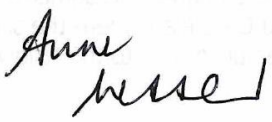
LDBS Academies Trust

Excellence and Equity for All Children in a Christian Context

Data Protection Policy

INSPIRING BELIEF
in God and one another

ST RICHARD'S SCHOOL

DATE APPROVED BY THE LAT	May 2020
DATE APPROVED BY THE LAC	May 2020
REVIEW DATE	May 2022
Signed Headteacher	
Signed Chair of LAC	

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 summarised in the school's own vision 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, working with the local community, 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.

Contents

1. Aim

The Trust aims to ensure that all Personal Data collected, stored, processed and destroyed by any natural person – whether they be a member of staff, a pupil, a parent, a LAC governor, a visitor, a contractor, a consultant, a member of supply staff or any other individual in any of the Trust's schools – is done so in accordance with the DPL, case law and any other statute.

This policy applies to all Personal Data collected, stored, processed and destroyed by the Trust or one of its schools, regardless of whether it is in paper or electronic format, or the type of filing system it is stored in and whether the collection of Processing of data was, or is, in any way automated.

2. Legislation and guidance

This policy meets the requirements of the DPL. It is based on guidance published by the ICO.

The policy meets the requirements of the Protection of Freedoms Act 2012, ICO's Code of Practice in relation to CCTV usage, and the DBS Code of Practice in relation to handling sensitive information. This policy also complies with the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's education record.

As with all Trust policies, this policy meets the expectations stated within the Trust's articles of association and funding agreement.

3. 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.

4. The Data Controller

The Trust, both in the work of its schools and its central functions, processes Personal Data relating to parents, pupils, staff, governors, visitors and others, and, therefore, is a Data Controller and a Data Processor.

The Trust is registered as a Data Controller with the ICO and will renew this registration annually or as otherwise legally required.

LDBS Academies Trust is registered with the ICO under ZA089623 and the LDBS Academies Trust 2 is registered with the ICO under ZA229902.

5. Roles and responsibilities

This policy applies to all staff employed by the Trust and to all external organisations or individuals working for the Trust or on the Trust's behalf. Non-compliance with this policy may result in disciplinary action being taken by the Trust.

5.1. The Board

The Board has overall responsibility for ensuring that the Trust's schools comply with all the relevant data protection obligations. The Trust will seek to perform its responsibility by reviewing this policy regularly, appointing a DPO and delegating the responsibility to implement this policy to the LACs.

5.2. The Local Academy Committees

The LACs have delegated responsibility to review this policy's implementation at the school level.

5.3. The Data Protection Officer

As a public body, the Trust have appointed Grow Education Partners Ltd as it's 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.

The DPO is responsible for overseeing the implementation of this policy in the first instance, before reviewing the Trust's compliance with the data protection law and developing related policies and guidelines where applicable.

The DPO will provide an annual report of compliance and risk issues directly to the Board with recommendations and advice. The DPO will also visit each school within the Trust and submit a data monitoring report to the LAC.

The DPO will be the named point of contact for individuals whose data the school processes and for the ICO. Full details of the DPO's responsibilities and duties are contained within the service level agreement the Trust has entered with Grow Education Partners Ltd.

5.4. The (Executive) Headteacher

The (Executive) Headteacher acts as the representative of the Data Controller on a day-to-day basis.

5.5. Staff

All staff (regardless of role) are responsible for:

- Collecting, storing, and Processing any Personal Data in accordance with this policy;
- Informing the school of any changes to their Personal Data (i.e. a change of address, telephone number, or bank details); and
- Reporting a Data Breach, Data Right Request or Freedom of Information Request.
- Contacting the DPO:
    - 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 the 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 of the European Economic Area;
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals; and
    - If they need help with any contracts or sharing Personal Data with third parties.

6. The Principles of Data Protection Law

The EU's General Data Protection Regulation is based on seven data protection principles that the Trust must comply with; these require that all data 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 is it is processed; and
- Processed in a way that ensures it is appropriately secure.

The accountability principle ties these together by requiring an organisation to take responsibility for complying with the principles, including having appropriate measures and records in place to be able to demonstrate compliance.

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

7. Collection of Personal Data

7.1. Lawfulness, fairness and transparency

The Trust will only process Personal Data where it has met one of the six lawful reasons to do under the Data Protection Act 2018. The six lawful reasons are that:

- The individual (or their parent / carer in the case of a pupil, where appropriate) has freely given clear **Consent;**
- The data needs to be processed so that the school 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 can **comply with a legal obligation**;
- The data needs to be processed to ensure the **vital interests** of the individual (i.e. to protect someone's life);
- The data needs to be processed so that the school, as public authority, can perform a **task in the public interest,** and carry out its official functions; and / or
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden).

