Data Protection Policy

Written by: Data Protection Officer and GDPR working group
CLT Sponsor: Richard Brine
Consulted with: Systems Development Group
Next Review Date: May 2020
Version: April 2018

1. Purpose

1.1. Exeter College collects and processes personal information belonging to applicants, students, employees, governors, contractors and others.

1.2. Maintaining the integrity and security of personal information, and ensuring its effective use for the intended purposes, is critical to the college's continued success.

1.3. This policy sets out to protect the 'rights and freedoms' of data subjects and to ensure that personal data is not processed without legal basis and, wherever possible, processed only with their knowledge. It sets the standards by which personal information is managed by the college in order to ensure effective operation and compliance with relevant legislation in the best interests of data subjects.

2. Definitions

2.1. Child

2.1.1. A natural person under the age of 13 years. Where no other legal basis applies, the processing of personal data of a child is lawful only with the consent of a person with parental responsibility.

2.2. Data controller

2.2.1. The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

2.3. Data

2.3.1. Any information relating to an identifiable natural person.

2.4. Data Subject

2.4.1. Any living individual who is the subject of personal data held by an organisation.

2.5. Explicit consent

2.5.1. Consent obtained for the processing of specified personal data for a particular purpose.

2.6. Filing system

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

2.7. General Data Protection Regulation (GDPR)

2.7.1. EU regulation enacted in UK law as the Data Protection Act 2018

2.8. Personal data

2.8.1. Any information relating to an identified or identifiable natural person ('data subject').

2.8.2. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.9. Personal data breach

2.9.1. A breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2.10. Processing

2.10.1. Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.11. Profiling

2.11.1. Any form of automated processing of personal data 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.

2.11.2. 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.

2.12. Special categories of personal data Personal data consisting of information as to

2.12.1. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

2.13. Third party

2.13.1. 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.

3. Policy

3.1. Overview

3.1.1. 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. Its approach to compliance is described by this and associated policies, including the Information Security Policy, along with related procedures.

3.1.2. This policy applies to all functions which process personal data, irrespective of the data source. Data subjects include but are not limited to: learners, clients, employers, governors, employees, workers, contractors, volunteers, suppliers and other partners.

3.1.3. The Data Protection Officer (DPO) will conduct an annual review of the register of processing and datasets. Such reviews will take account of changes to the college's business operations and any additional requirements identified by means of Data Protection Impact Assessments (DPIAs). This register will be available to the Information Commissioner on request.

3.1.4. Adherence to this policy is required of all employees including senior post holders, staff, workers, volunteers, contractors and governors of Exeter College. Potential breaches of this policy will be pursued in accordance with the Exeter College disciplinary policy and/or the terms of relevant contracts and other forms of agreement as appropriate.

3.1.5. Partners and any third parties working with or for Exeter College, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access or receive personal data controlled by Exeter College without having first entered into a data sharing agreement. Such an agreement must impose obligations on recipients which are no less onerous than those to which Exeter College is committed and must grant Exeter College the right to audit compliance with that agreement.

3.1.6. 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 practical.

3.2. Data protection principles

3.2.1. All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR and the Data Protection Act 2018. Exeter College's policies and procedures are designed to ensure compliance with the principles.

3.2.2. **Personal data must be processed lawfully, fairly and transparently**

3.2.2.1. Exeter College will identify an applicable lawful basis prior to commencing any processing of personal data. It will ensure that it provides privacy notices written in accessible, plain language and which make available to data subjects the information to which they are entitled. This applies whether the personal data is to be obtained directly from the data subjects or from other sources.

3.2.2.2. As a minimum, privacy notices will include:

1. the identity (if not implied by context) and the contact details of the college
2. the contact details of the Data Protection Officer
3. the purposes of the processing for which the personal data is intended
4. the legal basis for the processing
5. the period for which the personal data will be retained

6. the existence of the rights of access, rectification, erasure and to object to processing
7. the conditions relating to exercising these rights
8. the categories of personal data concerned
9. where applicable, the recipients or categories of recipients of the personal data
10. where applicable, that the college intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data
11. any further information necessary to guarantee fair processing

3.2.3. **Personal data must be collected for specific, explicit and legitimate purposes and not further processed**

3.2.3.1. All datasets and processes will be recorded on the register maintained by the DPO.

3.2.3.2. Data obtained for specified purposes must be used only for the purposes stated at the time of collection unless a further legal basis exists and is documented.

