DIOCESE OF CHICHESTER ACADEMY TRUST

Data Protection Policy

Date Agreed: **May 2017**

Review Date: **May 2018**

Approved by Diocese of Chichester Academy Trust

Revision Record

Revision No.	Date Issued	Prepared By	Approved	Comments
1	May 2017	DC/SJP		

Contents

1. Introduction

1.1 DCAT and its academies (the "**Trust**") is an independent charitable organisation established by the Diocese of Chichester and is a Department for Education approved academy sponsor, to support Diocesan schools. You will be employed by the Trust and must comply with the terms of this policy document.

1.2 The Trust processes Personal Data (as defined below) in order to enable it to provide education and other associated functions (and, additionally, where there is a legal requirement to process the personal data to ensure that it complies with its statutory obligations). This Data Protection Policy ("**Policy**") regulates the way in which the Trust obtains, uses, holds, transfers and processes Personal Data about individuals (including staff, learners, parents or carers and other individuals who come into contact with the Trust) and ensures all of its staff know the rules for protecting Personal Data. Further, it describes individuals' rights in relation to their Personal Data processed by the Trust.

1.3 The Trust has practices in place in relation to its handling of personal information to ensure that the Trust and its staff are acting in accordance with UK laws and regulatory guidance. These practices, together with this Policy and the Freedom of Information Policy ensure that all staff of the Trust fully understand the Trust's obligation to abide by the data privacy laws and regulations of the UK. The Trust is committed to complying with data protection legislation at all times and all its staff are required to comply with this Policy.

1.4 In this Policy, all references to "we" and "our" in this Policy refer to the Trust, unless distinguished in the text.

2. What is Personal Data?

2.1 Personal Data is any information (for example, a person's name) or combination of information about a living person which allows that living person to be identified from that information (for example a first name and an address).

2.2 Examples of Personal Data which may be used by the Trust in its day to day activities include names, addresses (email and property addresses), telephone numbers and other contact details, educational records, CVs, performance reviews, payroll and salary information and images obtained through CCTV.

2.3 The laws governing how we can use Personal Data apply whether the Personal Data is stored electronically (for example, in emails, on IT systems, as part of a database or in a word processed document) or in structured paper records (for example, in paper files, card indexes or filing cabinets).

2.4 Data protection laws are enforced in the UK by the Information Commissioner's Office ("**ICO**"). The Trust maintains a notification with the ICO which sets out how it Processes Personal Data and for what purposes. Our notification can be viewed by visiting https://ico.org.uk/ESDWebPages/DoSearch and searching for Diocese of Chichester Academy Trust, Registration No. ZA127282

3. What Activities are Regulated by this Policy?

3.1 The Trust processes Personal Data (including Sensitive Personal Data, see below for more information) of individuals including its staff, learners, parents or carers, contractors, business contacts, customers, suppliers and any other individuals who come into contact with the Trust, including job applicants, former staff, prospective and former learners, depending on the relationship with them, for a number of purposes, including:

i. provision of education and other associated functions;

ii. personnel record keeping and management employee performance management and professional development;

iii. employee benefits and succession planning;

iv. payroll and pensions;

v. contract performance, including buying and selling goods and services;

vi. recruitment;

vii. business and market development;

viii. building and managing external relationships;

ix. research and development;

x. work and business project scheduling;

xi. knowledge management;

xii. compliance programs and policies;

xiii. security and the prevention of crime; and

xiv. other purposes required by law or regulation and/or as notified to you separately from time to time.

3.2 When the Trust collects, stores, uses, discloses, updates or erases Personal Data for any of these purposes, this is called "Processing". If you make use of Personal Data (eg read, amend, copy, print, delete or send Personal Data to another organisation, whether to another school within the Trust or otherwise) this is also a type of Processing and is subject to the guidelines set out in this Policy.

3.3 We may share Personal Data with schools within the Trust. We may also share Personal Data with any third partyservice providers, such as in relation to our human resources information systems, or other service providers, which we appoint in the future to Process Personal Data on behalf of the Trust.

4. Related Policies and Documents

4.1 Freedom of Information policy
4.2 Accessing Information under the Freedom of Information Act guidance;
4.3 Safeguarding Policy;
4.4 Public Interest Disclosure (Whistleblowing) Policy;
4.5 Other policies and documents may be identified from time to time as circumstances change and may be added to this list.

