Chesterfield College Group

Ofsted Good Provider

Data Protection Policy

Policy Family:	Information Governance
Reference Code:	INF03
Issue Number:	7
Originator:	Data Protection Officer and Head of Compliance & BIS
Responsible Manager:	Data Protection Officer and Head of Compliance & BIS
Committee for Approval:	Finance and Corporate Services
Approval Date:	27 November 2024
Issue Date:	02 December 2024
Review Due:	2027/28

Impact Assessment Status: In preparing the Policy, any potential disproportionate impact it might have upon individuals with protected characteristics, as defined in the Equality Act 2010, have been carefully considered. It is the conclusion of the College Group that the Policy does not adversely impact on individuals with any of the protected characteristics.

Contents

Aim

The Data Protection Policy aims to ensure that the Chesterfield College Group explains the responsibilities of staff under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The Chesterfield College Group is committed to being transparent, lawful, and fair about how it collects and uses the personal data of its workforce, students, and stakeholders to ensure it meets its data protection obligations. This policy sets out the college's commitment to data protection, together with rights and obligations in relation to personal data.

Scope

This policy and associated operating procedures apply to Chesterfield College, which includes our subsidiary companies: Training Services 2000 Ltd, Learning Unlimited ATA Ltd, Recruit Unlimited Ltd and Chesterfield College Enterprises Ltd.

The policy applies to the collection, processing, and disposal of all personal and special category data connected to the work, studies, and other activities of Chesterfield College and its subsidiary companies.

The policy sets out the expected behaviours of all Chesterfield College Group employees, including apprentices, agency staff, contractors, governors, consultants, or anyone working on college premises on behalf of the College Group.

Policy Statements

Data Protection Legislation

The Data Protection Policy is informed by and meets the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, all applicable laws relating to the collection and use of personal data and privacy, and any applicable codes of practice issued by a regulator. Throughout this policy, this is referred to collectively as 'data protection legislation'.

The Data Controller

Chesterfield College as a corporate body is the Data Controller with overall control over the purposes and means of the processing of personal data within the College Group. The Corporation Board is ultimately responsible for the implementation of all appropriate policies and procedures to meet the college's obligations as the Data Controller.

The Data Protection Officer

The college's Data Protection Officer is the Head of Compliance and Business Intelligence Systems. The Data Protection Officer is responsible for monitoring day-to-day compliance with data protection legislation and raising awareness of data protection obligations. The Data Protection Officer's contact details will be published on the college website and will be widely available to all staff and students within the college.

Data Protection Business Partners

The following members of staff support the Data Protection Officer on specific aspects of data collection and processing activities:

- Assistant Principal People and Culture – data relating to staff and Health and Safety.
- Head of Information Services – data relating to students and funding agreements.
- Assistant Principal Student Experience and Wellbeing – data relating to enquiries, applications, learning support, safeguarding, and marketing activities.
- Head of Stakeholder Engagement – data relating to employers.
- Head of ICT – information and data security.

Data Protection Principles

Chesterfield College Group complies with the six data protection principles that guide data protection legislation. In summary, the college requires that:

1. Data is processed fairly, lawfully, and in a transparent manner.
2. Data is used for limited, specified, and stated purposes, and is not used or disclosed in any way incompatible with those purposes.
3. Data is adequate, relevant, and limited to what is necessary.
4. Data is accurate and, where necessary, up to date.
5. Data is not kept for longer than necessary.
6. Data is kept safely and securely.

In addition, the accountability principle requires the college to evidence compliance with the above six principles to ensure that individuals are not put at risk through the processing of their personal data. Failure to ensure compliance can result in breach of legislation, reputational damage, or financial penalties. To meet its obligations, the college has appropriate and effective measures in place to ensure compliance with data protection legislation. Staff have access to policies, procedures, and guidance to give them appropriate direction on the application of data protection legislation.

Lawful Use of Personal Data

To collect and/or use personal data, the college must show that the processing is lawful, fair, and transparent. It is not sufficient to show that the processing is lawful if it is fundamentally unfair or hidden from the individual concerned. In addition, when the college collects and/or uses special categories of personal data, it must show that additional conditions are met.