3.2.4. **Personal data must be adequate, relevant and limited to what is necessary for processing**

3.2.4.1. Collect and process personal data only to the extent that it is necessary for the operation and promotion of the college and in the best interests of the data subjects.

3.2.4.2. All data collection forms (electronic or paper-based) must include a privacy notice or link to a privacy statement and be approved by the Data Protection Officer.

3.2.4.3. The college will ensure that the effectiveness of its data protection and information security controls is subject to regular review within the internal audit programme.

3.2.5. **Personal data must be accurate and kept up to date with every effort to erase or rectify without delay**

3.2.5.1. Data stored by Exeter College must be reviewed and updated as necessary. No data should be retained unless it is reasonable to assume that it is accurate.

3.2.5.2. Staff involved in the collection and processing of data must do so with due regard for accuracy.

3.2.5.3. Data subjects, including parents, students, staff and governors, carry an obligation to ensure that their data, held by Exeter College, is accurate and up to date. Application, enrolment and other collection forms must include a declaration by the subject that the data contained therein is accurate at the date of submission.

3.2.5.4. Data subjects must be informed of the need to notify Exeter College of any changes in circumstance in order that personal records can be updated accordingly. It is the responsibility of Exeter College to ensure that any notification regarding change of circumstances is recorded and acted upon in a timely manner.

3.2.5.5. The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the frequency with which it might change and any other relevant factors.

3.2.5.6. On at least an annual basis, the administrators of each dataset must review the retention status of the personal data for which they are responsible. Data that is no longer required in the context of the registered purpose must be securely terminated or anonymised.

3.2.5.7. The Data Protection Officer is responsible for managing requests for rectification from data subjects within one month. If the college is unable to comply with the request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the Information Commissioner and seek judicial remedy.

3.2.5.8. Where third-party organisations may have been passed inaccurate or out-of-date personal data, the Data Protection Officer will make appropriate arrangements to inform the recipients that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned. Errors should be corrected where appropriate.

3.2.5.9. Personal data will be retained in line with the Data Retention Schedule and, once its retention period is achieved, it must be securely destroyed or anonymised.

3.2.5.10. Where personal data is retained beyond the processing date, it will be pseudonymised in order to protect the identity of the data subjects.

3.2.5.11. Any retention of data beyond the periods defined in the Data Retention Schedule must be authorised by the Data Protection Officer who will ensure that the justification is clearly identified and recorded in line with the requirements of data protection legislation.

3.2.6. **Personal data must be processed in a manner that ensures appropriate security**

3.2.6.1. The Data Protection Officer will advise the Senior Information Risk Owner (Vice Principal) on matters of information risk and mitigation measures both technical and organisational.

3.2.6.2. 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 each members.

3.2.6.3. Organisational measure will include:

1. Appropriate training for all Exeter College employees
2. Pre-employment checks
3. The inclusion of data protection in employment contracts
4. Inclusion of data protection obligations in the staff code of conduct
5. Robust disciplinary processes
6. Monitoring of security policy compliance
7. Physical access controls to electronic and paper based records
8. The locking, when unoccupied, of any area in which personal data is present
9. Adoption of a clear desk policy
10. Protocols governing the design and inception of new processes within college business units
11. Secure storage of paper-based data protected from environmental hazard such as fire and flood
12. Restriction on the use of portable electronic devices including storage devices
13. Restrictions on the use of employee-owned personal devices to access college data
14. Protocols governing the control of personal data accessed remotely for the purposes of home working, visits etc.

3.2.7. **Exeter College must be able to demonstrate accountability**

3.2.7.1. Exeter College will demonstrate compliance with the data protection principles by requiring adherence to policies, codes of conduct and stated procedure. It will adopt techniques such as data protection by design and conduct Data Protection Impact Assessments according to agreed protocols.