For Special Categories of Personal Data, the Trust will need to meet one of the special category conditions for Processing as set out in the Data Protection Act 2018. The conditions are when:

- The individual (or their parent / carer in the case of a pupil, where appropriate) has given **explicit Consent;**
- It is necessary for the purposes of carrying out the **obligations and exercising specific rights** of the controller or of the data subject in the field of **employment** of a Data Controller or of a Data Subject;
- It is necessary to protect the **vital interests** of the Data Subject;
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;
- The Personal Data has **manifestly been made public** by the Data Subject;
- There is the **establishment, exercise or defence of a legal claim**;
- There are reasons **of public interest** in the area of **public health**;
- Processing is necessary for the purposes of preventative or occupational medicine (e.g. for the **assessment of the working capacity of the employee**, the medical diagnosis, the provision of health or social care or treatment); and / or
- There are **archiving** purposes in the **public interest**.

If the Trust decides to offer online services to pupils, such as classroom applications, and the Trust intended to rely on Consent as a basis for Processing, the Trust will need to get parental consent for this (except for online counselling and preventative services).

Where the Trust collect personal data directly from individuals, the Trust will provide them with the relevant information required by data protection law, in the form of a privacy notice.

These privacy notices can be found in a location accessible and relevant to the data subjects:

- Pupils and Parents: School Website, School Office
- Staff: T-Drive, School Office
- Governors: Governor Hub, School Office

- Job Applicants: School Office, School Website, sent to candidate with application
- Suppliers / Contractors / Consultants:
- Trainees: School Office, given to candidate by mentor
- Visitors: School Office
- Volunteers: School Office, given to candidate on arrival

Hard copies of the Privacy Notices are available on request by contacting the Company Secretary and / or the Administrator for the Trust.

7.2. Limitation, minimisation and accuracy

The Trust will only collect Personal Data for specific, explicit and legitimate reasons. The Trust will explain such reasons to the individuals (or their parents / guardians, where appropriate) when the Trust first collects their data in accordance with the Trust's privacy notices.

If the Trust wishes to use the Personal Data for reasons other than those given when the data was first obtained, then the Trust will inform the individuals concerned before doing so and seek further Consent where necessary.

Staff must only process Personal Data where it is necessary in order to fulfil their designated duties.

When Personal Data is no longer required, staff must ensure that it is deleted. This will be done in accordance with the Document Retention Schedule, which states how long a particular type of document may be kept and how it should be destroyed.

Copies of the Document Retention Policy can be obtained by accessing the Trust's website https://www.ldbsact.org/ or by contacting the Company Secretary or the Administrator.

8. Sharing Personal Data

In order to efficiently, effectively and legally function as a data controller we are required to share information with appropriate third parties, including but not limited to;

- There is an issue with a pupil or parent / guardian that puts the safety of Trust's staff at risk; or
- The Trust needs to liaise with other agencies or services (the Trust pledges to seek Consent, as applicable, prior to sharing Personal Data in relation to this);
- The Trust's supplies or contractors need data to enable the Trust to provide services to staff and pupils (i.e. information technology companies). The Trust pledges that when sharing data, in this relation to this, it will:
    - Only appoint suppliers or contractors who can provide sufficient guarantees that they are in compliance with the data protection laws and have satisfactory security measures in place;
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful Processing of any Personal Data it shares; and
    - Only share data that the supplier or contractor needs to carry out their service and any such information necessary to keep them safe while working with the Trust.

The Trust will also share Personal Data with law enforcement and government bodies where it is under a legal obligation to do so, such as:

- The prevention or detection of crime and / or fraud;
- The apprehension or prosecution of offenders;
- The assessment or collection of tax owed to the HMRC;
- In connection with legal proceedings;
- Where the disclosure is required to satisfy the Trust's safeguarding obligations; and
- For research and statistical purposes, as long as the Trust is satisfied that the Personal Data shared will be sufficiently anonymised or Consent from the Data Subject has been obtained.

The Trust may also share Personal Data with emergency services and local authorities to help them response to an emergency situation affecting the Trust's pupils or staff.

In the event that the Trust transfers Personal Data to a country or territory outside of the European Economic Area, it will do so in accordance with data protection laws and will consult with the affected Data Subjects first.

9. Individual rights

9.1. Subject access requests

Data Subjects have a right to make a 'subject access request' to access any Personal Data held by the Trust 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;
- The source of the data, if not the individual; and / or
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

While the Trust will comply with the EU's General Data Protection Regulation when dealing with subject access requests submitted in a written form. Data Subjects are requested to submit their subject access requests by letter, email, or fax, addressed (or marked) for the attention of the DPO. All requests must include:

- The name of the Data Subject;
- A correspondence address;
- A contact number;
- An email address; and
- Details of the Personal Data requested.

