The Chesterfield College Group

Data Protection Policy

Family:	Information Governance
Reference Code:	INF03
Manager Responsible:	Data Protection Officer and Head of Compliance & BIS
Committee for Approval:	Finance and Corporate Services
Approval Date:	May 2022
Issue Date:	May 2022
Review Date:	May 2025

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.
Issue Number	6
Issue Date	May 2022
Review Date	May 2025
Originator	Data Protection Officer and Head of Compliance & BIS
Responsibility	Senior Management Team

Contents

Aim

The policy and associated procedures aim to ensure Chesterfield College Group explain the responsibilities of staff under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18).

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 data protection obligations. This policy sets out our commitment to data protection together with rights and obligations in relation to personal data.

Scope

This policy applies to the collection, processing, and disposal of all personal and special category data in connection with the work, studies, or other activities in association with Chesterfield College and any of its subsidiary companies. This includes data that enters the public domain through social networking sites and emails; the security of data transferred via these methods is also subject to the same data protection requirements.

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

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

Policy Statements

1. Data Protection Law

This policy is informed by and meets the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18) and all applicable laws relating to the collection and use of personal data and privacy and any applicable codes of practice issued by a regulator.

2. The Data Controller

The College as a corporate body is the data controller, and the Corporation is ultimately responsible for the implementation of all appropriate policies and procedures to meet its obligations.

Governors, staff, agency workers, contractors and consultants of the College are required to implement the policy on behalf of the College and are referred to throughout this document as ‘staff’.

3. The Data Protection Officer

The College’s Data Protection Officer is the DPO and Head of Compliance & Business Intelligence Systems. Their contact details will be published on the College website, as well as being widely available to all staff and students within the College.

4. Data Protection Business Partners

The College has Data Protection Business Partners, each of whom supports the Data Protection Officer on a particular aspect of data protection:

- Vice Principal People and Culture – data relating to staff and Health & Safety.
- Head of Information Services – data relating to students and funding agreements.
- Director of Student Experience and Wellbeing – data relating to enquiries, applications, learning support, safeguarding, and marketing activities.
- Director of Apprenticeships and Commercial Services – data relating to employers and apprentices.
- Head of ICT – information and data security.

5. Data Protection Principles

The Chesterfield College Group complies with the six data protection principles that guide data protection legislation. In summary, we require that personal data is:

1. Processed fairly, lawfully, and in a transparent manner.
2. Used only for limited, specified, stated purposes, and not used or disclosed in any way incompatible with those purposes.
3. Adequate, relevant, and limited to what is necessary.
4. Accurate and, where necessary, up to date.
5. Not kept for longer than necessary.
6. Kept safe and secure.

In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. Failure to do so can result in breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law. Our staff have access to policies, operational procedures, and guidance to give them appropriate direction on the application of data protection legislation.

6. Lawful Use of Personal Data

To collect and/or use personal data lawfully, the College must show the processing is lawful, fair, and transparent. It is not enough to show 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, the College must show that one of a number of additional conditions is met.

The College will carefully assess how it uses all personal data and document this within the Information Asset Register. If the College changes how it uses personal data, the College must update this record and may also need to notify individuals about the change. Any changes to the use of personal data must therefore be approved by the Data Protection Officer in advance and documented through an update to the Asset Register and Retention Policy, if applicable.

When collecting data the College will capture and retain consent, together with the version of the privacy information that accompanied the consent. If the legal basis for processing data is based on consent the College must respect the individual's right to withdraw consent at any time.

7. Transparent Processing – Privacy Statements

Where the College collects personal data directly from individuals, the College will inform them about how their personal data is used through the appropriate Privacy Statement published on the College website.

If the College changes how it uses personal data, the College may need to notify individuals 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 amendments to be made to the Privacy Statements and any other controls which need to apply.

8. Data Quality

Data Protection Laws require 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 a Privacy Statement and as set out in the College's Information Asset Register. The College is also required to ensure that the personal data held is accurate and kept up to date.