3.2.7.2. In the event of a data breach, the college will invoke its incident response plan and associated notification procedures where appropriate to do so.

3.3. Data subjects' rights

3.3.1. Exeter College will make provision such that data subjects can exercise:

1. Their right to be informed
2. Their right of access
3. Their right to rectification
4. Their right to erase
5. Their right to restrict processing
6. Their right to data portability
7. Their right to object
8. Their rights in relation to automated decision making and profiling

3.3.2. The Subject Access Request Procedure sets down the means by which such requests will be discharged in compliance with the legislation.

3.3.3. Data subjects have the right to complain to Exeter College in respect of the processing of their personal data. In such circumstances the handling of a request from a data subject will be subject to the terms of the college's Complaints Procedure.

3.4. Consent

3.4.1. Consent' must be explicitly and freely given. It must be a specific, an informed and unambiguous indication of the data subject's agreement to the processing of their personal data. Consent must be signified by a statement or by a clear affirmative action. The data subject can withdraw their consent at any time.

3.4.2. Where the data subject is not considered competent to provide informed consent, processing must be authorised by the subject's next of kin as named on college systems.

3.4.3. Where special categories of data are to be processed, explicit written consent from the data subject must be obtained unless an alternative legal basis for processing exists.

3.4.4. Consent to process personal and sensitive data must be obtained by using approved consent documents.

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. Where Exeter College provides online services to a child under 13 years of age, prior authorisation must be obtained from a person with parental responsibility.

3.5. Security of data

3.5.1. All employees are responsible for the security of the data to which they have access. Policies, procedures and codes of practice determine the means by which information is secured.

3.5.2. Employees must adhere to specific protocols which protect against the inappropriate sharing of personal data with third parties.

3.5.3. Employees must not access college information systems or records for any purpose which is not directly required for the discharge of their contracted duties on behalf of the college.

3.5.4. Systems will be designed such that personal data is accessible only to those who have professional need of it and access must only be granted in line with authorised procedures.

3.5.5. Detailed explanation of security measures can be found in the associated Information Security Policy.

3.5.6. Manual records must not be left unattended where they could be accessed by unauthorised personnel. Manual records must not be removed from college premises without explicit authorisation. Manual records no longer required for day-to-day operation must be removed to secure archive storage.

3.5.7. Personal data may only be deleted or disposed of in line with the Schedule of Retention Periods. Manual records that have reached their retention date must be disposed of as 'confidential waste'. Removable media carrying or potentially carrying personal data should be referred to the ICT Helpdesk for secure termination.

3.6. Disclosure of 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 should exercise caution when asked to disclose personal data to anyone other than the confirmed data subject. Employees will receive scenario-based training to support their handling of such requests.

3.6.2. From time to time the college is required to share personal information with government and other agencies. Wherever possible, the college will make this clear in the Privacy Notices displayed at the point of collection.

3.6.3. The college will ensure that data passed to such recipients is complete, accurate and up to date. It will transfer only information to which the recipient has a statutory right, where legislation requires it or the subject has consented to the transfer. 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 notices.

3.6.4. In most cases, data sharing with third parties will be handled by trained employees in a small number of roles. All requests to provide data to third parties must be documented and authorised by the Data Protection Officer.

3.7. Retention and disposal of data

3.7.1. 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.

3.7.2. The retention period for each category of personal data will be set out in the Schedule of Data Retention Periods. The Schedule will include the criteria used to determine such periods and state any statutory obligations to retain or erase data.

3.7.3. The Data Protection Officer will maintain the Schedule of Data Retention Periods on behalf of the college.

3.7.4. 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.

3.7.5. Personal data, in all formats, must be disposed of in accordance with the secure disposal procedure.

3.8. Data transfers

3.8.1. Exeter College will transfer personal data outside the EEA if one or more of the following safeguards, or exceptions, exist:

1. An adequacy decision
2. Privacy Shield assurance
3. Binding corporate rules
4. Model contract clauses

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

3.8.2.1. the data subject has explicitly consented to the proposed transfer having been informed of the possible risks of such transfers in the absence of appropriate safeguards.

