DIOCESE OF CHICHESTER ACADEMY TRUST

Privacy Notice for Staff, Governors, Trustees and Volunteers

Date Last Reviewed:	**October 2026**

Contents

Introduction 1
Lawful Basis 1
Collecting Information 2
The Categories of Information That We Collect, Process, Hold and Share 2
Purpose of Collection of Information 3
  Candidates Privacy Notices 5
  How We Collect This Information 7
How We Use Particularly Sensitive Information 7
Criminal Convictions 8
Automated Decision Making 8
Sharing Data 9
Storing your data 9
Who we Share Information With 10
Why we Share Your Information 10
Requesting Access to Your Personal Data and Your Data Protection Rights 10
Complaints 11
Contact us 12
Changes to This Privacy Notice 12

Introduction

The Diocese of Chichester Academy Trust is committed to protecting the privacy and security of your personal information. This privacy notice explains how the Diocese of Chichester Academy Trust (DCAT) collect, store and use personal data about individuals working in its schools in a voluntary capacity, including volunteers, governors and trustees. If it, or any information linked to it is unclear, please contact DCAT on 01273 425001 or contact@dcat.academy, or the Trust's Data Protection Officer:
The Diocese of Chichester Academy Trust (DCAT) is the data controller responsible for the personal information covered by this privacy notice. The Trust's Data Protection Officer is Handsam Ltd.
Handsam Ltd
27 East Moons Moat Business Centre
Oxleaslow Road
Redditch
Worcestershire
B98 0RE.
Email: info@handsam.co.uk
Telephone: 03332 070737

This privacy notice applies to current and former employees, workers and contractors, volunteers, governors, trustees and Trust members, as applicable. Separate privacy information may apply to job applicants and to particular processing activities where additional or more specific information is required.

Lawful Basis

Our lawful basis for collecting and processing your information is defined under Article 6 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation), and the following subparagraphs in the GDPR apply:

- (c) Processing is necessary to comply with the legal obligations of the controller.
- (e) Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education).

Our lawful basis for collecting and processing your information is also further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special, information and the following subparagraphs in the GDPR apply:

- The data subject has given explicit consent.
- It is necessary to fulfil the obligations of controller or of data subject.
- Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions).
- It is in the public interest.

Collecting Information

The Diocese of Chichester Academy Trust is a "data controller." This means that we are responsible for deciding how we hold and use personal information about you.
We are required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Where we obtain personal information about you from another source, this may include information provided by your appointing body, previous or current employers, the DBS, government departments, local authorities, professional advisers, occupational health providers, referees, recruitment agencies or other relevant third parties.

The Categories of Information That We Collect, Process, Hold and Share

The categories of information that we collect, hold and share include but are not limited to:

- Personal information (such as name, title, addresses, date of birth, marital status, national insurance number);
- Contact details and preference (phone numbers and personal email addresses);
- Emergency contact information (such as names, relationship, phone numbers and email addresses);
- Your business or other charitable interests;
- Information collected during the recruitment process that we retain during your employment / term of office including references, proof of right to work in the UK, application form, CV, qualifications, education and training details;
- Employment contract information such as start dates, hours worked, post, roles;
- Details of salary and benefits including payment details, payroll records, tax status information, national insurance number, pension and benefits information;
- Details of any dependants;
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;
- Information in your sickness and absence records such as number of absences and reasons (including sensitive personal information regarding your physical and/or mental health);
- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief, where this has been provided;
- Criminal records information as required by law to enable you to work with children;
- Your trade union membership;
- Information on grievances raised by or involving you;
- Information on conduct and/or other disciplinary issues involving you;
- Details of your appraisals, performance reviews and capability issues;
- Details of your time and attendance records;
- Information about the use of our IT, communications and other systems, and other monitoring information;

- Details of your use of business-related social media;
- Photographs (for internal safeguarding & security purposes, school newsletters, media and promotional purposes);
- Images of staff captured by the Trust/School's CCTV system;
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within the Trust/School, you will be notified separately if this is to occur); and
- Details in references about you that we give to others.

