Data Protection Policy

Written by: Data Protection Officer and Compliance Manager
CLT Sponsor: Richard Church
Consulted with: Systems Development Group
Next Review Date: April 2024
Version: April 2022

1. Purpose and Scope

1.1. Exeter College is committed to complying with the law in respect of personal data and the protection of the rights and freedoms of individuals whose information it collects and processes: learners, clients, employers, governors, employees, workers, contractors, volunteers, suppliers and others.

1.2. Maintaining the integrity and security of personal data and ensuring its effective use for the intended purposes is critical to the College's continued success. Its approach to compliance is described by this and associated policies and procedures as set out under section 5.

1.3. This policy applies to all functions which process personal data, irrespective of the data source.

1.4. All employees are required to adhere to this policy, including the senior post holders, staff, workers, volunteers, contractors and governors of Exeter College. Potential breaches of this policy will be pursued in accordance with the College's Disciplinary Policy and/or the terms of relevant contracts and other forms of agreements as appropriate.

1.5. No third party may access or receive personal data controlled by Exeter College without having entered into a data sharing agreement, a centre agreement or any other relevant agreement. Partners and third parties working with or for Exeter College and who have, or may have, access to personal data, will be expected to have read and understood this policy and to comply with it.

1.6. Where there is apparent potential for a criminal offence to have been committed, the matter will be reported to the appropriate authorities as soon as is practical.

2. Definitions

2.1. **Data Controller** – The natural or legal person, public authority or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

2.2. **Data Subject** – Any living individual who is the subject of personal data held by an organisation.

2.3. **Explicit consent** – Consent obtained from a data subject for the processing of specified personal data for a particular purpose.

2.4. **Filing System** – Any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed, on a functional or geographical basis.

2.5. **General Data Protection Regulation (UK GDPR)** – The UK GDPR is a legal framework that sets guidelines for the collection and processing of personal information from individuals. Adopted in April 2016, the Regulation came into full effect in May 2018. The UK GDPR is enshrined in UK law by the Data Protection Act 2018. As a result of Brexit and with effect from 1 January 2021, the UK stopped being part of the EU. This means that the EU GDPR ceased to protect the rights and freedoms of UK citizens regarding their personal information. The UK Government published an update to the Data Protection Act 2018 called the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. The UK government also revised the EU GDPR to remove references to the EU and Europe and to refine it to the requirements of the UK. This is now known as the UK GDPR.

2.6. **Personal Data** – Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. Identifiers are for example: name, contact details, identification number, location data, online identifier, photographs, video recordings, communications, medical data (to include occupational health), behaviour data, performance related information, financial data, genetic information, cultural and social information.

2.7. **Processing** – Any operation performed on personal data, whether, or not, by automated means, for example: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval,

consultation, use, disclose by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.8. **Special categories personal data** – Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning an individual's sex life or sexual orientation.

2.9. **Third Party** – A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor are authorised to process personal data.

2.10. **Profiling** - Any form of automated processing of personal data, automated or otherwise, intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour.

This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

2.11. **DSAR** – Data Subject Access Request

2.12. **DPIA** – Data Protection Impact Assessment

3. Policy

3.1. Data Protection Principles

All processing of personal data at Exeter College must be conducted in accordance with the six Data Protection Principles as set out in Article 5 of the General Data Protection Regulations (UK GDPR).

3.1.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subjects. **('lawfulness, fairness and transparency')**

- Exeter College will identify a lawful basis prior to commencing any processing of personal data.
- All electronic and paper-based data collection forms will include a privacy statement and/or a link to a privacy notice and be approved by the Data Protection Officer (DPO).

3.1.2 The collection of personal data must be limited to its collection only for specified, explicit and legitimate purposes. Further processing in a manner that is incompatible with those purposes is not permitted. **('purpose limitation')**

- The DPO Team will maintain an information/data asset register, recording all processes that involve processing personal data.
- The following types of processing will not be regarded as being incompatible for the purposes of this principle: archiving in the public interest, scientific or historical research purposes and statistical purposes.

3.1.3 Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. **('data minimisation')**

- Exeter College will collect and process personal data only where necessary for the operation and promotion of the College and in the best interest of the data subjects.
- The College will ensure data minimisation is effective throughout the organisation.