5. Why Should I Worry about Complying with This Policy?

5.1 The ICO can investigate complaints, audit the Trust's use or other Processing of Personal Data and can take action against the Trust (and you personally in some cases) for breach of these laws. Action may include making the Trust pay a fine and/or stopping the use by the Trust of the Personal Data, which may prevent the Trust from carrying on its educational and associated functions. Organisations who breach one or more laws on Personal Data also often receive negative publicity for the breaches which affects the reputation of the Trust and its activities as a result.

5.2 Each Trust staff member or Third Party is required to read and comply at all times with this Policy. In this Policy, a "Third Party" is anyone who is not employed by the Trust, for example employees of other schools, agents, external organisations, consultants, contractors, and service providers.

6. What Does "Fair and Lawful Use of Personal Data" Mean?

6.1 One of the main data protection obligations requires the Trust (and its staff) to process Personal Data fairly and lawfully. In practice, this means that the Trust (and each staff member) must comply with at least one of the following conditions when Processing Personal Data:

7. What is a Privacy Notice?

7.1 When an individual gives the Trust any Personal Data about him or herself, the Trust must make sure the individual knows:

i. that the Trust is responsible for the Processing of their Personal Data;

ii. for what purposes that Personal Data provided to it for;

iii. has sufficient information on any disclosures/transfers of that information to third parties; and

iv. any other information that the individual should receive to ensure the Processing carried out is within his/her reasonable expectations.

7.2 Providing this information is known as providing a "privacy notice". You should give individuals appropriate privacy notices when collecting their Personal Data about them.

7.3 You should only process Personal Data in a manner and for purposes consistent with the relevant privacy notice(s).

7.4 Even with consent or if one of the other lawful reasons for Processing applies, the Trust cannot make any use it wants of Personal Data. All the other rules explained in this Policy still have to be complied with. For example, the Trust still has to satisfy the other requirements described below, such as making sure the information collected is not excessive. Simply because a person has consented to giving you their information doesn't override that restriction. Similarly, Personal Data must not be used in a way which would infringe other laws, for example, for bribery, or racial, age, sexual, or disability discriminatory purposes. To do so would render its collection and use also unlawful (even if with consent).

7.5 Where collecting Personal Data about an individual indirectly (e.g. from a published source), the Trust must inform the individual that it holds that data and the purposes for which that data will be used. You must ensure there is suitable evidence that the provider has the lawful right to disclose these details to the Trust for the envisaged use(s) by the Trust.

8. What is Sensitive Personal Data and what conditions need to be met when dealing with it?

8.1 "Sensitive Personal Data" is Personal Data about a person's race or ethnicity, their physical or mental health, their sexual preference, their religious beliefs, their political views, trade union membership or information accusing an individual of any crime, or about any criminal prosecution against them, and the decision of the court and any punishment. Your Data Protection Officer (see section 20) can provide you with further information on what is Sensitive Personal Data and you should comply with their advice in respect of that data.

8.2 Where collected, Sensitive Personal Data should not be used unless strictly necessary. Extra care must be taken with it (in addition to the normal rules for Personal Data) and it must be kept more securely. Additional restrictions are placed on top of the lawful reasons for Processing Personal Data mentioned above. For example, it is difficult to lawfully use such details without the consent of the individual, which has to be explicit, free, voluntary, in writing and obtained prior to Processing any Sensitive Personal Data.

8.3 The Trust does not generally seek to obtain Sensitive Personal Data unless:

i. the individual concerned agrees in writing that we may do so, on the basis of a full understanding of why the Trust is collecting the data;

ii. to monitor learners' attendance and the reasons for non-attendance;

iii. the Trust needs to do so to meet its obligations or exercise its rights under employment law and/or pastoral duties on behalf of learners; or

iv. in exceptional circumstances such as where the Processing is necessary to prevent and/or detect crime or to protect the vital interests of the individual concerned (ie in "life or death" circumstances).

8.4 Staff should note that the "legitimate interest" criteria described above (in section 3) alone is not enough to process Sensitive Personal Data.

8.5 Sensitive Personal Data should not be emailed or disclosed unless measures are taken to encrypt or otherwise secure that information due to the potential for harm or distress if the email is received by unintended recipients or otherwise goes astray.

8.6 Sensitive Personal Data should be collected and used as little as possible, be kept separate from other details, be subject to more limited and strictly need to know access and used subject to greater security measures than other details.

9. Staff Obligations: Necessary and Accurate

9.1 The Personal Data you collect should be appropriate to and sufficient for the relevant purpose(s) you are collecting it for, but not excessive for that purpose(s). Only Process the data which is necessary for the task; minimise your use of Personal Data rather than maximising it. Don't collect and process more Personal Data than you really need - in the end, it simply adds to the Trust's compliance burden and storage costs. For example, if you will never telephone someone at home, you do not need their home telephone number.