Specifically for governors and trustees:

- Details of your qualifications, skills, and experience for skills audit purposes;
- Details of your appointment, including the appointing body, the date of appointment, and term of office;
- Training you have attended in your role as a governor or trustee;
- Your attendance and visits to the school in your role as a governor or trustee;
- Any roles or leadership responsibilities you hold within the governing body and trust board; and
- Details in references about you that we give to others.

We may also hold personal data about you from third parties, such as information supplied by the appointing body and from the Disclosure & Barring Service, to comply with our legal obligations and statutory guidance.

Purpose of Collection of Information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. We need all the categories of information in the list below primarily to allow us to perform our contract with you and to enable us comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain your information to us or if you have a choice in this. Where we have obtained consent to use your personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn. Please note that we may process your information without your knowledge or consent, where this is required or permitted by law.

The situations in which we will process your personal information are listed below: -

- To determine recruitment and selection decisions on prospective employees;
- In order to carry out effective performance of the employee's contract of employment and to maintain employment records;
- To comply with regulatory requirements and good employment practice;
- To carry out vetting and screening of applicants and current staff in accordance with regulatory and legislative requirements;
- Enable the development of a comprehensive picture of the workforce and how it is deployed and managed;
- To enable management and planning of the workforce, including accounting and auditing;
- Personnel management including retention, sickness and attendance;
- Performance reviews, managing performance and determining performance requirements;

- In order to manage internal policy and procedure;
- Human resources administration including pensions, payroll and benefits;
- To determine qualifications for a particular job or task, including decisions about promotions;
- Evidence for possible disciplinary or grievance processes;
- Complying with legal obligations;
- To monitor and manage staff access to our systems and facilities in order to protect our networks, the personal data of our employees and for the purposes of safeguarding;
- To monitor and protect the security of our network and information, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution;
- Education, training and development activities;
- To monitor compliance with equal opportunities legislation;
- To answer questions from insurers in respect of any insurance policies which relate to you;
- Determinations about continued employment or engagement;
- Arrangements for the termination of the working relationship;
- Dealing with post-termination arrangements;
- Health and safety obligations;
- Prevention and detection of fraud or other criminal offences; and
- To defend the Trust/School in respect of any investigation or court proceedings and to comply with any court or tribunal order for disclosure.

Specifically for governors, trustees and volunteers:

- Enable you to serve as a governor, trustee or volunteer;
- Enable us to comply with our statutory safeguarding obligations;
- Ensure we comply with our instrument of governance/terms of reference;
- Support effective governor development;
- Support effective management of the school;
- Fulfil statutory reporting to the Department for Education;
- Complete equalities monitoring and reporting;
- Respond to any governance issues;
- Improve the management of workforce data across the sector;
- Support the work of the school teachers' review body;
- Assess the quality of our services; and
- Comply with the law regarding data sharing.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Candidates Privacy Notices

As part of any recruitment process, the Trust collects and processes personal data relating to job applicants. The Trust is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the Trust collect?

The Trust collects a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- whether you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process;
- information about your entitlement to work in the UK; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health, and religion or belief.

The Trust collects this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment.

The Trust will also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Why does the Trust process personal data?

The Trust needs to process data to take steps at your request prior to entering into a contract with you. It also needs to process your data to enter into a contract with you.

In some cases, the Trust needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

The Trust has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the Trust to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The Trust may also need to process data from job applicants to respond to and defend against legal claims.

The Trust processes health information if it needs to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to carry out its obligations and exercise specific rights in relation to employment.

Where the Trust processes other special categories of data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is for equal opportunities monitoring purposes as permitted by the Data Protection Act 2018/reasons of substantial public interest.

For some roles, the Trust seeks information about criminal convictions and offences. Where the Trust seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment/it to comply with a regulatory requirement to establish whether an individual has committed an unlawful act or been involved in dishonesty or other improper conduct/the purposes of preventing or detecting unlawful acts.

The Trust will not use your data for any purpose other than the recruitment exercise for which you have applied.

Who has access to data?

Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles and with your current and former employers to obtain references for you, unless you have indicated on the application form that you would like these not to be contacted prior to an offer of employment.

The Trust will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. The Trust will then share your data with, former employers to obtain references for you (if not already obtained prior to interview), employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks. All references are marked as confidential in line with the ICO guidance.

The organisation will not transfer your data outside the UK.

