



# General Data Protection September 2019

*Office use*

<b>Published:</b> May 2018 Reviewed: May 2019 & September 2019 – minor amendments	<b>Next review:</b> September 2020	<b>Statutory/non:</b> Statutory	<b>Lead:</b> Alison Elway Data Protection Officer
<b>Associated documents:</b>			
Diverse Academies <a href="http://www.dalp.org.uk">www.dalp.org.uk</a> : Privacy Notices Information Services CCTV policy		Photography and Videography Subject Access Request information Retention policy Data Breach policy	
<b>Links to:</b>			
General Data Protection Regulation <a href="https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/">https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/</a> Records Management policy and retention guidelines <a href="http://irms.org.uk/page/SchoolsToolkit">http://irms.org.uk/page/SchoolsToolkit</a>		Freedom of Information Act <a href="https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/">https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/</a>	

## Contents

1	Policy statement .....	3
2	Basis for processing.....	4
3	Consent .....	5
4	Data Controller and Data Protection Officer .....	6
5	Personal details .....	7
6	Biometric data.....	7
7	Subject Access Requests (SAR).....	8
8	Photographic Images .....	8
9	CCTV .....	8
10	Data breaches .....	8
11	Confidential waste .....	9
12	Queries .....	9
13	Complaints.....	9
14	Other policies in connection with this policy can be found on our website <a href="http://www.dalp.org.uk">www.dalp.org.uk</a> .	10
15	Definitions .....	10

## 1 Policy statement

Diverse Academies is committed to a policy of protecting the rights and privacy of individuals, including students, staff, members/trustees/governors and parents/carers, in accordance with the General Data Protection Regulation (GDPR) which replaced the Data Protection Act (DPA) 1998 and which came into force on 25 May 2018. GDPR was a European Directive and the rules contained within it had to be encompassed into the laws of all countries that were part of the European Economic Area including the UK.

Since the DPA became law the use of the internet, social media sites, use of computers and methods of communicating with each other has changed significantly. To reflect these changes, the law has been updated to the General Data Protection Regulation (GDPR). The UK's withdrawal from the European Union does not affect GDPR.

The GDPR:

- Defines what is meant by 'personal' data
- Confers rights on 'data subjects' (all living individuals)
- Places obligations on 'data controllers' and 'data processors'
- Creates principles relating to the processing of personal data
- Provides for penalties for failure to comply with the above

There are six 'principles' of GDPR that we have to adhere to when processing personal data. We must and will ensure it is:

1. Processed fairly, lawfully and in a transparent manner
2. Used for specified, explicit and legitimate purposes
3. Used in a way that is adequate, relevant and limited
4. Accurate and kept up-to-date
5. Kept no longer than is necessary
6. Processed in a manner that ensures appropriate security of the data

Under GDPR all data subjects have:

- The right to be informed what information we hold;
- The right of access to any personal data
- The right to rectification if information is inaccurate;
- The right to erasure;
- The right to restrict processing;
- The right to data portability; having data transferred;
- The right to object to the processing of personal data; and,
- Rights in relation to automated decision making and profiling.

## 2 Basis for processing

Legislation is not intended to prevent processing personal data but to ensure it is done fairly and without adversely affecting the rights of the data subject.

For data to be processed fairly, data subjects must be made aware:

1. That the personal data is being processed
2. Why the personal data is being processed
3. What the lawful basis for processing is
4. Whether the personal data will be shared and if so with whom
5. How long it is being kept for
6. Of their rights in relation to the processing of personal data
7. How to raise a complaint with the Information Commissioners Office in relation to the processing

Before any personal data is processed we will conduct impact assessments to:

1. Ensure it is necessary for the performance of a contract with the data subject e.g. employment contract
2. Ensure it is necessary for compliance with a legal obligation e.g. the Education Act 2011
3. Ensure it is necessary to protect the interest of a data subject or another person
4. Ensure it is necessary to carry out tasks in the public interest
5. Ensure it is necessary for the purposes of legitimate interests

We will also ensure that only relevant and necessary information is being gathered.

