DDAT
Derby Diocesan Academy Trust

Diocese of Derby
THE CHURCH OF ENGLAND

Derby Diocesan Academy Trust 2

DATA PROTECTION POLICY

Date of adoption: 1st June 2019
Date to be revised: 1st June 2021

1 POLICY STATEMENT

1.1 Derby Diocesan Academy Trust 2 ('the Trust', 'we', 'us' and 'our') is committed to upholding individuals' rights to have their Personal Data protected. This policy is designed to take into account the General Data Protection Regulation and associated legislation including the Data Protection Act 2018 and successor legislation.

1.2 While carrying out its functions, the Trust will collect, store and process Personal Data about students, parents, employees and other third parties. Proper treatment of Personal Data is essential and in line with the Trust's values.

1.3 Trust staff are obliged to comply with this Policy when processing Personal Data on our behalf. Any breach of this Policy by Trust staff may result in disciplinary or other action.

2 ABOUT THIS POLICY

2.1 The Trust holds Personal Data about current, past and prospective students, parents, employees and others with whom the Trust communicates. Personal Data may be recorded on paper or stored electronically.

2.2 This Policy and other documents referred to in it set out the basis on which the Trust will process any Personal Data it collects from individuals, whether those data are provided to us by individuals or obtained from other sources. It sets out the rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store Personal Data.

2.3 This Policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 The Data Protection Officer is responsible for ensuring compliance with the Relevant Data Protection Laws and with this Policy. That post is held by Jason Hampton who can be contacted at ddatadmin@derby.anglican.org or on 01332 388650. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer.

3 DEFINITION OF DATA PROTECTION TERMS

3.1 In this Policy, the functions of the Trust are the provision of education and any pastoral, business, administrative, community or similar activities associated with that provision. References to the Trust 'carrying out its functions' or similar are references to these activities.

3.2 References to 'we' are references to the Trust.

3.3 **Criminal Convictions and Offences** means the commission of, or proceedings for, any offence committed or alleged to have been committee by a person, the disposal of such proceedings or the sentence of any court in such proceedings.

3.4 **Data Subjects** means identified or identifiable natural persons whose Personal Data the Trust holds. This Policy also refers to Data Subjects as 'individuals.'

3.5 **Data Controllers** are the people who, or organisations which, determine the

purposes for which any Personal Data are processed, including the means of the processing. The Trust is the Data Controller of all Personal Data used for carrying out its functions.

3.6 **Data Users** are, for the purposes of this Policy, those of our employees whose work involves processing Personal Data. Data Users must protect the data they handle in accordance with this Policy and any applicable data security procedures at all times. This Policy also refers to Data Users as 'Trust staff' or simply 'staff'.

3.7 **Data Processors** include any person or organisation, who is not a member of Trust staff, which processes Personal Data on our behalf. Employees of Data Controllers are excluded from this definition, but it could include suppliers that handle Personal Data on the Trust's behalf.

3.8 **Fair Processing Notices** are documents explaining to Data Subjects how their data will be used by the Trust. This Policy also refers to Fair Processing Notices as 'Privacy Notices'

3.9 **Personal Data** means any information relating to an identified or identifiable natural person; an identifiable natural 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 or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.10 **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

3.11 **Pseudonymisation** means the processing of Personal Data so that it can no longer be attributed to a specific person without the use of additional information, provided that such additional information is kept separately and is subject to measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

3.12 **Relevant Data Protection Law** means the General Data Protection Regulation ((EU) 2016/679), the Data Protection Act 2018 and any successor legislation, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) and all applicable laws and regulations relating to the processing of Personal Data and privacy as amended, re-enacted, replaced or superseded from time to time and where applicable the guidance and codes of practice issued by the United Kingdom's Information Commissioner.

3.13 **Special Categories of Personal Data** (formerly known as 'sensitive Personal Data') include information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and genetic or biological traits. Special Categories of Personal Data can only be processed under strict conditions.