9.2 In addition, you must take care to record and input Personal Data accurately. This is important. There can be serious problems if Personal Data is incorrect. Some Personal Data may change from time to time (such as addresses and contact details, bank accounts and the place of employment). It is important to keep current records up to date. If not there may be serious problems. For example, an employee's salary could be paid into the wrong bank account.

10. How Long Should I Keep Personal Data?

10.1 The Trust cannot keep or retain Personal Data forever. Some records have to be retained for minimum periods by law (such as records on employee payments and their taxation under tax laws). Other records must only be kept while in current use and for a reasonable period afterwards.

10.2 As a general rule, when Personal Data is no longer needed by the Trust for the purposes for which it was collected, this Personal Data should be securely and permanently destroyed as soon as practicable. Any proposed destruction of data must be discussed with your Data Protection Officer (see section 20) prior to any decision being made.

11. What are Individuals' Rights?

11.1 Individuals have certain rights in relation to their Personal Data:

i. the right to access Personal Data held about themselves;

ii. the right to prevent Processing of Personal Data for direct marketing purposes;

iii. the right to have Personal Data corrected;

iv. the right to compensation for any damage/distress suffered from any breach; and

v. the right to be informed of automated decision making about them.

11.2 There may also be occasions where a parent or carer has the right to assert these rights in relation to learners under their care. Different rules may apply to educational records and examinations. If an individual contacts you in relation to any of these rights or to withdraw consent, you must inform your Data Protection Officer (see section 20) promptly.

12. Requests Received for Access to Personal Data

12.1 Individuals can also ask for copies of the Personal Data the Trust holds about them and other details about how the Trust uses their Personal Data (a "**Subject Access Request**"). As mentioned above, there may be instances where a parent or carer asks for copies of Personal Data in relation to a learner under their care.

12.2 Subject to receipt of proof of ID where considered necessary (and further checks where the request is made by a parent or carer in respect of a learner under their care), on receipt of a written request from an individual for access to his/her Personal Data, the Trust will (to the extent requested by the applicant):

i. inform that individual whether the Trust holds Personal Data about him or her;

ii. describe the data it holds, the reason for holding the data and the categories of persons to whom it may disclose the data; and

iii. provide the individual with copies of the Personal Data held about him or her, together with an indication of the source(s) of the data.

12.3 If you receive such an access request, there are special legal rules which must be followed as part of this process. Therefore, any request should be passed on to your Data Protection Officer (see section 20) immediately. There are strict statutory deadlines for responding with which the Trust must comply so you must not delay. The Trust also charges the requestor the statutory fee of £10 before dealing with their request (depending on the amount of information requested, this fee may increase to up to £50 if the request relates to educational records).

12.4 You must not deal with such requests yourself unless authorised to do so by your Data Protection Officer (see section 20).

12.5 If you wish to make a Subject Access Request, please contact your Data Protection Officer (see section 20).

13. What kind of security might be appropriate?

13.1 The Trust must keep all Personal Data secure. This means that the Personal Data must be protected against being accessed by other organisations or individuals (for example, via hacking), from being corrupted (data corruption) or being lost or stolen. The Personal Data must also be protected so the wrong people cannot read or use the details. This applies to details in IT systems, emails and attachments and paper files.

13.2 You must comply with the Trust's security procedures whenever you handle Personal Data. The Trust relies on you to keep data secure and for data security. You must only access and use Personal Data you have a right to and which you properly need to use for your role. You must not access Personal Data held by the Trust for private reasons or to help any unauthorised third party.

13.3 If you work away from the Trust's premises, you must comply with any additional procedures and guidelines issued by the Trust for home working and/or offsite working and any supporting local policies and procedures.

13.4 Extra care is needed to secure Sensitive Personal Data because more damage is likely if it is lost. For example, if details of an individual's medical condition(s) got into the wrong hands it would be very distressing for that individual. Be especially careful if you want to send Sensitive Personal Data to another person - whether that is by fax or email - that it is sufficiently secure and can only be received and accessed by the intended recipient. A password protected attachment is not enough.

13.5 The Trust also recognises that adequate security is important where it arranges for outside service providers to process Personal Data on its behalf. Where such arrangements are established by the Trust, service providers must be bound by written contracts to protect the Personal Data provided to them. See section 15 below for more information.