As a group of academies, we need to gather and process certain information to enable us to provide education and other associated functions for various purposes such as, but not limited to:

1. The recruitment and payment of staff
2. The safety of pupils and staff
3. The administration of programmes of study and courses and allocating the correct teaching resource
4. Student enrolment
5. Examinations and external accreditation
6. Recording student progress, attendance and conduct
7. Collecting fees
8. Complying with legal obligations to funding bodies and government e.g. Department for Education (DfE) and the Education, Skills and Funding Agency (ESFA)

We collect this information in a variety of ways including but not exclusively from:

- Registration forms
- Medication forms

- Common Transfer Files (CTFs) from previous schools
- Staff contract information
- Child protection plans
- Member/Trustee/Governor information

We contract with various organisations who provide services to the Trust including, but not exclusively:

- Payroll providers
- Teachers Pensions and LGPS
- DBS check provider
- Occupational Health
- Legal advice
- Recruitment providers
- SIMs Capita
- Education Welfare and services from the local authority
- Online payment systems
- Parent portals
- School Trip recording
- Safeguarding recording

In order that these services can be provided effectively we are required to transfer personal data of data subjects to the data processors

Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

Contracts with data processors will comply with Data Protection Legislation and contain explicit obligations on the data processor to ensure compliance with the Data Protection Legislation, and compliance with the rights of Data Subjects

### **3 Consent**

If we do not have a legal basis for processing data (described above) we will ensure consent has been obtained from the data subject. We will generally seek consent directly from a student/pupil and whilst GDPR does not set an age related limit as a Trust, we deem this to be the age of 13. However, we recognise that in certain circumstances this may not be appropriate and therefore we may seek consent from an individual with parental responsibility.

If consent is needed we will:

- Inform the data subject of exactly what we intend to do with the information
- Require them to positively confirm that they consent – we cannot ask them to opt-out rather than an opt-in. Consent must be freely given
- Inform the data subject of how they can withdraw their consent and how this can be done
- Keep a record of any consent, including how it was obtained and when.

Diverse Academies understand consent to mean that the individual has been fully informed of the intended processing and has signified their agreement. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

In Diverse Academies we take the collection and control of data very seriously. Any serious infringement of the Act will be treated seriously and may be considered under disciplinary procedures. Each of our academies has a Data Protection Team. Please contact the individual academy if you have any specific queries about your data or for the general helpline please contact [gdpr@dalp.org.uk](mailto:gdpr@dalp.org.uk)

#### **4 Data Controller and Data Protection Officer**

Diverse Academies is made up of two Trusts; Diverse Academies Trust and National Church of England Academy Trust and collectively will be the 'data controllers' under the terms of the legislation – this means each Trust is ultimately responsible for controlling the use and processing of personal data. The Trusts have appointed a Data Protection Officer (DPO) – whose contact details are at the end of this policy, and a GDPR team in each academy who are available to address any concerns regarding the data held by our academies and how it is processed, held and used.

The Senior Leadership Team in each academy are responsible for all day-to-day data protection matters, ensuring that all members of staff, contractors, short-term and voluntary staff and visitors receive training and abide by this policy and for developing and encouraging good information handling within the academies.

Staff members must ensure that:

1. all personal data is kept securely
2. no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party
3. personal data is kept in accordance with the Diverse Academies retention schedule [www.dalp.org.uk](http://www.dalp.org.uk)
4. any queries regarding data protection, including subject access requests and complaints, are promptly advised to the academy GDPR Team and [gdpr@dalp.org.uk](mailto:gdpr@dalp.org.uk)

5. any data protection breaches are swiftly brought to the attention of [gdpr@dalp.org.uk](mailto:gdpr@dalp.org.uk) and that staff are instrumental in resolving breaches
6. where there is uncertainty around a data protection matter advice is sought from [gdpr@dalp.org.uk](mailto:gdpr@dalp.org.uk)
7. privacy notices may be found at [www.dalp.org.uk](http://www.dalp.org.uk)

Details of the Trusts' registration can be found on the Office of the Information Commissioner's website.

Our data registration number for Diverse Academies Trust is ZA096084 and for National Church of England Academy Trust Z278831X

## **5 Personal details**

Diverse Academies will ensure that any forms used to gather data on an individual will contain a statement explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing. Information will be kept in line with our Retention Policy which can be found at [www.dalp.org.uk](http://www.dalp.org.uk)

### **How we use your personal information**

Please refer to our policies on our website [www.dalp.org.uk](http://www.dalp.org.uk):

- Privacy notice for pupils
- Privacy notice for staff
- Privacy notice for Members/Trustees/Governors

## **6 Biometric data**

Biometric Information is information about a person's physical or behavioural characteristics that can be used to identify them, for example, information from their fingerprint. Diverse Academies may use information from a person's fingerprint for the purposes of providing access to the library and catering facilities at the academies.