4 DATA PROTECTION PRINCIPLES

4.1 Anyone processing Personal Data for or on behalf of the Trust must comply with the principles of good practice contained in Relevant Data Protection Law. These

principles state that Personal Data must be:

4.1.1 processed fairly, lawfully and transparently;

4.1.2 processed for specified, limited and legitimate purposes and in an appropriate way;

4.1.3 adequate, relevant and not excessive for the purposes for which they are processed;

4.1.4 accurate and, where necessary, kept up to date;

4.1.5 not kept longer than necessary for the intended purpose of processing; and

4.1.6 processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Trust will keep a record of all data processing activities and must be able to demonstrate its compliance with these principles and with the wider requirements of Relevant Data Protection Law.

5 FAIR, LAWFUL AND TRANSPARENT PROCESSING

5.1 For Personal Data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in Relevant Data Protection Law. These are as follows:

5.1.1 the Data Subject has given consent to the processing of his or her Personal Data for one or more specific purposes;

5.1.2 processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;

5.1.3 processing is necessary for compliance with a legal obligation to which the controller is subject;

5.1.4 processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;

5.1.5 processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

5.1.6 processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

5.2 Where a type of data processing is likely to pose a high risk to individuals' rights and freedoms, the Trust will carry out an appropriate Privacy Impact Assessment.

5.3 *Special Categories of Personal Data*

5.4 When Special Categories of Personal Data are being processed, the individual's explicit consent to processing of those data must be obtained unless the processing:

5.4.1 is necessary for the purposes of carrying out the obligations and exercising specific rights of the Trust or of the individual in the field of employment and social security and social protection law;

5.4.2 is necessary for the assessment of the working capacity of an individual where the individual is an employee or for the provision of health or social care;

5.4.3 relates to Personal Data which are manifestly made public by the individual;

5.4.4 is necessary for reasons of substantial public interest; or

5.4.5 is necessary to protect the vital interests of the individual.

5.5 Processing of data relating to Criminal Convictions and Offences can only take place under control of an official authority, such as instructions from the police or an order of the court, or where UK or EU law states that processing must take place.

5.6 *Consent of adults and organisations*

5.7 Where an individual gives consent to Data Processing, that consent must be freely given, specific, informed and unambiguous and should be either in the form of a statement (whether or not prepared by the Trust) or a positive action demonstrating consent. Any requests that the Trust makes for consent must be in clear language.

5.8 An individual has the right to withdraw consent at any time and will be informed of this right and how to exercise it when the Trust requests consent.

5.9 *Consent of children and young people*

5.10 Parental consent to Data Processing must be obtained for pupils or other children younger than 13 years of age.

5.11 A young person aged 13 or over is able to give or revoke consent (unless they do not have capacity).

5.12 Where consent is required from a young person aged 13 or over the requirements in relation to consent, as set out for adults, still apply and the information in relation to such consent must be made clear to the young person.

6 PROCESSING FOR SPECIFIED, LIMITED AND LEGITIMATE PURPOSES

6.1 In the course of carrying out its functions, the Trust may collect and process Personal Data. This may include data we receive directly from an individual (for example, by completing forms or by corresponding with us by post, phone, email or otherwise) and data we receive from other sources (including, for example, the local authority or other public bodies, business suppliers or service providers, professional advisers and others).

6.2 The Trust will only process Personal Data for the specific purposes set out in the Record of Processing Activities or for any other purposes specifically permitted by Relevant Data Protection Law. We will explain those purposes to the Data Subject.

7 ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

7.1 We will only collect Personal Data to the extent that it is required for the specific purpose notified to the individual;

7.2 If a member of staff has any doubt as to whether any processing exceeds the purposes for which that data were originally collected, he or she should notify the Data Protection Officer.

8 ACCURATE AND UP-TO-DATE DATA

8.1 We will ensure that Personal Data we hold are accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

8.2 It is the responsibility of staff to ensure that Personal Data is accurate and kept up to date. Further, parents and anyone who provides Personal Data should also inform the Trust as soon as possible if there is any change to their Personal Data.

9 TIMELY PROCESSING

9.1 We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which are no longer required. We will be guided by the Information Records Management Society guidance in respect of decision making concerning the retention of Personal Data.

9.2 If a member of staff has any doubt as to whether any Personal Data has been or will be kept longer than is necessary for the purpose or purposes for which they were collected, he or she should notify the Data Protection Officer.