In the event that a subject access request is submitted to a member of Trust's staff, it should be immediately forwarded to the School Business Manager.

9.2. Pupils and subject access requests

An individual's Personal Data belongs to them. Therefore, the Trust recognises that a pupil's Personal Data belongs to that pupil, and not the pupil's parents / carers.

However, pupil under the age of 12 are legally not always regarded to be mature enough to understand their rights and the implications of invoking a data request. Therefore, subject

access requests from the parents of pupils under the age of 12 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.

Where a pupil is judged to be of sufficient age and maturity to exercise their rights and a request is invoked on their behalf, the Trust will seek consent from the pupil to authorise the action to be undertaken.

9.3. Responding to subject access requests

When responding to requests, the Trust:

- May request the Data Subject to provide two forms of identification from the list below:
    - Passport,
    - Driving licence,
    - Utility bills with the current residential address of the Data Subject,
    - P45 / P60, and
    - Credit card or mortgage statement;
- May contact the Data Subject via phone to confirm the request;
- Will respond without delay and within 1 month of receipt of the request;
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this as soon as possible and explain why the extension is necessary.
- Will provide the information free of charge (unless it is found to be onerous, excessive or unfounded). Any fee charged will be reasonable and would only account for the administrative costs incurred while complying with the request.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual; or
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests; or
- Is contained in adoption or parental order records; or
- Is given to a court in proceedings concerning the child.

If the request is manifestly unfounded or excessive, we may refuse to act on it, or charge a fee as explained above.

A request will be deemed to be manifestly unfounded or excessive if it is repetitive or asks for further copies of the same information.

In the event the Trust refuse a request, we will tell the individual why, and tell them they have the right to refer a complaint to the ICO.

9.4. Other data protection rights of the Data Subject

In addition to the right to make a subject access request and to receive information when the Trust is collecting the data and about how the Trust uses and processes the data; Data Subjects also have the right to:

- Withdraw their consent to processing at any time, this only relates to tasks which the school relies on consent to process the data;
- Ask the Trust to rectify, erase, or restrict Processing of the Data Subject's Personal Data, or object to the Processing of it in certain circumstances;

- Prevent the use of any Personal Data for direct marketing;
- Challenge Processing which has been justified on the basis of public interest;
- Request a copy of agreements under which their Personal Data is transferred to outside the European Economic Area;
- Object to decisions based solely on automated decision making or profiling (e.g. decisions taken with no human involvement that might negatively affect them);
- Be notified of a Data Breach in certain circumstances;
- Make or lodge a complaint with the ICO; and / or
- Ask for their Personal Data to be transferred to a third part in a structured, commonly used and machine-readable format (in certain circumstances).

Data Subjects should submit any request to exercise these rights to the School Business Manager (office@strichards.hounslow.sch.uk).

If staff receive such a request, they must immediately forward it to the School Business Manager (office@strichards.hounslow.sch.uk).

9.5. Parental requests to see the education record

While parents do not have any automatic right of access to pupil's files in academies generally, the Trust does allow this to happen. The Trust grants parents / guardians the access to see their child's educational record within 15 school days after receiving a written request.

Requests should be made in writing to the Headteacher via the school and should include:

- The name of the individual requesting information;
- The correspondence address;
- The contact number; and
- The email address.

10. Closed Circuit Television

The Trust uses CCTV in various locations around the various school for the prevention and detection of crime However, footage may be used for additional reasons specified more fully in the CCTV Policy. The Trust adheres to the ICO's Code of Practice for the use of CCTV and provides training to staff in its use. Any enquiries about the CCTV system used by the Trust should be directed to the DPO.

The Trust does not need to ask individuals' permission to use CCTV, but makes it clear where individuals are being recorded with security cameras, which are clearly visible and accompanied by prominent signs explaining that CCTV is in use, where not clear, directions will be given on how the individual may obtain further information.

The full CCTV policy can be found by http://www.strichardsschool.org.uk/about-our-school/policies/. Any enquiries about the CCTV system should be directed to the DPO.

11. Photographs and videos

As part of school activities, the Trust may take photographs and record images of individuals within the Trust schools.

The Trust uses photographs:

- Within the Trust's schools on notice boards and in school magazines, brochures, newsletters and prospectuses;
- Outside of the Trust's schools by external agencies and partners such as the school photographer, the local and national newspapers, and local and national campaigns that the Trust or a Trust school may be involved with; and
- Online on the Trust's or the Trust's school's website or social media pages.

The Trust will clearly explain how photographs and or video will be collected and used to both the parent / carer and the pupil, when obtaining consent.