The information will be used as part of an automated biometric recognition system. This system will take measurements of a fingerprint and convert these measurements into a template to be stored on the system. An image of fingerprint is not stored. The template (i.e. measurements taken from a fingerprint) is what will be used to permit access to services. The academy cannot use the information for any purpose other than those for which it was originally obtained and made known to parents.

In order to be able to use biometric information, the written consent of at least one parent is required. However, consent given by one parent will be overridden if the other parent objects in writing to the use of their child's biometric information. Similarly, if a child objects to this, the academy cannot collect or use his/her biometric information for inclusion on the automated recognition system. Parents/staff can also object to the proposed processing of biometric information at a later stage or withdraw any consent that has previously been given. Please note that any consent, withdrawal of consent or objection from a parent must be in writing. Even if a parent has consented, a child can object or refuse at any time to their biometric information being taken/used. His/her objection does not need to be in writing. The law says that schools/academies must provide reasonable alternative arrangements for students who are not going to use the automated system.

When a child leaves the academy, or if some other reason he/she ceases to use the biometric system, his/her biometric data will be securely deleted.

## **7 Subject Access Requests (SAR)**

Any individual has a right to access personal data relating to them which is held by the Trusts by means of a 'Subject Access Request' (SAR)

Personal data is information relating to an individual and a Subject Access Request may be made in any form e.g. in hard or soft copy in writing, by social media, by email, verbally etc.

Any member of staff receiving a SAR must forward it to the GDPR Team in the academy. Under GDPR regulations, the information will be provided free of charge and will be responded to within a calendar month. Please refer to our SAR form if you would like to request information [www.dalp.org.uk](http://www.dalp.org.uk)

## **8 Photographic Images**

Please see our Photography and Videography Policy [www.dalp.org.uk](http://www.dalp.org.uk)

## **9 CCTV**

Please see our CCTV Policy [www.dalp.org.uk](http://www.dalp.org.uk)

## **10 Data breaches**

Where a data protection breach occurs, or is suspected to have occurred all staff are aware that they need to inform the GDPR team at their academy. The GDPR team will advise the Data Protection Officer as soon as they have received notification of a breach [gdpr@dalp.org.uk](mailto:gdpr@dalp.org.uk) The DPO will work alongside the relevant academy/department(s) to:

- a. minimise the damage

- b. assess the extent of the damage and determine whether the Information Commissioners Office (ICO) should be notified
- c. notify individuals affected as appropriate
- d. ascertain how the breach occurred and, if appropriate, determine how to prevent or minimise future breaches

Please refer to our Data Breach policy [www.dalp.org.uk](http://www.dalp.org.uk)

## 11 Confidential waste

Confidential waste will be securely stored and disposed of in line with our Records Management policy and Retention guidelines [www.dalp.org.uk](http://www.dalp.org.uk). Shredding companies who have been certified as being GDPR compliant will be used to dispose of any secure waste and a record of destruction will be retained.

## 12 Queries

If you have any queries about our policy please contact:

Data Protection Officer – Alison Elway [gdpr@dalp.org.uk](mailto:gdpr@dalp.org.uk)

c/o Diverse Education Centre

Old Hall Drive

Retford

Notts

DN22 7EA

Or any GDPR Team in one of our academies.

Our GDPR link Trustee is Ian Storey who can be contacted on [gdpr@dalp.org.uk](mailto:gdpr@dalp.org.uk)

## 13 Complaints

Any complaints will be dealt with in the first instance according to the Diverse Education Complaints Policy [www.dalp.org.uk](http://www.dalp.org.uk). If the complaint is unresolved by following this policy, any complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at:

Wycliffe House Water Lane

Wilmslow

Cheshire

SK9 5AF

[www.ico.gov.uk](http://www.ico.gov.uk)

or report a concern online at <https://ico.org.uk/concerns>

- Call 0303 123 1113

**14 Other policies in connection with this policy can be found on our website [www.dalp.org.uk](http://www.dalp.org.uk)**

- CCTV
- Records Management policy and retention guidelines
- Freedom of Information Act
- Photography and Videography
- Privacy Notices
- Data Breach
- Subject Access Request

**15 Definitions**

Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); 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
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our workforce (including Members/Trustees/Governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times

Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data 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 also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Workforce	Includes, any individual employed by Trust such as staff and those who volunteer in any capacity including Governors and/or Trustees/Members/parent helpers