The college will carefully assess how it uses all personal data and document this within an Information Asset Register. If the college changes how it uses personal data, the Information Asset Register must be updated, and individuals may need to be notified about the change. Therefore, any changes to the use of personal data must be approved by the Data Protection Officer in advance so that the Information Asset Register can be updated and individuals notified if applicable.

If the legal basis for collecting and processing personal data is consent, the college will capture and retain this consent together with the version of the privacy notice that accompanied the consent. The college must respect an individual's right to withdraw their consent at any time.

Transparent Processing – Privacy Notice

Where the college collects personal data directly from an individual, the individual will be informed about how their personal data will be used through the appropriate Privacy Notice published on the college website.

If the college changes how it uses personal data, individuals may need to be notified about the change. If staff, therefore, intend to change how they use personal data they must notify the Data Protection Officer, who will decide whether the intended use requires an amendment to the relevant Privacy Notice and any other controls which apply.

Data Quality

Data protection legislation requires that the college only collects and processes personal data to the extent that it is required for the specific purpose(s) notified to the individual in the relevant Privacy Notice and as set out in the Information Asset Register. The college is also required to ensure that the personal data held is accurate and kept up to date.

Students must ensure that all personal data they provide to the college is accurate and up to date. Students must notify the Enrolment Team of any changes to their personal data either in person at the Enrolment Team office, by email to enrolment@chesterfield.ac.uk, or by phone on 01246 500769.

All staff that collect and record personal data must ensure that the personal data is recorded accurately and is kept up to date and must also ensure that they limit the collection and recording of personal data to that which is adequate, relevant, and limited to what is necessary in relation to the purpose for which it is collected and used.

All staff that obtain personal data from sources outside the college must take reasonable steps to ensure that the personal data is recorded accurately, is kept up to date, and is limited to that which is adequate, relevant, and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require staff to independently check the personal data obtained.

The college's quality measures include:

- Correcting personal data in a timely manner if it is discovered to be incorrect, inaccurate, incomplete, ambiguous, misleading, or outdated, even if the individual does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted use or applicable statutory retention period.
- The removal of personal data if in violation of any data protection principles, or if the personal data is no longer required.

The college recognises the importance of ensuring that personal data is amended, rectified, erased, or its use restricted where this is appropriate under data protection legislation.

Data Security

The college takes information security very seriously and has policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure

that data is not accessed except by staff in the proper performance of their duties. Please see the college's Information Security Policy (INF01) and IT Acceptable Use Policy (INF02) for further details.

Staff are personally responsible for ensuring that any personal data they have acquired, manage, process, share, store, or dispose of is kept securely and is not disclosed orally or in writing, accidentally or otherwise, to any unauthorised third party.

Insecure communication channels must not be used to share restricted, confidential, or highly confidential information.

All personal data held on paper records must be kept in a locked filing cabinet or desk drawer. All personal data held electronically must be stored securely, with access only available to those who require it. Holding personal data on removable media or mobile devices is discouraged and the use of encryption is mandatory where this happens.

The college's official cloud storage solution for personal data is OneDrive/Office365. A Data Protection Impact Assessment is mandatory prior to the use of any other cloud-based storage services.

The creation or implementation of new IT systems that include the storage of personal data must consider privacy in the design process. This should include, but is not limited to, the ability to log and manage user access.

Records Management

The college has a legal responsibility not to keep personal data for longer than it is needed for the specific purpose(s) agreed when it was collected. At the end of the agreed period for each type of information, the college will take steps to delete such data from its information systems, databases, and electronic files, and to destroy paper records using agreed, secure processes.

The agreed retention period for each type of information and the reasons for this are documented on the college's Information Asset Register, which provides a central record of all information processed by the college. Further details can be found in the college's Data Retention Policy (INF06).

When setting retention periods, consideration will be given to the following key factors:

- The purpose for which the data was obtained.
- Any specific consents provided by the data subject in relation to the use or retention of the data.
- Whether the original purpose has been fulfilled.
- Whether the data needs to be retained to support any potential legal process.