10 PROCESSING SECURELY AND IN LINE WITH RIGHTS OF DATA SUBJECTS

10.1 We will process data in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

10.2 We are committed to upholding the rights of individuals to access Personal Data the Trust holds on them.

10.3 We will process all Personal Data in line with individuals' rights, in particular their rights to:

10.3.1 be informed, in a manner which is concise, transparent, intelligible and easily accessible and written in clear and plain language, of the purpose, use, recipients and other processing issues relating to data;

10.3.2 receive confirmation as to whether your Personal Data is being processed

by us;

10.3.3 access your Personal Data which we are processing only by formal written request. We may charge you for exercising this right if we are allowed to do so by Relevant Data Protection Law. Trust employees who receive a written request should forward it to their senior leader and the Data Protection Officer immediately;

10.3.4 have data amended or deleted under certain circumstances where data is inaccurate or to have data completed where data is incomplete by providing a supplementary statement to the Trust (see also Clause 8);

10.3.5 restrict processing of data if one of the following circumstances applies:

10.3.5.1 the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the controller to verify the accuracy of the Personal Data;

10.3.5.2 the processing is unlawful, and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;

10.3.5.3 the controller no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;

10.3.5.4 the Data Subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the Data Subject.

10.3.6 Where processing has been restricted, as above, such Personal Data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State and the Data Subject shall be informed.

10.3.7 where processing is restricted under one of the grounds in Clause 10.3.5, the data shall only be processed with the individual's consent or in relation to the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or the United Kingdom;

10.3.8 an individual who has obtained restriction of processing under Clause 10.3.5 shall be informed by the Trust before the restriction of processing is lifted;

10.3.9 receive data concerning the individual, which he or she has provided to the Trust and is processed by automated means, in a structured, commonly used and machine-readable format and to transmit those data to another controller without hindrance from the Trust;

10.3.10 object to data processing on grounds relating to his or her particular

situation unless the Trust demonstrates compelling legitimate grounds for processing which overrides the interests, rights and freedoms of the individual or for to the establishment, exercise or defence of legal claims; and

10.3.11 not to be subject to a decision based solely on automated decision-making and profiling which produces legal effects concerning him or her or similarly significantly affects him or her unless the decision is based on the individual's explicit consent.

10.4 It is the responsibility of all staff to ensure that any request by an individual under Clause 10.1 is brought to the attention of the Data Protection Officer without undue delay.

10.5 The Trust may refuse a request by an individual wishing to exercise one of the above rights in accordance with Relevant Data Protection Law.

10.6 The Trust shall provide information on action taken on a request under Clause 10.1 to the individual within one month of receipt of the request unless the Trust deems it necessary to extend this period by two further months where the request is complex and informs the individual of such extension with reasons within one month of receipt of the request.

10.7 When receiving telephone enquiries, we will only disclose Personal Data we hold on our systems if the following conditions are met:

10.7.1 We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

10.7.2 We will suggest that the caller put his or her request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

10.7.3 We will also verify the identity of the person making the request by whatever reasonable means are considered appropriate.

10.8 Our employees will refer a request to their senior leaders and the Data Protection Officer for assistance in difficult situations. Employees should not feel pressured into disclosing information if they have concerns about disclosing it and should refer any questions to a senior leader or the Data Protection Officer.

11 NOTIFYING DATA SUBJECTS

11.1 If we collect Personal Data directly from individuals, we will at the time of collection inform them about the processing including:

11.1.1 the identity and contact details for the Trust and its Data Protection Officer;

11.1.2 the purpose or purposes for which we intend to process those Personal Data as well as the legal basis for the processing;

11.1.3 where the processing is necessary for the purposes of legitimate interests, the legitimate interests pursued;

11.1.4 the recipients or categories of recipients of the Personal Data;

11.1.5 where applicable, the fact that the Trust intends to transfer the Personal Data to a third country;

11.1.6 the period for which the Personal Data will be stored;

11.1.7 the existence of the rights of the Data Subject;

11.1.8 where the processing is based on consent, the right to withdraw consent at any time;

11.1.9 the right to lodge a complaint with a supervisory authority;

11.1.10 whether the provision of Personal Data is a statutory or contractual requirement and the possible consequences of failure to provide such data;

11.2 the existence of any automated decision-making, including profiling. If we receive Personal Data from a source other than the individual we will, except in certain circumstances, provide the individual with the information in Clause 11.1 above at the following times:

11.2.1 within one month of receiving the Personal Data;

11.2.2 if the Personal Data are to be used for communication with the individual, at the time of the first communication to the individual;

11.2.3 if a disclosure to another recipient is envisaged by us, at the time of the disclosure to that recipient.