All staff that collect and record personal data shall ensure that the personal data is recorded accurately, is kept up to date, and shall 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 shall take reasonable steps to ensure that the personal data is recorded accurately, is 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 quality measures include:

- Correcting personal data in a timely manner that is discovered to be incorrect, inaccurate, incomplete, ambiguous, misleading, or outdated, even if the individual does not request rectifications.
- Keeping personal data only for the period necessary to satisfy the permitted uses 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 Laws.

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

10. Contracts and Third-Party Arrangements to Access the College's Personal Data

If the College appoints a third party involving the processing of the College's personal data, the College can only appoint them where sufficient due diligence has taken place and only where the College has

an appropriate contract in place. The contract must have a duty of confidentiality and 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.

The College is considered as having appointed a Data Processor when we engage someone to perform a service for us and, as part of that service, they may get access to the College's personal data. The College, as the Data Controller, remain responsible for what happens to the personal data.

Data Protection Law requires all contracts with a Data Processor to contain the following obligations as a minimum:

- To only act on the written instructions of the Data Controller.
- To not export personal data without the Controller's instruction.
- To ensure staff are subject to confidentiality obligations.
- To take appropriate security measures; to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract.
- To keep the personal data secure and assist the Controller to do so; to assist with the notification of data breaches and Data Protection Impact Assessments.
- To assist with subject access/individual rights.
- To delete/return all personal data as requested at the end of the contract; to submit to audits and provide information about the processing.
- To tell the Controller if any instruction is in breach of Data Protection Law.

In addition, contracts between Chesterfield College 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 Controller.

11. Data Protection by Design

To meet the requirements of Data Protection Law and protect the rights of data subjects, the College is responsible for implementing appropriate technical and organisational measures, such as pseudonymisation and data minimisation, in an effective way to ensure the necessary safeguards for processing before we can commence processing and at the time of the processing itself.

When designing new systems or processes, and/or reviewing or expanding existing systems or processes, each will go through an approval process before continuing. 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.

12. Data Protection Impact Assessment (DPIA)

Staff must ensure a Data Protection Impact Assessment (DPIA) is completed where a type of processing, in particular processing using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of an individual.

It is important to conduct a DPIA to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar

processing operations to ensure compliance with approved codes of conduct, special category or criminal conviction data, views of the data subject before the intended processing, and in the interests of the security of the processing operation. This process, supported by the Data Protection Team, will include 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.

13. Subject Access Requests and Administration of Individual Rights

Individuals have the right under Data Protection Law to ask the College to confirm what personal data is held about them by making a Subject Access Request. All Subject Access Requests will be directed to the Data Protection Team 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 information requested may disclose personal data about another individual. In such cases, information will be redacted or withheld as necessary to protect that person's rights.

Individuals have a number of rights which they can exercise with regards to the processing of their personal information. The College will investigate and respond without undue delay, and at least within one month of the notification, where appropriate, with supporting action taken. This is set out on the Data Protection page of the College website.

14. Right of Erasure (Right to be Forgotten)

This is a limited right for individuals to request the erasure of personal data concerning them where:

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

The College will respond to all requests for data erasure within 30 days and will confirm what categories of personal data have been erased, as well as any categories of data retained where 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, the individual has a right to object to processing at any time. Where the individual objects, the personal data will be erased or, if also retained for another legitimate reason, clearly annotated to prevent future use for marketing purposes.

15. Right of Data Portability

An individual has the right to request that data concerning them is provided to them in a structured, commonly used, and machine-readable format, where the processing is based on consent or a contract, and the processing is carried out by automated means. This right is not the same as Subject Access and is intended to give individuals a subset of their data.

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.

16. Right of Rectification and Restriction

Individuals are also given the right to request that any personal data is rectified if 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 Laws and will ensure that it allows individuals to exercise their rights in accordance. 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.

17. Marketing and Consent

The College will sometimes contact individuals to send them marketing or to promote the College. Where the College carries out any marketing, activities will be carefully planned to ensure compliance with Data Protection Law and other applicable legal and regulatory frameworks.

For any advertising or marketing communication directed to individuals using their personal information, the College will operate within a framework of consent and maintain records 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, and 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.