Data Protection by Design

To meet the requirements of data protection legislation and protect the rights of data subjects, the college is responsible for implementing appropriate technical and organisational measures, such as pseudonymisation and data minimisation, to ensure the necessary safeguards for processing before it can commence processing and at the point of processing.

When designing or implementing new systems or processes, or reviewing or expanding existing systems or processes, a Data Protection Impact Assessment will be conducted which will allow the college to assess the impact of the new or altered processing operations on the protection of personal data.

Data Protection Impact Assessment (DPIA)

Staff must ensure a Data Protection Impact Assessment (DPIA) is completed where a new or amended system or process is likely to result in a high risk to the rights and freedoms of individuals. The nature, scope, context, and purpose(s) of the processing must be considered when assessing the level of risk, particularly when the processing uses new technologies.

It is important to conduct a DPIA to assess the impact of the envisaged processing operations on the protection of personal data. The DPIA will consider the processing operations to assess compliance with approved codes of conduct, the views of data subjects, and the security of the data processing. The process will include consideration of the purposes for which the activity is carried out, the risks to individuals, and the measures that can be put in place to mitigate the risks.

The Data Protection Officer will support staff to complete a Data Protection Impact Assessment where required.

Data Breaches

A personal data breach is defined as any failure to keep personal data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration, or unauthorised disclosure of personal data. All staff are required to understand the internal reporting process for personal data breaches and comply with the strict timeframes set out within the college's Data Breach Notification procedure.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, the affected individuals must be notified and provided with information about the likely consequences and the measures for mitigation undertaken.

In accordance with procedure, any high-risk data breach will be reported immediately to the Information Commissioners Office (ICO) by the Data Protection Officer, in parallel with a report to the college Principal, the Chair of the Corporation Board, and the Chair of the Audit Committee.

All breaches will be investigated formally by the Data Protection Officer and reported to the Audit Committee of the Corporation Board. Where an investigation identifies a case to be answered by one or more members of staff, this will be addressed through the Staff Disciplinary Policy (PHR20).

Where a breach involves the Data Protection Officer, the investigation will be undertaken by the Head of Governance, who will report their findings to the Audit Committee as above.

The Chair of the Audit Committee will be responsible for providing the Corporation Board with a report of any breaches or issues in relation to data protection through the minutes of the Audit Committee and their presentation at Corporation Board meetings.

Data Subject Rights - Subject Access Requests

Under data protection legislation, individuals have the right to ask the college to confirm what personal data the college holds about them, and receive a copy of the personal data held, by making a Subject Access Request. Subject Access Requests should be directed to the Compliance Management Team (dataprotection@chesterfield.ac.uk) who will ensure that the agreed procedure is followed to establish the identity of the individual, the scope of their request, and the timely provision of a response.

The college will not charge a fee for the processing of a Subject Access Request but reserves the right to pass on the cost of providing additional or repeat copies of the same information, as well as the cost of meeting any manifestly unfounded or excessive requests.

Situations may arise whereby providing the information requested would disclose information about another individual. In such cases, information will be redacted or withheld as necessary to protect the rights and privacy of the other individual(s).

Under data protection legislation, the college must respond to a Subject Access Request in full without undue delay and at the latest within one month of receipt. The Data Protection Officer can authorise an extension of up to a further two months if the request is complex or multiple requests have been received from the same individual.

Data Subject Rights - Right of Erasure (Right to be Forgotten)

There is a limited right for individuals to request the erasure of their personal data where:

- The use of the personal data is no longer necessary.
- Their consent is withdrawn and there are no other legal grounds for the processing of the personal data.
- The individual objects to the processing and there are no overriding legitimate grounds for the processing.
- The personal data has been processed unlawfully.
- The personal data must be erased to comply with a legal obligation.

Requests for the erasure of personal data should be directed to the Compliance Management Team (dataprotection@chesterfield.ac.uk). The college will respond to all requests for data erasure within 30 days and will confirm what categories of personal data, if any, have been erased, and what categories of personal data have been retained as they do not fall within the scope of this right.

