Data Protection Policy 2024-25

Document Control	
Owning Function:	Data Protection Officer
Date Approved by Executive:	
Date Approved by Board:	23.10.24
Next Revision Date:	Term 3 2026/27

Change History	
Date	**Description**
01	Revised to include GDPR requirements.
02	Included new sections to cover wider range of requirements in main policy document. Following annexes removed: • Electronic Information Security Policy (separate Policy) • DPIA (separate guidance) • Lawful basis of processing data (incorporated within Policy) • Personal data breach procedure (separate guidance and referenced in main body). Added Data Champion role (appendix 1). Amended SAR form (appendix 2).

1. Introduction

The University of Chichester Academy Trust ('the Trust') is a group of academies and SCITT operating under a single legal entity. This policy covers all aspects of the Trust's work including the activity of its academies and its SCITT.

The Trust collects and uses personal information, referred to in the General Data Protection Regulation (GDPR) as personal data, about staff, students and pupils, parents/carers, governors, volunteers and other individuals who are involved in academy activity. This information is gathered to enable the provision of state funded education and its associated functions. The Trust is required by law to collect, use and share certain information in the public interest.

2. Purpose

This policy sets out how the Trust, including each if its academies, deal with personal information correctly and securely and in accordance with the General Data Protection Regulations (GDPR), and other related legislation.

This Policy applies to all personal information however it is collected, used, recorded and stored by the Trust including each of its academies and SCITT and whether it is held on paper or electronically.

3. Scope

This policy applies to all staff employed by the Trust, regardless of length of contract, to all Trustees and governors appointed, and to external organisations or individuals undertaking activity or processing data for the benefit of any one of our academies, SCITT or central office. Non-compliance may result in disciplinary action, termination of contract or removal of office or role.

4. What is Personal Information/data?

Personal data includes information that relates to a living person. It is information that identifies an individual either on its own or together with other information that is in the organisation's possession currently or in the future, such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Any form of personal data that is filed, electronically stored or processed is covered by the Data Protection Act 2018 and the General Data Protection Regulations (GDPR). The Data Controller is responsible to observe the legal rights of individuals. Only data that is of specific relevance and importance will be required by the Data Controller, who will ensure that the data is securely stored to maintain an individuals' right of privacy. Personal information data will only be shared with relevant personnel or individuals from related agencies or organisations.

5. The Data Controller

As detailed in the Information Governance Framework, the Trust is the Data Controller and has appointed a Data Protection Officer to oversee its legal obligations and requests for data, with the Local Governing Body overseeing the Trust's legal obligations relevant academy specific data. A Data Champion has been appointed to lead compliance and promote data protection at academy level.

6. Data Protection Principles

The Trust will operate in accordance with the principles of the General Data Protection Regulations (GDPR) and comply with duties stated in the regulations. Personal data:

1. will be processed lawfully, fairly and in a transparent manner.

2. will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. collected will not be excessive and will be adequate, relevant and limited to what is necessary to the purposes for which it is processed (data minimisation).

4. will be accurate and kept up to date.

5. will be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

6. shall be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

7. will not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

8. available to data subjects where they are entitled to exercise certain rights in relation to their personal data.

7. Lawful Basis for Processing Data

The UK GDPR provides six lawful bases for processing personal data. The Trust will only process personal data where it is necessary, and it has identified at least one valid lawful basis. The appropriate lawful basis will be determined by the specific purpose and context of the processing:

- **Public task:** Necessary to perform a task in the public interest or for an official function, which has a clear basis in law.
- **Contract**: Necessary for fulfilling a contract or, in order to take steps at the individual's request in order to enter into a contract.
- **Legal obligation**: Necessary to comply with the law (excluding contracts).
- **Vital interest**: Necessary to protect the life of an individual.
- **Legitimate interest**: Necessary for the Trust's legitimate interests or the legitimate interest of another party, unless this is good reason to protect the individual, which over-rides the legitimate interest.
- **Consent**: Must be freely given, specific, informed and unambiguous. The data subject must be informed of their absolute right to withdraw consent at any time.

8. Personal Data about Children and Young People

Children have the same rights as adults over their personal data and can exercise their own rights, provided they are competent to do so. Where a child is not considered to be competent, an adult with parental responsibility may exercise the child's data protection rights on their behalf.

This Policy applies equally to children as it does to adults. When dealing with Personal Data belonging to a child/young person the following considerations will be given:

- when relying on consent, we will make sure that the child understands what they are consenting to, and we do not exploit any imbalance in power in the relationship between us;
- when relying on 'necessary for the performance of a contract', we will consider the child's competence to understand what they are agreeing to, and to enter in to a contract;
- when relying upon 'legitimate interests', we will take responsibility for identifying the risks and consequences of the processing and put age-appropriate safeguards in place.
- The right to erasure is particularly relevant when an individual originally gave their consent to processing when they were a child.