18. Automated Decision Making and Profiling

Any automated decision making or profiling which the College carries out can only be done once the College is confident that it is complying with Data Protection Laws. If staff wish to carry out any automated decision making or profiling, they must inform the Data Protection Officer.

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

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

19. International Data Transfers

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

The UK Government has stated that transfers of data from the UK to the European Economic Area (EEA) are permitted. The UK is England, Scotland, Wales, and Northern Ireland. It does not include Crown dependencies or UK overseas territories. The UK Government will allow transfers to Gibraltar to continue.

Appropriate safeguards must be implemented to ensure data flows are mapped for any international data transfer (including Cloud). Staff must, therefore, notify the Data Protection Team before any

agreements are considered. The Data Protection Team are responsible for logging all activities confirming the Records of Processing Activities (ROPA).

20. Records Management

The College has a legal responsibility not to keep personal data for longer than needed for the specific purposes 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 information 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 in the College Information Asset Register, which provides a central record of all information processed by the College.

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 that data.
- Whether the original purpose has been fulfilled.
- Whether the data needs to be retained to support any potential legal process.

21. Data Breach

The College takes information security very seriously. However, it is possible that a personal data breach could occur. 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 consequence and the measures for mitigation undertaken.

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

All breaches will be investigated formally by the Data Protection Team and reported to the Audit Committee. 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 occurs involving the Data Protection Officer, the investigation will be undertaken by the Clerk to the Corporation, 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.

Implementation

The Chesterfield College Group will ensure that:

1. 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.

2. Meetings are held which introduce staff to the Data Protection Policy, including Staff Induction, College Management Team, and department team meetings, to enable ongoing dialogue around protecting personal data held by the Chesterfield College Group.

3. All Chesterfield College Group staff receive a level of training appropriate to their role, with refresher training annually. This will be recorded and monitored through central Workforce Development records.

4. Support staff with the primary responsibility for processing personal and sensitive information also 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 for the implementation of this policy and associated procedures.

5. Information technologies are used to ensure that this policy is accessible to all Chesterfield College Group users.

6. The Data Protection Officer will undertake the minimum prescribed tasks as follows:
   - Inform and advise the SMT Strategic Lead about all data protection matters and ensure that all staff understand their obligations to comply with Data Protection Laws.
   - Monitor compliance with Data Protection Laws, 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 ICO and for individuals whose data is processed.

Individuals with a complaint about the processing of their personal data should comply with the Complaints and Compliments Policy (CSE06).

Communication Flow

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

The policy is communicated to all staff through Staff Induction, the College intranet, the College Virtual Learning Environment (VLE), email, mandatory training, and refresher training on a 3-year cycle.

Awareness and acceptance of the policy is a probationary requirement for new staff.

The policy is available on request to members of the public.

Users of Chesterfield College Group IT facilities and those with access to personal information 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 Group.

The Data Protection Officer will be supported in managing the framework for data protection by named Data Protection Business Partners with existing responsibility for ICT Services, Information Services, Human Resources and Business Development.

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

A Data Protection Report will be presented to 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 and managers including the Head of ICT, who has responsibility for Information Security.

The Data Protection Policy is reviewed every 3 years by the Senior Management Team and according to a documented programme of review by the Finance and Corporate Services Committee.

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 (EC Directive) Regulations 2003 (as amended)

Further guidance:

- The Information Commissioners Office Guide to Data Protection: https://ico.org.uk/for-organisations/guide-to-data-protection/
- The JISC Data Protection Guide: https://www.jisc.ac.uk/guides/data-protection

The IT Acceptable Use Policy (INF02) contains a full list of IT-related legislation.

Related Chesterfield College Group Policies and Documents

- Staff Code of Conduct (PHR19)
- Information Security Policy (INF01)
- IT Acceptable Use Policy (INF02)
- Safeguarding Policy (GOV05)

- Staff Disciplinary Policy (PHR20)
- Student/Apprentice Disciplinary Policy (TLA03)
- Complaints and Compliments Policy (CSE06)