In a marketing context, where personal data is collected and processed for direct marketing purposes, an individual has the right to object to processing at any time. Where an individual objects, their personal data will be erased or, if retained for another legitimate reason, clearly annotated to prevent future use for direct marketing purposes.

Data Subject Rights - Right of Data Portability

An individual has the right to request that their personal data is provided to them in a structured, commonly used, and machine-readable format. This right only extends to processing that is based on consent or a contract, and where the processing has been carried

out by automated means. This right is not the same as a Subject Access Request and is intended to give individuals a subset of their data.

Requests for portable data should be directed to the Compliance Management Team (dataprotection@chesterfield.ac.uk). The college will respond to all requests to provide portable data within 30 days, providing either a suitable dataset for transport or a detailed explanation as to why the request cannot be fulfilled.

Data Subject Rights - Right of Rectification and Restriction

Individuals have the right to request that any personal data is rectified if it is inaccurate, and to have use of their personal data restricted to a particular purpose in certain circumstances.

The college will use all personal data in accordance with the rights given to individuals under data protection legislation and will ensure that it allows individuals to exercise their rights. The Data Protection Officer will investigate any cases where an individual feels that their rights, including to the rectification of incorrect information or the restriction of use, have not been met.

Contracts and Third-Party Arrangements

If the college wishes to appoint a third-party for any function that involves the processing of personal data, the third-party can only be appointed if sufficient due diligence has taken place and an appropriate contract is in place. The contract must have a duty of confidentiality and the third-party must implement appropriate technical and organisational measures to ensure the security of data. The contract must be in writing and approval for signatory must be granted from the Senior Management Team.

A third-party is considered a Data Processor when they are engaged to perform a service and, as part of that service, they are granted access the college's personal data. The college, as the Data Controller, remains responsible for what happens to the personal data.

Data protection legislation requires that all contracts with a Data Processor contain the following obligations as a minimum:

- The Data Processor will only act on the written instructions of the Data Controller.
- The Data Processor will not export personal data without instruction from the Data Controller.
- The Data Processor will ensure that its staff are subject to confidentiality obligations.
- The Data Processor will take appropriate security measures and will only engage sub-processors with the prior consent (specific or general) of the Data Controller and under a written contract.
- The Data Processor will keep the personal data secure and will assist the Data Controller with the notification of data breaches and Data Protection Impact Assessments.
- The Data Processor will assist with Subject Access Requests and other data subject rights.
- The Data Processor will delete or return all personal data as requested at the end of the contract.

- The Data Processor will submit to audits and provide information about the processing of personal data.
- The Data Processor will tell the Data Controller if any instruction is in breach of data protection legislation.

In addition, contracts between the Chesterfield College Group and any Data Processor should set out:

- The subject matter and duration of the processing.
- The nature and purpose of the processing.
- The type of personal data and categories of individuals.
- The obligations and rights of the Data Controller.

Marketing and Consent

The college will sometimes contact individuals to promote the college or send other marketing materials. Where the college carries out any marketing, activities will be carefully planned to ensure compliance with data protection legislation and other applicable legal and regulatory frameworks.

For any advertising or marketing communications directed to individuals using their personal data, the college will operate within a framework of consent and will maintain records of this consent within its central systems for student records and customer relationship management.

For electronic marketing, the college will provide a clear and simple opt-in system for individuals, with a simple means to withdraw consent at any time.

Where information is collected face-to-face or by telephone as part of a specific marketing activity, the college will use a soft opt-in record of consent and provide the individual with an opportunity to opt-out on all occasions that the information is used.

Automated Decision Making and Profiling

The college can only carry out automated decision making or profiling once it is confident that it is complying with data protection legislation. If staff wish to carry out any automated decision making or profiling, they must inform the Data Protection Officer.

Staff must not carry out any automated decision making or profiling without the approval of the Data Protection Officer.

The college does not carry out any automated decision making or profiling in relation to its employees.

International Data Transfers

Staff must not export any personal data outside of the UK without the approval of the Data Protection Officer.

Transfers of personal data from the UK to the European Economic Area (EEA) are permitted. The UK is defined as England, Scotland, Wales, and Northern Ireland and does not include

Crown Dependencies or UK Overseas Territories. Transfers of personal data to Gibraltar are permitted.