14. What Should I Do if I Lose Personal Data or I Think There is a Data Security Breach?

14.1 There are potentially significant repercussions for the Trust and the individuals affected arising from a security breach. Where a security breach arises you must:

i. immediately report the details to your academy and **Trust** Data Protection Officers (see section 20) providing them with as much information as you have available;

ii. follow their guidance on dealing with the security breach and keep them up to date with any further information about it that you become aware of; and

iii. not approach any individual data subjects, any other organisations, regulators or make any public announcements about the security breach incident without the prior agreement of your Data Protection Officer (see section 20).

15. Can I Disclose Personal Data to Third Parties?

15.1 A disclosure of Personal Data is a form of Processing. That means that the rules described above, including those in relation to fair and lawful use have to be satisfied. You must not disclose Personal Data to a third party outside the Trust, including other schools within the Trust, unless that disclosure constitutes a lawful reason for Processing and satisfies the privacy notice requirements as explained above. Your Data Protection Officer (see section 20) will be happy to discuss this with you.

15.2 There are some exceptions to deal with disclosures such as those requested lawfully by police where the information is necessary to prevent or detect a crime. If you receive a request for information about an individual from government, police or other similar bodies or from journalists or other investigators you should pass that request immediately to your Data Protection Officer (see section 20) to be dealt with. The application of the relevant exceptions needs careful consideration.

15.3 Unlawful disclosure (however well-meaning and however seemingly authoritative the requestor) risks placing the Trust in breach of several obligations under data protection legislation. Special care is needed with telephone requests for information, often used by unauthorised parties to obtain Personal Data to which they are not entitled. Always make sure you are certain who you are dealing with, ideally have a written request for information and ensure any disclosures are justified in advance.

15.4 Access to Personal Data must be restricted to those employees of the Trust and Third Parties who need to access it in order to perform their role. You must only process Personal Data where and to the extent you need to see and process it to carry out your job / role properly.

15.5 The Trust may use Third Parties to provide services to it - for example, running its IT systems or to run a marketing campaign. Where such Third Parties use the Trust's Personal Data, special rules apply. The Trust must have in place a written contract with that Third Party which contains specific limitations on what they can do with the Personal Data and places security obligations upon them. Please contact your Data Protection Officer (see section 20) who will be able to provide you with the appropriate wording to include. You must not contract with such a Third Party without this wording being included.

15.6 The Trust is responsible for their use of its Personal Data and so this is important.

16. Can I Send Personal Data Overseas?

16.1 There are special rules on whether Personal Data collected in the UK can be transferred to another country. Within the EU, there are restrictions on the transfer of Personal Data outside of the EEA (such a transfer can happen, for example, where Personal Data is emailed outside the EEA; where the Trust IT servers are hosted outside the EEA; or where you log in from outside the EEA to an IT system within the EEA). This is to make sure the Personal Data remains safe and the individuals concerned do not lose the protection and rights they have under local law in respect of their Personal Data when transferred.

16.2 If you plan to make any new transfers of any Personal Data to another jurisdiction, please contact your Data Protection Officer (see section 20) in advance to discuss any compliance measures that may be required.

16.3 The fact that there will be transfers of Personal Data to other countries, especially to outside the EEA, should be clearly set out in the privacy notices described in section 7 of this Policy so that it is expected by the affected individuals.

17. Equality Analysis

17.1 By virtue of the provisions of the Equality Act 2010, the Trust has a duty to have due regard to the need to:

i. eliminate unlawful discrimination, harassment and victimisation and other prohibited conduct;
ii. advance equality of opportunity between people of different groups;
iii. foster good relations between people from different groups.

17.2 In implementing this Policy and associated procedures, the Trust will actively take these aims into account as part of its decision making process and will demonstrate how this has been undertaken.

17.3 Where necessary a full equality impact assessment will be undertaken.

18. Complaints

18.1 Complaints will be dealt with in accordance with the Trust's complaints policy. Staff should be aware that individuals may complain to the ICO about the Trust's practices relating to Personal Data.

19. Implementation, Monitoring and Review of this Policy

19.1 This Policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Trust's Chief Executive Officer, or nominated representative.