9. Special Category Data

In some circumstances, the Trust will process special categories of personal data, also known as

sensitive data, as defined by data protection legislation. This includes data concerning an individual's:

- race or origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- health;
- sex life;
- sexual orientation;
- genetic data; and
- biometric data

To process special category data, the Trust must have satisfied both a lawful basis for the processing and one (or more) conditions, e.g. explicit consent, that apply to this type of data and the data subject gives explicit consent to the processing.

In addition, the Trust will process personal data relating to criminal convictions and offences for the purpose of determining suitability during the recruitment of staff, volunteers, governors and trustees, contractors and any other provider of services to the Trust or its academies for safeguarding purposes and preventing fraud.

10. CCTV

A number of our academies use CCTV in various locations to ensure the site remains safe. We will adhere to the ICO's code of practice for the use of CCTV, pp.12-19. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded.

Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about academy CCTV systems should be directed to the academy themselves. Any enquiries about CCTV at other locations should be sent to unicat@chi.ac.uk.

11. Relationship with Existing Policies

This policy forms part of the Trust's Information Governance framework. It should be read in conjunction with the following policies:

- Privacy Notice
- Data Retention and Deletion Policy
- Electronic Information Security Policy
- Freedom of Information Policy
- Photography Policy
- Critical Incident Plan of relevant academy

12. Legislation and Guidance

This policy provides information about how we meet the requirements of the Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR). It is based on guidance published by the Information Commissioner' Office (ICO), the UK regulatory body for data protection.

13. Management

All staff with management responsibilities are responsible for ensuring compliance with this policy and must implement appropriate practices, processes, controls and training to ensure such compliance.

The Data Protection Officer (DPO) is responsible for overseeing this policy and, as applicable, developing additional guidance and procedures. The DPO will be a link to the data champions, LGB, ICO and report to the Finance and Audit Committee. The Trust's DPO is Louise Birch, who is contactable on unicat@chi.ac.uk or on 01243 793500.

Please contact the DPO with any questions about the operation of this policy or the applicable data protection legislation or if you have any concerns that this policy is not being or has not been

followed. You must always contact the DPO in the following circumstances:

- if there has been a Data Breach;
- if you are intending to transfer Personal Data outside the EEA;
- if a Data Subject invokes their rights, for example, to a copy of all data we hold on them, or their right to be forgotten (see below);
- If you receive a Freedom of Information Request
- whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see below);
- if you plan to use Personal Data for purposes others than what it was collected for; or
- If you plan to undertake any activities involving Automated Processing or Automated Decision-Making (see below).

Each academy has a named Data Champion (DC) with responsibility for data activity and protection at academy level, **appendix 1** refers. The DC will be the first point of contact within the academy for parents and the local community and keep the DPO informed of any breaches in data control.

14. Consent

Where we rely on the Consent of the data subject as our lawful basis for Processing, Consent will be indicated clearly either by a statement or positive action in respect of the Processing. We will not use silence, pre-ticked boxes or inactivity as an indication of consent.

Where we rely on Consent for Processing Special Categories of Personal Data, that consent must be explicitly given. Usually, we will be relying on another legal basis (and so will not require explicit consent) to Process most types of Special Categories of Personal Data. Where explicit consent is required, the data subject will be issued with a Privacy Notice to capture explicit consent.

Data Subjects may withdraw their consent at any time and this will be promptly honoured. To withdraw consent, you should contact the academy's Headteacher or Data Champion. Consent can also be revoked by contacting the DPO at unicat@chi.ac.uk.

15. Privacy Notice

Whenever we collect Personal Data directly from Data Subjects we will provide the Data Subject with reference to the Trust's Privacy notice available to download on its website, or provide a Privacy Notice that states the identity of the Data Controller and DPO and how and why we will use, process, disclose, protect and retain that Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), the Data Subject will receive details of the Trust's Privacy notice as soon as possible after collecting/receiving the data. We also require our third party processors to collect data in accordance with the applicable data protection legislation and on a basis, which allows for our proposed Processing of that Personal Data.

The academies will issue Privacy Notices (also known as a Fair Processing Notices), as required, when students/pupils join their academy and will be available to view on the academy's website. If these notices are reviewed or changed, eligible parents/carers and students will be notified. These notices summarise the personal information held about pupils/students, the purpose for which it is held and who it may be legitimately shared with in order to deliver the academy's public duty. It also provides information about an individual's rights in respect of their personal data. Central HR will take responsibility for updating staff privacy notices.

16. Sharing Personal Data

Generally, Personal Data should not be shared with third parties unless certain safeguards and contractual arrangements have been put in place.

The Trust however, may share personal data held with another staff member, or other representative of the Trust or third party if the recipient has a need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

Any Personal Data we hold shared with third parties, such as our service providers, must be on the basis that:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions; and
- a fully executed written contract that contains Trust Solicitor approved third-party clauses has been obtained.