11.3 A notification in the form of a Privacy Notice will be in writing or via a link to our website, unless the individual requests an oral notification.

11.4 We will also inform individuals whose Personal Data we process that the Trust is the Data Controller with regard to those data and who the Data Protection Officer is.

12 DATA SECURITY

12.1 We will take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

12.2 We will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data will only be transferred to a Data Processor if he or she agrees to comply with those procedures and policies, or if he or she puts in place adequate measures.

12.3 Trust staff can find details of their obligations in relation to security of Personal Data in the Trust's E-Safety Policy.

12.4 All Trust staff must:

12.4.1 assist the Trust in upholding individuals' data protection rights;

12.4.2 only act in accordance with the Trust's instructions and authorisation;

12.4.3 notify their line manager and the Data Protection Officer immediately of any Personal Data Breaches, allegations of Personal Data Breaches or suspicions of Personal Data Breaches in accordance with Clause 12.5;

12.4.4 comply at all times with the terms of any agreements with the Trust and with their responsibilities under Relevant Data Protection Law;

12.4.5 satisfy the Trust, within a reasonable period following request, of their compliance with the provisions of Clause 12.4.4.

12.5 The Trust will notify the Information Commissioner's Office where necessary, in respect of any relevant breach without undue delay.

12.6 If any Personal Data breach is likely to adversely affect individual's rights and freedoms, the Trust will inform those individuals without undue delay.

12.7 We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

12.7.1 **Confidentiality:** only people who are authorised to use the data can access them;

12.7.2 **Integrity:** Personal Data should be accurate and suitable for the purpose for which they are processed;

12.7.3 **Availability:** authorised users should be able to access the data if they need it for authorised purposes. Personal Data should therefore be stored on the Trust's central computer system. Individual computers, tablets or other media will not be used to hold Personal Data unless they are password-protected and fully encrypted.

12.8 Security procedures include:

12.8.1 **Entry controls:** any stranger seen in entry-controlled areas should be reported.

12.8.2 **Secure lockable desks and cupboards:** desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential).

12.8.3 **Methods of disposal:** paper documents should be shredded. Digital storage devices should be professionally processed and physically destroyed when they are no longer required.

12.8.4 **Equipment:** Trust staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their computers, tablets or other devices when left unattended.

12.8.5 **Data storage methods:** measures to store data securely, such as Pseudonymisation or key-coding, will be implemented where appropriate.

12.9 The Trust shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement data-protection principles and to

integrate the necessary safeguards into processing activities.

12.10 The Trust shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the processing are processed.

13 REGISTER OF PROCESSING ACTIVITIES

13.1 The Trust must maintain an accurate and up-to-date register of processing activities carried out by the Trust.

13.2 The Trust must record the following information for each processing activity:

13.2.1 the identity and contact details for the Trust and its Data Protection Officer;

13.2.2 the purpose or purposes for which the processing activity has occurred;

13.2.3 descriptions of the categories of individuals involved in the processing activity;

13.2.4 descriptions of the categories of Personal Data involved in the processing activity;

13.2.5 descriptions of the categories of recipients of the Personal Data involved in the processing activity;

13.2.6 details of any transfers to third countries, including documentation of the transfer mechanism safeguards in place;

13.2.7 retention schedules;

13.2.8 descriptions of technical and organisational security measures in place relating to the processing activity.

13.3 It is the responsibility of all staff, in particular the Data Protection Officer, to ensure that the register of processing activities is accurate and kept up to date.