How does the Trust protect data?

The Trust takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties.

For how long does the Trust keep data?

If your application for employment is unsuccessful, the Trust will hold your data on file for six months after the end of the relevant recruitment process. At the end of that period, your data is deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment and for six years after the termination date of your employment. The periods for which your data will be held will be provided to you in a new privacy notice.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing; and

- ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether your interests override the organisation's legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact [name, contact email or address].

If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to the organisation during the recruitment process. However, if you do not provide the information, the organisation may not be able to process your application properly or at all. If your application is successful, it will be a condition of any job offer that you provide evidence of your right to work in the UK and satisfactory references.

You are under no obligation to provide information for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such information.

How We Collect This Information

The Trust and its schools use technical and organisational systems to protect staff, pupils, volunteers, governors, trustees, visitors and the Trust's information systems. These may include network monitoring, email and internet monitoring, filtering, malware and security monitoring, access-control systems, CCTV, device management, audit logs and other security technologies. These systems may process information about your use of Trust systems, devices, networks, email, internet services and other communications systems. Such processing may be necessary for safeguarding, online safety, cybersecurity, prevention of unauthorised access, investigation of incidents, compliance with policies and legal obligations, and the protection of individuals and Trust information. Further information may be provided through the Trust's acceptable-use, online-safety, filtering and monitoring, CCTV and information-security policies.

We may collect this information from you, your personnel records, the Home Office, pension administrators, your doctors, from medical and occupational health professionals we engage, the DBS, your trade union, other employees, other professionals we may engage (e.g. to advise us generally), automated monitoring of our websites and technical systems such as our computer networks and connections, CCTV and access control systems, remote access systems, email and instant messaging systems, intranet and internet facilities.

How We Use Particularly Sensitive Information

Special category personal data requires additional protection because it is particularly sensitive. We will only process special category data where we have both an Article 6 lawful basis and a separate Article 9 condition under the UK GDPR. Where required, we will also satisfy the relevant condition in Schedule 1 to the Data Protection Act 2018 and maintain an appropriate policy document.

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring (or in relation to our pension scheme);
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards. Less commonly, we may process this type of information where it

is needed in relation to legal claims or where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent.

We will use this information in the following ways: -

- Collecting information relating to leave of absence, which may include sickness absence or family related leave;
- To comply with employment and other laws;
- Collecting information about your physical or mental health, or disability status, to ensure your health and welfare in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to manage sickness absence and to administer benefits;
- Collecting information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- To record trade union membership information to pay trade union premiums and to comply with employment law obligations.

Criminal Convictions

Information relating to criminal convictions and offences is subject to additional legal safeguards. We will only process such information where authorised by UK law and where the requirements of Article 10 of the UK GDPR and, where applicable, the Data Protection Act 2018 are satisfied.

Where appropriate we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of working for us.

Automated Decision Making

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision making in the following circumstances: -

- Where we have notified you of the decision and given you 21 days to request a reconsideration;
- Where it is necessary to perform the contract with you and appropriate measures are put in place to safeguard your rights; or
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

Where we use solely automated decision-making that produces or is likely to produce a legal or similarly significant effect on you, we will comply with the requirements of the UK GDPR as amended by the Data (Use and Access) Act 2025.

Where applicable, appropriate safeguards will include providing information about the decision, enabling you to make representations about the decision, enabling you to obtain human intervention, and enabling you to contest the decision.

Where special category data is used in solely automated decision-making with a significant effect, additional restrictions apply.

Where we use profiling or automated processing that does not constitute solely automated decision-making with a legal or similarly significant effect, we will provide appropriate information about that processing where required. You will not be subject to decisions that will have a significant impact on

you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

Sharing Data

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. These include the following: -

- the Department for Education (DfE);
- Ofsted;
- Other academies within the Trust;
- Prospective Employers;
- Welfare services (such as social services);
- Law enforcement officials such as police, HMRC;
- LADO;
- Training providers;
- Professional advisors such as lawyers and consultants;
- Support services (including HR support, insurance, IT support, information security, pensions and payroll);
- The Local Authority;
- Occupational Health;
- DBS; and
- Recruitment and supply agencies.

