause them any harm (physical, material or non-material) through (but not limited to) loss of control over the data, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, reputational damage, loss of confidentiality and / or significant economic or social disadvantage. This decision must be documented and stored with in the Data Breach Log.

3.4.4. The ICO can be notified online via the 'report a breach page' on their website (https://ico.org.uk/), or via the breach report-line (030 3123 1113). If it decided that the breach should be reported to the ICO, then this must be completed within 72 hours of becoming aware of the breach. The report must contain all the details stipulated by paragraph 3.4.2. If there are details which are unknown, the report must explain that there is a delay in procuring all the information, the reasons for the delay and when the outstanding information could be shared with the ICO.

3.5. Remedial actions

3.5.1. The investigating officer must conclude their investigation by determining future actions which could be used to prevent a similar breach from occurring. Such actions may include, but are not limited to, anonymisation and minimisation of data, encryption of digital data drives, secure access to servers, requirements for passwords to be strong (i.e. containing lowercase letters, uppercase letters, numerals, and special characters), training and support for staff and / or the use of encryption in emails.

3.5.2. At the conclusion of this procedure, the investigating officer should create a short report to supply to the (Executive) Headteacher, the LAC, and the Trust.