14 REGISTER OF BREACHES

14.1 The Trust must maintain an accurate and up-to-date register of all Personal Data Breaches. If anyone becomes aware of a data protection breach they must inform the Trust immediately.

15 DATA PROTECTION OFFICER

15.1 The Data Protection Officer is responsible for monitoring compliance with Relevant Data Protection Law and with this Policy. That post is held by Jason Hampton, ddatadmin@derby.anglican.org. The Data Protection Officer reports to the Trust's lead GDPR Director, the finance subcommittee and board of trustees but fulfils his data protection functions independently.

15.2 Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer.

15.3 Where a Personal Data Breach has occurred, it will be for the Data Protection Officer to decide whether, under the circumstances and in accordance with Relevant Data Protection Law, the individual concerned must be informed of the breach.

16 USING DATA PROCESSORS

16.1 The Trust retains the right to engage by written contract any person or organisation, who is not a member of Trust staff, to process Personal Data on our behalf.

16.2 Data Processors must:

16.2.1 assist the Trust in upholding individuals' data protection rights;

16.2.2 only act in accordance with the Trust's instructions and authorisation;

16.2.3 maintain a written record of processing activities carried out on behalf of the Trust and provide this to the Trust within a reasonable period following request;

16.2.4 notify the Trust of Personal Data Breaches without undue delay and maintain a register of breaches in accordance with Clause 13;

16.2.5 comply at all times with the terms of any agreements with the Trust and with their responsibilities under Relevant Data Protection Law;

16.2.6 satisfy the Trust, within a reasonable period following request, of their compliance with the provisions of Clause 12.4.4.

17 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

17.1 Individuals have particular rights with regard to transfers of their Personal Data outside the European Economic Area ('EEA'). Circumstances in which the Trust may need to transfer data outside the EEA might include use of IT services hosted overseas, arrangement and administration of school trips and cultural exchange projects.

17.2 Subject to the requirements in Clause 12.1 above, Personal Data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Those staff may be engaged, among other things, in the processing of payment details and the provision of support services.

17.3 We may transfer any Personal Data we hold to a country outside the EEA provided that:

17.3.1 the transfer to the country or countries in question is permitted by Relevant Data Protection Law; and

17.3.2 any transfer to a country or countries outside the EEA is subject the escalation procedure under Clause 17.4.

17.4 Before a transfer of Personal Data is made outside the EEA, the following safeguards must be provided to ensure that the rights of Data Subjects and effective legal remedies for Data Subjects are available:

17.4.1 confirmation by implementing act by the European Commission of the adequacy of the level of protection afforded by the relevant third country

17.4.2 standard data protection clauses adopted by the European Commission in accordance with Relevant Data Protection Law must be included in relevant documentation;

17.4.3 ensuring explicit consent is given by the Data Subject to the proposed transfer after having been informed of the possible risks of such transfer;

17.4.4 confirmation that the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject;

17.4.5 confirmation that the transfer is necessary for important reasons of public interest;

17.4.6 the Data Protection Officer must authorise the transfer.

18 DISCLOSURE AND SHARING OF PERSONAL INFORMATION

18.1 We may share Personal Data we hold with staff at any academy within the Trust.

18.2 We may also disclose Personal Data we hold to third parties:

18.2.1 if we are under a duty to disclose or share an individual's Personal Data in order to comply with any legal obligation;

18.2.2 in order to enforce or apply any contract with the individual or other agreements; or

18.2.3 to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of child welfare and fraud protection.

18.3 We may also share Personal Data we hold with selected third parties for the purposes set out in the Record of Processing Activities.

19 REQUESTS FOR INFORMATION

19.1 Requests for information may take the following forms:

19.1.1 requests for education records;

19.1.2 freedom of information requests;

19.1.3 subject access requests.

19.2 Where a person with parental responsibility requests information about a child's educational records then the information should usually be provided unless there are some specific concerns about disclosing the information and the Data Protection Officer should be contacted. There is no legal right of access under the Education (Pupil Information) (England) Regulations 2005 to a child's educational record if the child attends an academy, independent or free school.