17. Reporting a Data Breach

The applicable data protection legislation requires all organisations to report certain types of data breach to the relevant supervisory authority within 72 hours, and in some cases to the Data Subjects individuals affected.

We have put in place procedures to deal with any suspected Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO, or if the DPO is unavailable, the Data Champion or Headteacher and follow the Data Security Breach Management Process. You should preserve all evidence relating to the potential Data Breach.

18. Subject Access Request (SAR)

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. Individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

Requests should be made in writing to the academy's headteacher or data champion. Although not a requirement, appendix 2, provides a template form to request a SAR.

Information will be provided free of charge unless a request is considered manifestly unfounded or excessive, particularly if it is repetitive. In addition, a charge may be applicable if the individual requests copies of information already supplied and will be based on the administrative cost of providing the information. The individual will be informed if a charge applies.

The individual will receive acknowledgement of the request and informed when they will receive the data requested, if eligible. This will be within one month of the request, unless the period needs to be extended due to the request being complex, numerous or for another significant factor. The extension will be up to a further two months. The individual will be notified of such an extension and the reason why.

Where a request is refused, the individual will receive an explanation why and will be informed of right to complain to the ICO authority and to a judicial remedy without undue delay and at the latest within one month.

It is important that only subject data is given to the individual or, to a nominated person. Before providing the data, it is therefore important to verify the identity of the person making the request, if the request does not provide sufficient assurance. This could mean refusal of a request until further information is given.

For requests made electronically, the information will normally be provided electronically, but this may not always be the case.

Where a request is for a large quantity of information about an individual, the GDPR permits the Trust to ask the individual to specify the information the request relates to (recital 63).

For the purpose of monitoring and recording requests, the DPO retains a central record of requests. Academies should contact the DPO for support in responding to SARs.

19. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law;
- Completing data protection impact assessments (DPIA) where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, when using new systems and when introducing new technologies. Separate guidance and procedures are in place for DPIAs.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly train members of staff on data protection law, this policy, any related policies, and any other data protection matters; record of attendance will be retained in accordance with the Retention Policy.
- Regularly conduct reviews and audits to test privacy measures and ensure compliance.
- Maintain records of processing activities.

20. Data Security and Storage of Records

All individuals who are permitted and hold or have access to personal data has a responsibility to keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage. In particular:

- Papers containing confidential personal data must not be left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access. They should be kept under lock and key when not in use.
- Staff, pupils, governors and trustees must be aware of and comply with the Password Standards policy, device loan agreement (where applicable) and the Electronic Information Security policy.
- Where personal data is shared with a third party, due diligence and compliance checks of the third party should be undertaken to ensure information is stored securely and adequately protected.

21. Disposal of Records

Personal data that is no longer required will be disposed of securely and in line with the Trust's Retention Policy and Retention and Destruction guidance. A log of documents destroyed will be held by the Data Champion or function area.

22. Complaints

Complaints relating to the handling of personal information will be dealt with in the first instance in accordance with the complaints policy and will be overseen by the Data Champion or the Data Protection Officer. The Chair of the LGB will be notified immediately.

23. Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every three years. The policy review will be undertaken by the Data Protection Officer and approved by Trustees of the Finance and Audit Committee.

24. Contacts

If you have any enquires in regard to this policy, please email unicat@chi.ac.uk or call (01243) 793500.

Appendix 1
Role of Data Champion

Data Champions are either members of the senior leadership team across the Trust, or who represent SLT and have responsibility for data protection within a specific function area or academy.

Each academy has a Data Champion who will keep the Data Protection Officer informed of any breaches in data control and will be the first point of contact within the academy for parents and the local community.

The role of the Data Champion is to ensure:

- information is handled and managed properly, keeping the academy's record of data (the database) up to date at all times;
- that Data Impact Assessments are completed for any new type of data processing activity;
- due diligence checklist is completed for all new third-party data processors and that contracts are compliant with GDPR;
- good data protection and GDPR awareness in the school and induction and ongoing training for all staff;
- the promotion and awareness of best practice;
- the Information Asset Register is updated that they have responsibility for;
- compliance with data protection and that appropriate access and security controls are in place;
- the accuracy and integrity of the information is assured and consistent;
- To report to the governing body on any issues which have arisen and the actions taken to resolve them.

Appendix 2
Subject Access Request Form

The following form is optional when requesting a SAR. The SAR should be marked urgent, for the attention of the Data Champion or Headteacher.

Subject Access Request Form

Person requesting information:	
Academy/School:	
Relationship with the academy/school:	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address:	
Preferred method of contact i.e telephone, text message, e-mail, in-person:	
Contact Details (include telephone number and email address).	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* • *Your child's medical records* • *Your child's behavior record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

Reason for request (**optional** – this is requested as it may assist in locating key documents).	`
Signed:	
Dated:	