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

The parent / carer or the pupil can withdraw consent by writing to the (Executive) Headteacher.

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

Please refer to the Trust's Keeping Children Safe in Education Policy for further information on the Trust's use of photographs and videos.

This can be found online on the Trust's website http://www.strichardsschool.org.uk/about-our-school/policies/

12. Data protection by design and default

The Trust will put measures in place to show that the Trust has integrated data protection into all of its data collection and Processing activities. These include, but are not limited to, the following organisational and technical measures:

- Appointing a suitably qualified DPO and ensuring that the DPO has 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 the relevant data protection regulations;
- Integrating data privacy impact assessments where the school's Processing of Personal Data presents a high risk to the rights and freedoms of Data Subjects and when introducing new technologies or Processing tools, in such cases advice will be sought from the DPO;
- Integrating data protection into internal documents including this policy and any related policies and privacy notices;
- Regular (at least annual) training of staff, LAC governors, and directors on data protection law, this policy and any related policies and any other data protection matters (records of attendance will be kept to record the training sessions and ensure that all data handlers receive appropriate training);
- Periodic reviews and audits to test the Trust's privacy measures and make sure that the Trust remains compliant; and
- Maintaining records of the Trust's Processing activities, including:
    - Making available the name and contact details of the Trust and the Trust's DPO and all information the Trust is required to share regarding its use and Processing of Personal Data (via the Trust's Privacy Notices) – for the benefit of Data Subjects; and

- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

13. Data security and storage of records

The Trust will protect all 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, the Trust's organisational and technical measures include:

- Keeping paper-based records and portable electronic devices, such as laptops, tablets and hard drives that contain Personal Data under lock and key when not in use.
- Not leaving papers containing Personal Data on office and classroom desks, on staffroom tables, pinned to notice / display boards, or left anywhere else where there is general access.
- Passwords that are at least eight (8) characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils should be reminded to change their passwords at regular intervals.
- Encryption software is used to protect any devices such as Laptops, Tablets and USB Devices where saving to the hard drive is enabled.
- Staff, pupils or governors who store Personal Data on their personal devices are expected to follow the same security procedures as for school-owned equipment (please refer to the Trust's Online & E-Safety Policy, the ICT Policy, and the User Agreements and Email Use Policy for further information).
- Where the Trust needs to share Personal Data with a third party, the Trust will carry out due diligence and take all reasonable steps to ensure that Personal Data shared will be stored securely and protected adequately.

14. Disposal of records

Personal Data that is no longer needed will be disposed securely. Personal Data that has become inaccurate or out of date will be disposed securely, in the instance where the Trust does not need to rectify it or update it.

For instance, the Trust will shred paper-based records and overwrite or delete electronic files. The Trust may also use a third party to safely dispose records on the Trust's behalf. In this instance, the Trust will require the third party to provide sufficient guarantee that it complies with the data protection law and a certificate of destruction, which will be recorded on to the Trust's systems.

When records are disposed of as part of the Data Retention schedule this is then recorded on our record of destruction log.

15. Personal Data breaches

The Trust will make all reasonable endeavours to ensure that there are no Personal Data breaches. In the unlikely event of a suspected Data Breach, the Trust will follow the procedure as set out in the Trust's Breach Management Policy.

All potential or confirmed Data Breach incidents should be reported to the (Executive) Headteacher and the CEO where they will be assigned a unique refence number and recorded in the school's data breach log.

Once logged, incidents will then be investigated, the potential impact assessed, and appropriate remedial action undertaken. The DPO will be consulted as required.

Where appropriate, the Trust will report the data breach to the ICO and affected Data Subjects within 72 hours.

The full procedure is set out in the Trust's Breach Management Policy, which can be found here http://www.strichardsschool.org.uk/parents-information/general-data-protection-regulations-gdpr/

Examples of a Data Protection Breach include but are not limited to:

- Personal data being let unattended in a meeting room/in the staffroom / in the staff Planning, Preparation and Assessment room;
- Sending information relating to a pupil or family to the wrong member of staff in school, or to the wrong parent;
- 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; and / or
- The theft of a school laptop containing non-encrypted personal data about pupils.

16. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy as part of the general monitoring and compliance work, they carry out.

The DPO will work with the Headteacher, School Business Manager and the Company Secretary to ensure that this policy remains contemporaneous and appropriate.

This policy will be reviewed every two years.

17. Links with other policies

This policy must be read in conjunction with the Trust's:

- Asset Management Policy.
- Breach Management Policy.
- Business Continuity Plan and Risk Register.
- CCTV Policy.
- Data Retention Schedule.
- Freedom of Information Policy and Publication Scheme.
- ICT User Agreements and Email Use Policy.
- Keeping Children Safe in Education Policy.
- Online & E-Safety Policy.