19.3 If a person makes a request for information under the Freedom of Information Act then the information should usually be provided unless there are some specific concerns about disclosing the information. Common concerns in the school context may be that information relates to other people, is confidential or legally privileged. There is extensive guidance on the ICO website. If a freedom of information request is made and there are any concerns about disclosing information then the Data Protection Officer should be contacted.

19.4 If a person makes a subject access request then they are requesting the personal information that the Trust has about them. There are exemptions to disclosing some information, but these are more limited as a person has a right to know what information is held on them. If a subject access request is made then the Data Protection Officer should be contacted immediately.

20 CHANGES TO THIS POLICY

We reserve the right to change this Policy at any time. Where appropriate, we will notify individuals of those changes by mail or email.

APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

'A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.'

Information Commissioner's Office website

21 IDENTIFYING A DATA BREACH

21.1 A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

21.2 This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security, such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches include:

- leaving a mobile device on a train;
- theft of a bag containing documents;
- destruction of the only copy of a document;
- sending an email or attachment to the wrong recipient;
- leaving paper documents containing personal data in a place accessible to other people.

22 REPORTING A DATA BREACH

22.1 If anyone processing Personal Data for, or on behalf of, the Trust suspects or becomes aware that a data breach may have occurred, either by them, a member of staff, a volunteer, a data processor, or any other individual, then they must immediately contact the School Business Manager, the Headteacher or the Data Protection Officer (DPO), Jason Hampton, ddatadmin@derby.anglican.org.

22.2 The DPO will investigate the report and determine whether a breach has occurred. The DPO will decide if the data breach needs to be reported to the ICO and notified to data subjects. This will depend on the risk to data subjects. This must 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, for example emotional distress, including through:

- loss of control over their data;
- discrimination;
- identify theft or fraud;

- financial loss;
- unauthorised reversal of pseudonymisation (for example, key-coding);
- damage to reputation;
- loss of confidentiality;
- any other significant economic or social disadvantage to the individual(s) concerned.

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO. The DPO will document the decision, whether or not the ICO is notified, in the event it is challenged at a later date by the ICO or an individual affected by the breach.

22.3 Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website or by calling the ICO directly within 72 hours. As required, the DPO will set out:

- a description of the nature of the Personal Data breach including, where possible:
  - the categories and approximate number of individuals concerned;
  - the categories and approximate number of Personal Data records concerned;
- 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 breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

22.4 The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will work with the School and the Trust to promptly inform, in writing, all individuals whose Personal Data has been breached. This notification will set out:

- the name and contact details of the DPO and relevant School, and Trust, contacts;
- 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 DPO will work with the School and the Trust to notify any relevant third parties who can help mitigate the loss to individuals, for example, the police, insurers, banks or credit card companies.

23 INVESTIGATING A SUSPECTED DATA BREACH

23.1 The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. The focus will be on containing any data breach and recovering any Personal Data. Appropriate measures may include:

- remote deactivation of mobile devices;
- shutting down IT systems;
- contacting individuals to whom the information has been disclosed and asking them to delete the information.

23.2 The DPO will work with the School and/or Trust to investigate how and why the data breach occurred. This is critical to ensuring that a similar data breach does not occur again and to enable steps to be taken to prevent this from re-occurring. Technical steps are likely to include investigating, using IT forensics where appropriate, to examine processes, networks and systems to discover:

- what data/systems were accessed;
- how the access occurred;
- how to fix vulnerabilities in the compromised processes or systems;
- how to address failings in controls or processes.
- Other steps are likely to include discussing the matter with individuals involved to appreciate exactly what occurred, and why, and reviewing policies and procedures.

23.3 The DPO will document each breach in a 'Data Breach Risk Assessment' document, irrespective of whether it is reported to the ICO. For each breach, this record will include:

- a description of the breach;
- the Personal Data that has been potentially accessed;
- actions taken to contain and minimise the breach;
- the potential impact of the breach including a risk assessment;
- remedial actions (such as establishing more robust processes or providing further training for individuals).

The document will be reviewed and remedial agreed by those involved in the data breach to minimise the risk of re-occurrence. The document will be stored in the Trust's Google drive folder and a link to the document included in the Data Breach log for review by the Trust Board and Finance Subcommittee.