3.1.4 Personal data processed must be accurate and, where necessary, kept up to date. **('accuracy')**

- Staff involved in collection and processing of personal data must ensure its accuracy. Data stored must be reviewed and updated as necessary and no data should be retained unless it is reasonable to assume that it is accurate.

- Data subjects will be informed of the need to notify Exeter College of any changes involving their personal data. Data subjects, including parents, students, staff and governors carry an obligation to ensure that their data, held by the College, is accurate and up to date.
- Requests for rectification from data subjects must be actioned within one calendar month. If the College is unable to comply with the request, the DPO must respond to the individual to explain the reason and to inform them of their right to complain to the Information Commissioner.

3.1.5 Personal data must be kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which it is processed. **('storage limitation')**

- The Information Asset Owners of each dataset must review the retention status of the personal data for which they are responsible on an annual basis. Data that is no longer required in the context of the registered purpose must be securely destroyed or anonymised.
- Personal data will be retained in line with the Data Retention Schedule and destroyed or anonymised accordingly. Where personal data is retained beyond the processing date, it will be pseudomised to protect the identity of the data subjects.
- Any retention of personal data beyond the periods defined in the Data Retention Schedule must be authorised by the DPO, who will ensure that the justification is clearly identified and recorded in line with the requirements of data protection legislation.

3.1.6 Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. **('integrity and confidentiality')**

- The DPO will advise the Senior Information Risk Owner (SIRO) on matters of information risk and mitigation measures both technical and organisational. Technical security standards will be informed by the Information Security Policy and agreed by the Systems Development Group, of which the SIRO and DPO are members.
- Organisational measures will include:
  - Appropriate training for all Exeter College employees
  - Pre-employment checks
  - The inclusion of data protection in employment contracts
  - Robust disciplinary processes
  - Monitoring of Information Security Policy compliance
  - Physical access controls to electronic and paper-based records
  - The locking, when unoccupied, of any area in which personal data is present
  - Adoption of a clear desk policy
  - Protocols governing the design and inception of new processes within College business units in line with 4.1.6 of the Information Governance Policy
  - Secure storage of paper-based data protected from environmental hazard such as fire and flood
  - Restriction on the use of portable electronic devices including storage devices in line with the Information Security Policy
  - Protocols governing the control of personal data accessed remotely for the purposes of remote working e.g., from home, during visits, in transit as set out in the Information Security Policy.

3.2. Accountability

3.2.1 Exeter College will demonstrate compliance with the data protection principles by requiring adherence to policies, codes of conduct and relevant procedures.

3.2.2 The College will adopt techniques such as data protection by design and conduct Data Protection Impact Assessments (DPIAs) according to agreed protocols.

3.2.3 In the event of a data breach, the College will invoke its Data Loss Response Procedure.

3.3. Data subjects' rights

3.3.1 Exeter College will make provision for data subjects to exercise their rights according to the UK GDPR:

- Access to personal data and to information regarding processing
- Data portability
- Rectification
- Erasure ('right to be forgotten')
- Restriction
- Objection
- Prevention of automated decision-making
- Compensation
- Complaints to the Commissioner

3.3.2 Data subjects have the right to complain to Exeter College in respect of the processing of their personal data. The handling of such a request will be subject to the terms of the College's Compliments, Comments and Complaints Procedure.

3.4. Consent

3.4.1 Consent must be explicitly and freely given. It must be a specific, informed and unambiguous indication of the individual's agreement to the processing of their personal data. The data subject can withdraw their consent at any time.

3.4.2 If the data subject is not considered competent to provide informed consent, processing must be authorised by the individual's next of kin as named on the College's MIS system.

3.4.3 Consent to process personal and special category data must be obtained by using approved consent forms.

3.4.4 Where special category data is processed, explicit written consent from the data subject must be obtained, unless an alternative legal basis for processing exists.

3.4.5 Where consent is the legal basis for processing, the process must be subject to an appropriate mechanism for managing that consent.

3.4.6 The DPO and Compliance Team holds a directory of approved data collection forms where consent is the legal basis on which Exeter College processes personal data. Where updates or amendments are made it is the responsibility of the relevant Information Asset Owner to ensure that dated or amended forms are shared with the DPO and Compliance Team to ensure re-approval.

3.5. Data security

3.5.1 All employees are responsible for the security of the data to which they have access and must adhere to specific protocols which protect against the inappropriate sharing of personal data with third parties.

