General Data Protection September 2021

Office use

Published: May 2018 Reviewed: May 2019 & September 2019 & September 2020 September 2021	**Next review:** September 2022	**Statutory/non:** Statutory	**Lead:** Alison Elway Data Protection Officer
Associated documents:			
Diverse Academies https://www.diverseacademies.org.uk/about-us/policies/ Privacy Notices Information Services CCTV policy		Photography and Videography Subject Access Request information Retention policy Data Breach policy	
Links to:			
UK General Data Protection Regulation https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ Records Management policy and retention guidelines http://irms.org.uk/page/SchoolsToolkit		Freedom of Information Act https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/	

Contents

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 UK General Data Protection Regulation (UK GDPR). The policy sets out the basis on which we will process any personal data we collect from data subjects or that is provided to us by data subjects or other sources.

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as a trust, we will collect, store and process personal data about our pupils, workforce, parents and others. This makes us a data controller in relation to that personal data.

1.2 We are committed to the protection of all personal data and special category personal data for which we are the data controller.

1.3 The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

1.4 All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

1.5 All staff have annual training on their roles and responsibilities for protecting personal data. Students are also advised of how to keep their information safe within the appropriate curriculum lessons.

2 Data protection principles

There are six ‘principles’ of UK 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 - we will take reasonable steps to destroy or amend inaccurate or out-of-date data.
5. Kept no longer than is necessary - we will take all reasonable steps to destroy, or erase from our systems, all personal data which is no longer required.
6. Processed in a manner that ensures appropriate security of the data.

3 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 with third parties 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 the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.
8. Whether the personal data will be transferred outside the European Economic Area ('EEA') and if so the safeguards in place.
9. The existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making.
10. How to raise a complaint with the Information Commissioners Office in relation to the processing.

4 Legal processing activity

For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the data protection legislation. We will normally process personal data under the following legal grounds:

1. Where it is necessary for the performance of a contract with the data subject e.g. employment contract.
2. Where it is necessary to protect the vital interest of a data subject or another person.
3. Where the law otherwise allows us to process the personal data, or we are carrying out a task in the public interest e.g. the Education Act 2011.
4. Where it is necessary for compliance with a legal obligation e.g. not an action in the normal course of educating students.
5. Where none of the above apply then we will seek the consent of the data subject to the processing of their personal data.

5 Processing in line with data subject's rights

We will process all personal data in line with data subject's rights in particular:

- 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 of their personal data.
- The right to data portability; having data transferred.
- The right to object to the processing of personal data.
- Rights in relation to automated decision making and profiling.

6 Special category personal data

When special category personal data (see definition in annex) is being processed then an additional legal ground must apply to that processing. We will normally only process special category personal data under the following legal grounds:

1. Where the processing is necessary for employment law purposes, for example in relation to sickness absence.
2. Where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment.
3. Where the processing is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities.
4. Where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.

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

We will inform data subjects of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a student joins us.

If any data user is in doubt as to whether they can use any personal data for any purpose, then they must contact the Data Protection Officer (DPO) before doing so.

7 Vital Interests

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

8 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 when they reach Year 9 (12/13-year-olds). However, we recognise that in certain circumstances this may not be appropriate and therefore we may seek consent from an individual with parental responsibility for that student.

In relation to students below Year 9, we will seek consent from an individual with parental responsibility for that student.

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 and as a rule we will rely on written consent, however consent may occasionally be given verbally (e.g. in the case of ad-hoc photos). We will always record that this has been 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.

9 Information 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 or 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), Ofsted, health authorities and professionals, the Local Authority.

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 to enable us to pay our employees
- Teachers Pensions and LGPS
- DBS check provider
- Occupational Health
- Legal advice
- Recruitment providers
- Management Information Systems
- Education Welfare and services from the local authority
- Online payment systems to enable parents to pay for school meals, trip, uniforms etc.
- Parent portals/communication systems to enable us to effectively communicate with parents

- School trip recording
- Safeguarding recording
- School meal providers
- HR systems for effective management of staff

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.

The trust will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

In some circumstances we will not share safeguarding information. Please refer to our Child Protection policy.

Further detail is provided in our Schedule of Processing Activities.

10 Data protection impact assessments

In certain circumstances the law requires us to carry out detailed assessments of proposed processing. This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the number of people that this might affect, types of data we will be processing or the way that we intend to do so.

The trust will complete an assessment of any such proposed processing and has a template document which ensures that all relevant matters are considered.

The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

11 Data Controller and Data Protection Officer

Diverse Academies Trust data registration number with the Information Commissioners Office is ZA096084.

Diverse Academies Trust is the 'data controller' under the terms of the legislation – this means the trust is ultimately responsible for controlling the use and processing of personal data. The trust has appointed a Data Protection Officer (DPO). Our DPO is Mrs Alison Elway and she can be contacted on gdpr@diverseacademies.org.uk. The DPO is responsible for ensuring compliance with the data protection legislation and with this policy. The trust has also formed 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.

12 Expectations of staff

Staff members must ensure that:

1. All personal data is kept securely, and personal data is locked in drawers/cupboards.
2. No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.
3. Individual monitors do not show confidential information to passers-by.
4. Paper documents should be shredded in a cross-cut shredder or via secure disposable waste systems. IT assets must be disposed of in accordance with IT policies.
5. Electronic devices must be password protected and locked when not in use.
6. Documents must be collected immediately from printers and photocopiers.
7. Professional email etiquette must be maintained at all times.
8. Personal data is retained in accordance with the Diverse Academies retention schedule (available on request).
9. Any queries regarding data protection, including subject access requests and complaints, are promptly advised to the academy GDPR Team and gdpr@diverseacademies.org.uk
10. Any data protection breaches are swiftly brought to the attention of gdpr@diverseacademies.org.uk and that staff are instrumental in resolving breaches.
11. Where there is uncertainty around a data protection matter advice is sought from gdpr@diverseacademies.org.uk

13 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 taking 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 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.

14 Photographic images

Please see our Photography and Videography policy: https://www.diverseacademies.org.uk/wp-content/uploads/sites/25/2018/08/Photography-and-Videography.pdf

15 CCTV

Please see our CCTV policy:
https://www.diverseacademies.org.uk/wp-content/uploads/sites/25/2018/08/CCTV.pdf

16 Subject access requests (SAR)

Any individual has a right to access personal data relating to them which is held by the trust 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 https://www.diverseacademies.org.uk/wp-content/uploads/sites/25/2018/08/Subject-Access-Request-Form.pdf

17 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@diverseacademies.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 https://www.diverseacademies.org.uk/wp-content/uploads/sites/25/2019/05/Data-Breach-Policy.pdf

18 Confidential waste

Confidential waste will be securely stored and disposed of in line with our records management policy and retention guidelines (available on request). 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.

19 Queries

If you have any queries about our policy, please contact:

Data Protection Officer – Alison Elway gdpr@diverseacademies.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@diverseacademies.org.uk

20 Complaints

Any complaints will be dealt with in the first instance according to the Diverse Education Complaints policy.

https://www.diverseacademies.org.uk/wp-content/uploads/sites/25/2018/08/Concerns-and-complaints.pdf

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

Call 0303 123 1113.

21 Other policies in connection with this policy

Other policies in connection with this policy can be found on our website:
https://www.diverseacademies.org.uk/about-us/policies/

- CCTV

- Records management policy and retention guidelines (available upon request)
- Freedom of information
- Photography and videography
- Privacy notices (for staff, students, parent/carer, member/trustee/governors)
- Data breach
- Subject access request
- Privacy and cookies information can be found at the bottom of the trust and each academy website pages.

22 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