3.8.2.2. the transfer is necessary for the performance of a contract between the data subject and the college or the implementation of pre-contractual measures taken at the data subject's request.

3.8.2.3. the transfer is necessary for the conclusion or performance of a contract between the college and another natural or legal person which is in the interest of the data subject.

3.8.2.4. the transfer is necessary for important reasons of public interest.

3.8.2.5. the transfer is necessary for the defence or exercising of legal claims by the college.

3.8.2.6. the transfer is necessary in order to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent.

3.9. Register of datasets and processes

3.9.1. Exeter College has established a register of datasets and processes which defines:

1. business processes that use personal data

2. sources of personal data
3. volume of data subjects
4. classes of personal data involved
5. classes of data subject involved
6. purpose of the processing
7. recipients, and potential recipients, of the personal data
8. the system, repository or nature of the storage media

3.9.2. The Data Protection Officer maintains a description of the flow of data between processes within college functions.

3.9.3. The Data Protection Officer maintains a Schedule of Retention Periods and disposal requirements.

3.10. Risk and impact assessments

3.10.1. Prior to processing personal data, Exeter College will assess the level of risk to the rights and freedoms of data subjects. It will implement mitigation measures proportionate to the identified risk.

3.10.2. Where a process is likely to result in a high risk, through the introduction of new technologies or due to its nature, scope or purpose, Exeter College shall, prior to the processing, carry out a Data Protection Impact Assessment (DPIA).

3.10.3. When required, DPIAs will be carried out in relation to the processing of personal data by Exeter College and processing undertaken by other organisations on its behalf.

3.10.4. Where a DPIA indicates that a planned process could cause damage and/or distress to the data subjects, the decision as to whether or not to proceed must be escalated for review to the Senior Information Risk Owner via the DPO.

3.10.5. In the event that significant concerns exist regarding the potential for damage or distress, or in respect of the volume of data concerned, the DPO will advise the SIRO on the need to escalate the matter to the Information Commissioner.

3.10.6. In all cases, proportionate controls must be applied such that processing meets the requirements of the current legislation within the limits of risk exposure acceptable to the college.

3.11. External Data Processors and Cloud Computing

3.11.1. Authority to use external suppliers or partners to process personal information must be obtained from the Systems Development Group. This applies to the use of processing services to meet specific requirements; for example using external mailing houses or bureau services.

3.11.2. Prior to any data sharing or processing taking place, a Data Processor Agreement must be in force. The terms of such agreements must be proportionate to the potential for impact on the rights and freedoms of the data subjects.

3.11.3. 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.

3.11.4. 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 in order for security arrangements to be validated prior to entering any contract or the transfer of personal data.

3.11.5. The Systems Development Group may, from time to time, delegate authorisation to the DPO or the SIRO.

3.12. Partnership working

3.12.1. 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 which includes a definition of the legal status of each partner in respect of Data Protection.

3.12.2. Parties should be designated as Data Controller, Data Controllers in Common, Joint Data Controllers or Data Processors. Advice should be sought from the Data Protection Officer in determining these arrangements for particular initiatives.

3.13. Customer Service

3.13.1. 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 the progress of legitimate business.

3.13.2. 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.

3.13.3. Wherever possible (MIS student information screens for example) the college will provide contextual advice on how to respond to particular circumstances. However, if faced with a new or unexpected data protection question or situation, college members should contact the Data Protection Officer or one of the designated managers listed on the college portal.

4. Implementation

4.1. The College, including its subsidiary businesses, aims to use personal data in the best interests of data subjects.

4.2. All employees, and others having access to data on behalf of the college, are required to use the policy mechanisms set out above and in associated documents to ensure legal compliance and the protection of personal information. Training and further support is available from the DPO and other managers listed on the Data Protection portal pages.

4.3. In order to support the implementation of the above policy, the college will:

4.3.1. Appoint a named individual with specific responsibility for data protection in the organisation (the Data Protection Officer).

4.3.2. Ensure that the Systems Development Group receives reports on Data Protection matters at its regular meetings.

4.3.3. Provide appropriate guidance materials and audited training for employees according to their role in handling personal information.