3.5.2 Employees must not access College information systems or records for any purpose which is not directly related to discharging their contractual duties on behalf of Exeter College.

3.5.3 Personal data is accessible only to those who have a professional requirement and access is only granted in line with authorised procedures.

3.5.4 Manual records

- must not be left unattended where they could be accessed by unauthorised personnel
- must not be removed from College premises without explicit authorisation from CLT, SIRO or DPO
- no longer required for day-to-day operation must be removed to secure archive storage
- that have reached their retention date must be disposed of as 'confidential waste'

3.5.5 Personal data may only be deleted or disposed of in line with the Data Retention Schedule.

3.5.6 Removable media carrying, or potentially carrying, personal data should be referred to the ICT Helpdesk for secure termination if the item cannot be repatriated with its owner.

3.6. Disclosure of personal data

3.6.1 Exeter College must ensure that personal data is not disclosed to third parties, including family members and public bodies, without appropriate authority. All employees must exercise caution when asked to disclose personal data to anyone other than the confirmed data subject and where appropriate refer to the Identity Verification Procedure.

3.6.2 From time to time, the College is required to share personal data with government and other agencies and, where possible, this should be made clear in the privacy statement/privacy notice displayed at the point at which personal information is collected.

3.6.3 The College will ensure that data passed to such recipients is complete, accurate and up to date. Only information to which the recipient has a statutory right or where legislation requires it or where consent has been given, will be transferred. The College will take steps to ensure the security of such data up to the point where control passes to the recipient. Thereafter, handling of the shared information by the recipient will be subject to the terms of the recipient's privacy policies.

3.7. Data Transfers

3.7.1 Exeter College will transfer personal data outside the UK if one or more of the following safeguards or exceptions exist:

- An adequacy decision
- Standard Contractual Clauses (SCCs)
- Binding corporate rules

3.7.2 In the absence of any of the above, transfer of personal data to a third country or to an international organisation shall not take place unless at least one of the following conditions exists:

- The data subject has explicitly consented to the proposed transfer, having been informed of the possible risks in the absence of appropriate safeguards
- The transfer is necessary for the performance of a contract between the data subject and the College or at the data subject's request
- The transfer is necessary for the performance of a contract between the College and another natural or legal person which is in the interest of the data subject
- The transfer is necessary for important reasons of public interest
- The transfer is necessary for the defence or exercising of legal claims by Exeter College
- The transfer is necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent.

3.8. Register of datasets and processes

3.8.1 Exeter College keeps a register of datasets and processes which defines:

- Business processes that use personal data
- Sources of personal data (type of collection method)
- Volume of data subjects affected by the process
- Classes of personal data involved
- Classes of data subjects involved
- Purpose of processing
- Recipients and protentional recipients of the personal data
- The system, repository or nature of the storage media

3.8.2 The DPO and Compliance Team maintains a description of the flow of data between processes within College functions and maintains a schedule of retention periods and disposal requirements.

3.9. Risk and impact assessments

3.9.1 Exeter College will assess the level of risk to the rights and freedoms of data subjects in accordance with section 3.14 of this policy.

3.10. External Data Processors and Cloud Computing

3.10.1 The Systems Development Group (SDG) must authorise the use of external suppliers or partners to process personal information. This applies to the use of processing services to meet specific requirements, for example using external mailing houses or bureau services.

3.10.2 Prior to any data sharing or processing taking place, a Data Sharing Agreement must be in place.

3.10.3 The performance of the data processor must be sponsored by, and subject to the oversight of, a named College manager and, from time to time, the College's internal auditors.

3.10.4 Proposals to use externally hosted (Cloud) processing and/or data storage, as part of a College business system, must be referred to the Systems Development Group so that security arrangements can be validated prior to entering any contract or the transfer of personal data.

3.11. Partnership working

3.11.1 Where the processing of personal data is carried out to support partnership activities between the College and other organisations, there must be a written data sharing agreement in place which includes a definition of the legal status of each partner in respect to data protection.

3.11.2 Parties should be designated as Data Controller, Joint Data Controller or Data Processor.

3.12. Customer Service

3.12.1 Excellent customer service is expected in all aspects of College operation. Data protection legislation should not be used as a reason to refuse to assist an enquirer or to prevent progress of legitimate business.