Information will be provided to those agencies securely or anonymised where possible.
The recipient of the information will be bound by confidentiality obligations, we require them to respect the security of your data and to treat it in accordance with the law.
We may transfer your personal information outside the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

Storing your data

Any information about you is kept secure and except as otherwise permitted or required by applicable law or regulation, the Trust/School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

To determine the appropriate retention period for personal data, the Trust/School considers the amount, nature, and sensitivity of personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for processing the personal data, whether we can fulfil the purposes of processing by other means and any applicable legal requirements.

Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy. Please refer to our data storage and retention appendices in the GDPR policy.

The Trust/School typically retains personal data for 6 years, subject to any exceptional circumstances or to comply with laws or regulations that require a specific retention period.

We have data protection policies and procedures in place, including strong organisational and technical measures, which are regularly reviewed.

Who we Share Information With

We routinely share information with appropriate third parties, including:

- the Department for Education (DfE);
- Ofsted;
- Other academies within the Trust;
- Prospective Employers;
- Welfare services (such as social services);
- Law enforcement officials such as police, HMRC;
- LADO;
- Training providers;
- Our auditors, to ensure our compliance with our legal obligations;
- Professional advisers and consultants – for us to develop our service to best provide our public service; and
- Police forces, courts, tribunals.
- Support services (including HR support, insurance, IT support, information security, pensions and payroll);
- The Local Authority;
- Occupational Health;
- DBS; and
- Recruitment and supply agencies.

Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law

Why we Share Your Information

We share personal information where this is lawful and necessary for the purposes described in this privacy notice. Depending on the circumstances, the lawful basis may be a legal obligation, performance of a contract, public task, legitimate interests, consent or another lawful basis. Consent is therefore not required for every disclosure.

We do not share information about you with anyone without consent unless the law and our policies allow us to do so. We share personal data with the Department for Education (DfE) on a statutory basis.

Specifically for governors and trustees:

Under s.538 of the Education Act 1996, and the Academies Financial Handbook, the Secretary of State requires boards to provide certain details they hold about people involved in governance, as volunteered by individuals, and the information kept up to date.

Requesting Access to Your Personal Data and Your Data Protection Rights

Under data protection legislation, staff, governors and volunteers have the right to request access to information about them that we hold, through a Subject Access Request.
If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it;
- Tell you why we are holding and processing it, and how long we will keep it for;
- Explain where we got it from, if not from you or your child;
- Tell you who it has been, or will be, shared with;
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this; and
- Give you a copy of the information in an intelligible form.

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

We will respond to a valid Subject Access Request without undue delay and normally within one month of receiving the request, or, where applicable, from the date on which we receive information reasonably required to confirm identity or other information required by law. Where a request is complex or you have made a number of requests, the response period may be extended by up to a further two months where permitted by law. Where we reasonably require clarification of a request in order to respond to it, the time period may be paused until the requested clarification is received. We will carry out a reasonable and proportionate search for the information requested. dpo@dcat.academy

-
- Depending on the circumstances and subject to applicable exemptions and restrictions, you may also have the right to: Object to processing of personal data that is likely to cause, or is causing, damage or distress (however, this will not apply if the data is part of a legal requirement);
- Prevent processing for the purpose of direct marketing;
- Object to decisions being taken by automated means;
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- Claim compensation for damages caused by a breach of the Data Protection regulations.

Complaints

We take data-protection complaints seriously and have a procedure for handling complaints about the way we process personal information. You can make a data-protection complaint to us using the contact details below. We will provide a clear means of making a complaint, acknowledge receipt within 30 days and, without undue delay, take appropriate steps to investigate the complaint, keep you informed about progress and communicate the outcome.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.
To make a complaint, please contact our Data Protection Officer:

Handsam Ltd:
27 East Moons Moat Business Centre
Oxleaslow Road
Redditch

Worcestershire
B98 0RE.
Email: info@handsam.co.uk
Telephone: 03332 070737

Alternatively, or failing a satisfactory conclusion, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer:
Handsam Ltd:
27 East Moons Moat Business Centre
Oxleaslow Road
Redditch
Worcestershire
B98 0RE.

Email: info@handsam.co.uk
Telephone: 03332 070737

Changes to This Privacy Notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.