4.3.4. Ensure that employees understand that they have a contractual obligation to manage the personal data in their care appropriately.

4.3.5. Ensure 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.

4.3.6. Put in place appropriate systems to collect, store, manage, process and dispose of data and explain to employees that the use of alternative mechanisms is contrary to college policy.

4.3.7. Fully document systems, processes and data flows.

4.3.8. Ensure that security is a priority objective in the design of new systems and processes.

4.3.9. Conduct Data Privacy Impact Assessments prior to introducing new processes which are assessed as high-risk.

4.3.10. Ensure the robustness and security of physical and electronic systems for processing data and subject them to regular third-party review.

4.3.11. Ensure that detailed Privacy Notices, written in accessible language, are available to data subjects at the point of data collection and that these are regularly reviewed.

4.3.12. Ensure that data is not processed for purposes other than those stated unless some other over-riding lawful basis applies.

4.3.13. Establish internal mechanisms to manage formal requests for access to personal data from data subjects and third parties.

4.3.14. Establish internal mechanisms to manage potential, suspected and actual data-loss incidents.

4.3.15. Establish quality assurance mechanisms to ensure the integrity of data particularly in respect of high volume processes.

5. Associated Documentation

5.1. The policy should be used in conjunction with the Information Governance Framework and, in particular, the following associated documents:

- Fair Processing Notices
- Code of Practice for users of students' personal information
- Code of Practice for Systems Administrators
- Information Security Policy
- Schedule of Data Retention Periods
- Accessing learners' personal information – guide for parents and guardians
- Data sharing protocols
- s29 Protocol (disclosure of information to the Police and other law enforcement agencies)
- Subject access request protocol
- Standard Data Processor Agreement

5.2 Associated Legislation:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Privacy of Electronic Communications Regulations 2003

6. Monitoring, Review and Evaluation

6.1. The Data Protection Officer is responsible for the maintenance, review and monitoring of the Data Protection Policy.

6.2. The policy, and any subsequent versions of it, will be formally adopted on behalf of the college, subject to the recommendation of the Systems Development Group and the Senior Leadership Team, by the Board to the Corporation.

6.3. Copies of this policy and associated documents are available from the college website and portal.

7. Equality Analysis

Please use the 'equality analysis procedure' to guide you to complete the text boxes below, expanding them as you wish. If this is a review - please add date and make any amendments if required.

April 2018

7.1. Is your policy equality- relevant? If yes, please list which groups of people will be affected by this policy. If no people are affected by this policy it has no equality relevance and you should write no and you need not answer any more questions. **The policy affects all individuals equally**

7.2. How have you involved people from minority groups who may be affected by this policy? Describe any activities such as conversations, interviews, feedback. **The policy applies equally to all individuals. No groups have been selected for consultation.**

7.3. What evidence have you considered? List any sources of data and research you have used. This can include college or national monitoring data, surveys, reports, consultations, focus groups, pilots, evaluations. **Best practice drawn from the Information Commissioner's website.**

7.4. How will your policy fulfil the public sector duty by helping fight discrimination, advance equality of opportunity and foster good relations?

Characteristic	How does your policy help fulfil the public sector duty?
Age	**This policy implements UK data protection legislation which is age neutral for data subjects over the age of 13.**
Disability	**Consent to processing is subject to the individual being competent to give consent. If this is not the case, consent will be sought on the individual's behalf from a named next of kin. See paragraph 3.4.2.**
Gender	**Data protection legislation is gender neutral.**
Pregnancy & maternity	**Sensitive personal data will be processed according to the requirements of the legislation.**
Race	**Sensitive personal data will be processed according to the requirements of the legislation.**
Religion and belief	**Sensitive personal data will be processed according to the requirements of the legislation.**
Sexual orientation	**Sensitive personal data will be processed according to the requirements of the legislation.**
Transgender	**Sensitive personal data will be processed according to the requirements of the legislation.**

7. 5. Describe any potential adverse impacts that may arise as a result of the policy. If any are identified, you should also state what actions will be taken to mitigate that negative impact. If yes, do you need an action plan to carry this out? **None**