3.12.2 While information security is paramount, there are, in almost all circumstances, correct ways to proceed which will be both compliant and helpful to individuals and the College.

3.13. Retention

3.13.1 Exeter College will retain and dispose of personal data in line with its Retention and Disposition Policy and Data Retention Schedule.

3.13.2 Exeter College will not keep personal data in a form that permits identification of data subjects for longer than the period necessary for the purpose(s) for which the data was originally collected.

3.13.3 The retention period for each category of personal data will be set out in the Data Retention Schedule. The DPO will maintain the Data Retention Schedule on behalf of the College.

3.13.4 Exeter College may store personal data for longer periods if it is to be processed solely for statistical research and archiving purposes which are in the public interest. In such circumstances the College will implement technical and organisational measures to safeguard the rights and freedoms of data subjects.

3.14. Data Protection Impact Assessment

3.14.1 In accordance with the UK GDPR (Article 35) a DPIA assesses the risks to personal data as part of a project or business process. Exeter College works with the concept of, "Privacy by design and default" and as a result, will always comprehensively assess and address risks to the processing of personal information. Focus is put on processing activities which are "likely to result in high risk to the rights and freedoms of the data subjects" with the view to minimise these as far as is practicable.

3.14.2 The UK GDPR requires that a DPIA is completed if the project or business process plans to:

- use systematic and extensive profiling with significant effects
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale

3.14.3 The Information Commissioner's Office (ICO) requires a DPIA if the project or business process plan to:

- use innovative technologies
- use profiling or special category data to decide on access to services
- profile individuals on a large scale
- process biometric data
- process genetic data
- match data or combine datasets from diverse sources.
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')
- track individuals' location or behaviour
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach

3.14.4 Exeter College requires all projects and business processes to undergo a DPIA if one or more of the following will apply:

- using personal information for the purpose not currently used for
- sharing personal information with organisations of people who have not previously had access
- systematic and extensive profiling with significant effects
- process special category or criminal offence data on a large scale
- systematically monitor publicly accessible places on a large scale
- use innovative technologies
- use profiling or special category data to decide on access to services
- process biometric data or genetic data
- match data or combine datasets from diverse sources
- collect personal data from a source other than the individual without providing them with a privacy notice ("invisible processing")
- track individuals' location or behaviour
- profile children or target marketing or online services at them
- process data that might endanger the individual's physical health or safety in the event of a security breach
- using innovative technology that might be perceived as being privacy intrusive
- may result in Exeter College making decisions, or acting against individuals in ways that can have a significant impact on them
- involves information about individuals that could be considered particularly private
- requiring Exeter College staff to contact individuals in ways that they may find intrusive (e.g. unexpected telephone calls
- sharing personal information from live or operational systems for access or transfer outside the UK (e.g., Cloud, Hybrid, offshore support services)
- using personal information that might raise privacy concerns or expectations (e.g., health records)

3.14.5 If there is uncertainty regarding whether a DPIA should be carried out, the expectation is that a DPIA will be completed as it is a useful tool that will help the College to comply with data protection law. In very exceptional circumstances it may be necessary for the Data Protection Officer to seek the guidance of the ICO. The ICO will not be consulted unless approval has been given, in writing, by the Data Protection Officer.

3.14.6 Changes to the way personal data is processed will require a DPIA.

In the event of a security breach a DPIA may be required to ensure that all identified risks are being appropriately managed.

3.14.7 Following approval of the DPIA and when processing activities have started, the DPIA will be kept under regular review considering any changes to the processing activities or broadening of the scope of the original initiative.

3.15. Data Subject Access Requests

3.15.1 The UK GDPR sets out in Article 15 that a data subject should have the right to access their personal data which have been collected concerning them and to exercise that right easily to be aware of, and verify, the lawfulness of the processing. Individuals have the right to obtain a copy of their personal data, as well as other supplementary information held about them.

3.15.2 That right should not adversely affect the rights or freedoms of others.

3.15.3 A Data Subject Access Request can be a verbal or written request made by a data subject to access their data, in a portable format if requested.

3.15.4 Where Exeter College processes a large quantity of information concerning the data subject, the College should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

3.15.5 Exeter College (the data controller) will use all reasonable measures to verify the identity of the data subject who requests access.