Appropriate safeguards must be implemented to ensure data flows are mapped for any international data transfer (including cloud storage). Staff must, therefore, notify the Data Protection Officer before any agreements are considered. The Data Protection Officer is responsible for logging all activities in the Record of Processing Activities (ROPA).

Implementation

The Chesterfield College Group will ensure that:

- A member of the Senior Management Team acts as the Strategic Data Protection Lead, supported by the Data Protection Officer, who also has a direct line of reporting to the Audit Committee of the Corporation Board.
- Meetings are held which introduce and remind staff of their responsibilities under data protection legislation, including induction, departmental team meetings, and College Management Team meetings.
- All staff receive a level of training appropriate to their role with refresher training every 3 years. This will be recorded and monitored through central Workforce Development records.
- Support staff with primary responsibility for processing personal and sensitive data receive training appropriate to their day-to-day duties via their line manager and are required to maintain a level of operational understanding and awareness of the Data Protection Policy and associated operating procedures.

The Data Protection Officer will undertake the minimum prescribed tasks as follows:

- Inform and advise the Strategic Data Protection Lead about all data protection matters.
- Ensure that all staff understand their obligations to comply with data protection legislation.
- Monitor compliance with data protection legislation, including managing internal data protection activities, advising on Data Protection Impact Assessments, supporting training, and conducting internal audits.
- Be a named point of contact for the Information Commissioners Office (ICO) and for individuals whose data is processed.

Individuals with a complaint about the processing of their personal data should refer to the college's Complaints and Compliments Policy (CSE06).

Communication Flow

The policy is approved by the college's Finance and Corporate Services Committee.

The policy is available to view on the staff intranet and the college website. Details of the policy and associated operating procedures are communicated through staff induction and refresher training. Awareness and acceptance of the policy is a probationary requirement for new staff.

Users of Chesterfield College Group IT facilities and those with access to personal and sensitive data receive a level of training appropriate to their role with refresher training every 3 years. This is recorded and monitored through central Workforce Development records.

All individuals are kept informed of their rights as a data subject through clear, simple information provided at the point of data collection, and via the college website.

Monitoring

The Chesterfield College Group has appointed the Head of Compliance and Business Intelligence Systems as the designated Data Protection Officer with specific responsibilities and accountability for data protection across the College Group.

The Data Protection Officer will be supported in managing the framework for data protection by the named Data Protection Business Partners.

In discharging their duties, the Data Protection Officer will have a direct line of reporting through the Head of Governance to the Audit Committee of the Corporation Board.

The Data Protection Officer will present a data protection report at every meeting of the Audit Committee, providing a summary of all assurances and improvement actions taken in respect of data protection in the period since the last report, along with a summary of Subject Access Requests received and responded to.

The implementation of the Data Protection Policy is continuously monitored by the Data Protection Officer.

The policy is formally reviewed every 3 years or in response to significant legislative changes.

Associated Information and Guidance

Relevant legislation includes:

- Data Protection Act 2018.
- Human Rights Act 1998.
- Data Protection (Processing of Sensitive Personal Data) Order 2000.
- Regulation of Investigatory Powers Act 2000.
- Freedom of Information Act 2000.
- Freedom of Information (Scotland) Act 2002.
- Privacy and Electronic Communications Regulations 2003 (as amended).

Further guidance:

- Information Commissioners Office Guide to Data Protection.
- JISC Data Protection Guide.

Related Chesterfield College Group Policies and Documents

- Information Security Policy – INF01
- IT Acceptable Use Policy – INF02

- Freedom of Information Policy – INF05
- Data Retention Policy – INF06
- Data Classification, Handling and Disposal Policy – INF09
- Clear Desk and Clear Screen Policy – INF10
- Complaints and Compliments Policy – CSE06
- Business Continuity Plan – FIN10
- Safeguarding Policy – GOV05
- Online Safety Policy – GOV12
- Staff Induction and Probation Policy – PHR12
- Staff Code of Conduct – PHR19
- Staff Disciplinary Policy – PHR20
- Student and Apprentice Disciplinary Policy – TLA03