20. Data Protection Officers and Contacts

20.1 The Data Controller is DCAT.

20.2 The Chief Financial Officer, **[Mr Darren Carpenter]** is the Trust's **Data Protection Officer** and the named contact for the purpose of this policy. Tel: 01273 425001, Email: contact@dcat.academy

20.3 Each school in the Trust has a Data Protection Officer and a named contact for the purpose of this policy as follows: [NB: academies to update as necessary]

School Name	Contact	Email address/Tel No.
All Saint's CE Junior Academy	Ms A Brignall	finance@allsaintscejunioracademy.org Tel: 01424 421397
St Leonard's CEP Academy	Marie Burgess – Headteacher	head@stleonardsceprimaryacademy.org Tel: 01424 422950
St Paul's CE Academy	D Lewis H Wallbank	dlewis@stpaulsceacademy.org hwallbank@stpaulsceacademy.org Tel: 01424 424530
St Catherine's College	Ms M Milligan	mmilligan@stcatherines.college Tel: 01323 465400
Central CE Academy	S Farrell	sbm@centralschool-chichester.org.uk Tel: 01243 783709
Christ Church CE Primary and Nursery Academy	Mrs A Hanney	ahanney@christchurch.e-sussex.sch.uk Tel: 01424 422953

20.4 Further advice and information for individuals and organisations about data protection legislation is available from the Information Commissioner's Office, https://ico.org.uk or by phone: 0303 123 1113 (local rate) or 01625 545 745 (national rate).

APPENDIX 1

Privacy Notices:

Information about **pupils** in academies, alternative provision, pupil referral units and children in early years settings

[Suggested wording for academies]

Data Protection Act 1998: How we use pupil information

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school, local authority and/or the Department for Education (DfE). We use this personal data to:

- support our pupils' learning
- monitor and report on their progress
- provide appropriate pastoral care; and
- assess the quality of our services

This information will include their contact details, national curriculum assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics such as their ethnic group, any special educational needs they may have as well as relevant medical information. For pupils enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about your learning or qualifications.

[For institutions with students aged 13+]
Once our pupils reach the age of 13, the law requires us to pass on certain information to [insert name of local authority or the provider of Youth Support Services in your area] who have responsibilities in relation to the education or training of 13-19 year olds. We may also share certain personal data relating to children aged 16 and over with post-16 education and training providers in order to secure appropriate services for them. A parent/guardian can request that **only** their child's name, address and date of birth be passed to [insert name of local authority or the provider of Youth Support Services in your area] by informing [insert name of academy administrator]. This right is transferred to the child once he/she reaches the age 16. For more information about services for young people, please go to our local authority website [insert link].

[Careers guidance – schools that pass young people's information to careers guidance services or the national careers service may wish to set out details here.]

We will not give information about our pupils to anyone without your consent unless the law and our policies allow us to do so. If you want to receive a copy of the information about your son/daughter that we hold, please contact:

- [insert name/contact details of your academy administrator].

[For academy and free school use only:] We are required, by law, to pass some information about our pupils to the Department for Education (DfE). This information will, in turn, then be made available for use by the LA.

DfE may also share pupil level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998.

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to pupil level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit: https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: https://www.gov.uk/government/publications/national-pupil-database-requests-received

If you need more information about how our local authority and/or DfE collect and use your information, please visit:

- our local authority at [insert relevant LA website link]; or
- the DfE website at https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

APPENDIX 2

Privacy Notices:

The academy workforce: those employed to teach, or otherwise engaged to work at, an academy or a local authority

[Suggested wording for academies]

The Data Protection Act 1998: How we use your information

We process personal data relating to those we employ to work at, or otherwise engage to work at, our academy / local authority [delete as appropriate]. This is for employment purposes to assist in the running of the academy / authority [delete as appropriate] and/or to enable individuals to be paid. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body

This personal data includes identifiers such as names and National Insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- our local authority [for use by academies only - delete if not appropriate]
- the Department for Education (DfE)

If you require more information about how we and/or DfE store and use your personal data please visit:

- our website [Insert LA's relevant website page]
- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you want to see a copy of information about you that we hold, please contact:

- [Insert your relevant academy/LA contact's name and contact details here]

APPENDIX 3

Privacy Notices:

Children in need or children looked after

: information held by local authorities

[Suggested wording for academies]

The Data Protection Act 1998: How we use your information

We collect and process information about children in our care and children to whom we provide services. We use this personal data to:

- support these children and monitor their progress
- provide them with pastoral care; and
- assess the quality of our services

We will not give information about children in our care to anyone without relevant consent unless the law and our policies allow us to do so.

We are required, by law, to pass on some of this information to the Department for Education (DfE) which uses it to; develop national policies, manage local authority performance, administer and allocate funding and identify and encourage good practice.

DfE may share child level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998.

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to pupil level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit: https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: https://www.gov.uk/government/publications/national-pupil-database-requests-received

If you require more information about how we and/or the DfE use this information, please visit:

- our website at: [insert your website link]
- the DfE's website at: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

or write to us at:

- [Insert details and link to the appropriate contact at your LA]

If you are within one of these groups of children and want to see a copy of information about you that we hold, please contact:

- [Insert your relevant LA contact's name and contact details here]