3.15.6 Exeter College will retain personal data in accordance with its Retention and Disposition Policy and its Data Retention Schedule. In accordance with the UK GDPR the College will not retain personal data for the sole purpose of being able to react to potential DSAR requests.

3.15.6 Exeter College implements Article 15 of the UK GDPR in line with this policy and the Data Subject Access Procedure.

4. Implementation

4.1. Roles and responsibilities of the Board of the Corporation, the Senior Leadership Team, the Senior Information Risk Owner, the Data Protection Officer, the ICT Manager, The Information Asset Owners, the Senior Resources Systems Development Group, the Director of Finance, Funding and MIS, the Director of Estates and Information Technology, the Heads of Department and Faculty, line managers and all employees are set out in detail under 4.1 of the Information Governance Policy.

4.2. All employees and others having access to data on behalf of the college, are required to comply with the Data Protection Policy and associated documents. Training and further support is available from The DPO Team.

4.3. Exeter College will appoint a named individual with specific responsibility for data protection in the organisation (the Data Protection Officer).

4.4. Exeter College will ensure that the Senior Resources Systems Development Group receives reports on Data Protection matters at its regular meetings.

4.5. Appropriate guidance materials and training will be provided for employees according to their role in handing personal information.

4.6. Exeter College will ensure that employees understand that they have a contractual obligation to manage the personal data in their care appropriately.

4.7. It will be expected that any third-party organisation that processes data on the College's behalf has adequate control measures in place and is subject to an appropriate contractual agreement.

4.8. Appropriate systems will be put in place to collect, store, manage, process and dispose of data and explain to employees that the use of alternative mechanism is contrary to college policy.

4.9. Exeter College will fully document systems, processes and data flows.

4.10. It will be ensured that security is a priority objective in the design of new systems and processes.

4.11. Data Privacy Impact Assessments (DPIAs) will be carried out prior to introducing new processes which are assessed as high-risk.

4.12. Exeter College will ensure the robustness and security of physical electronic systems for processing data and that regular third-party reviews take place.

4.13. Detailed privacy statements/notices, written in accessible language, will be available to individuals at the point of data collection and these will be reviewed regularly.

4.14. Exeter College will use its DSAR Procedure to manage formal requests for access to personal data from data subjects and third parties.

4.15. A policy and procedure are in place to manage actual and potential data breaches and data-loss incidents.

5. Associated Documentation

5.1. This policy should be used in conjunction with the following policies:

5.1.1 Information Governance Policy
5.1.2 Information Security Policy
5.1.3 Retention and Disposition Policy

5.2. This policy should be used in conjunction with the following procedures and other documentation:

5.2.1 Privacy Notices
5.2.2 Staff Code of Conduct
5.2.3 s29 Protocol for disclosure of information to the Police and other law enforcing agencies
5.2.5 Data Sharing Agreements and Standard Contractual Clauses
5.2.5 Data Loss Response Procedure
5.2.6 The Data Subject Access Request Procedure
5.2.7 The Data Retention Schedule
5.2.8 Compliments, Comments and Complaints Procedure
5.2.9 DPIA Request (MS Form)
5.2.10 DPIA Screening Questions (MS Form)
5.2.11 DPIA Screening Questions for third party software (MS Forms)
5.2.12 DPIA Report
5.2.13 Risk Matrix
5.2.14 Risk Register
5.2.15 Identity Verification Procedure

5.3. Associated Legislation

5.2.1 Data Protection Act 2018
5.2.2 Freedom of Information Act 2000
5.2.3 Computer Misuse Act 1990
5.2.4 Regulation of Investigatory Powers Act 2000
5.2.5 Privacy of Electronic Communications Regulations 2003
5.2.5 UK General Data Protection Regulation (UK GDPR)
5.2.6 The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019

6. Monitoring, Reviews and Evaluation

6.1. The Senior Leadership team is responsible for the approving of the Data Protection Policy.

6.2. The Board (Audit and Risk Committee) is responsible for adopting the Data Protection Policy.

6.3. Exeter College is committed to complying with the law in respect of personal data and the protection of the rights and freedoms of individuals whose information it collects and processes.

6.4. The Data Protection Officer and Compliance Manager is responsible for the maintenance, review and monitoring of the Data Protection Policy and will conduct a bi-annual review.

6.5. The definitive version of the policy is stored in the College Leadership SharePoint Site