Reference Number: *P27*

# DATA PROTECTION POLICY

| Policy Review | | | | | |
|---|---|---|---|---|---|
| **Author/Owner** | **Position** | **Approved by: Signature:** | **Approval Date** | **Review Cycle Review Date** | **Published on Website Y/N** |
| Emma Cox | VP Finance & Resources |  | SMT: 22/8/23<br>Corp: 24/8/23 | Annually<br>May | Y |

**Document Control – Revision History (Policies only)**

| Author/Owner | Summary of Changes | Date | Date last reviewed by SED | Version | Recommend to SED Y/N |
|---|---|---|---|---|---|
| Emma Cox | Re-written to reflect GDPR requirements | 27.04.18 | 11.11.15 | | Yes |
| Emma Cox | Amendments made to include CCTV protocol | 04.07.19 | 11.11.15 | | No |
| Craig Cullen | Additional information to include Body Cams | 9/6/22 | | v1 | No |
| Emma Cox | Annual update. Changes in line with Open University recommendations following the introduction of the UK GDPR and establishment of best practise shared by the Information Commissioner's Office. | 15/8/23 | | v2 | NO |

**Initial Equality Impact Screening**

**Has anyone else been consulted on this policy and/or procedure?** Yes, Karen Foster.

**What evidence has been used for this impact screening (e.g. related policies, publications)?**

**Declaration (please tick one statement and indicate any negative impacts)**

[X] I am satisfied that an initial screening has been carried out on this Policy and/or Procedure and a full Equality Impact Assessment is not required. There are no specific negative impacts on any of the Protected Characteristics groups.

[ ] I recommend that an Equality Impact Assessment is required by the Equality and Diversity group, as possible negative impacts have been identified for one or more of the Protected Characteristics groups as follows:

- ☐ Age
- ☐ Disability
- ☐ Gender Reassignment
- ☐ Race
- ☐ Religion or belief
- ☐ Sex
- ☐ Sexual orientation
- ☐ Marriage & civil partnership
- ☐ Pregnancy & maternity

| **Completed by:** | Emma Cox | **Position:** | VP F&R | **Date:** | 14/8/23 |
|---|---|---|---|---|---|

Reviewed by Equality & Diversity Group: YES If Yes: Date: 09.05.18

I confirm that any recommended amendments have been made

**Summary of Comments including Recommendations from Equality & Diversity Group Review:**

| **Amended by Author:** | Emma Cox | **Position:** | VP F&R | **Date:** | 14/8/23 |
|---|---|---|---|---|---|

Contents

## 1. PURPOSE OF THE POLICY

1.1 This Policy sets out the obligations of Yeovil College (the "College") regarding data protection and the rights of customers, suppliers and/or both old and new and members of staff including employees, temporary and agency workers, contractors, interns, volunteers and apprentices, whether existing or not ("Data Subjects") in respect of their Personal Data under the Data Protection Act 2018 (DPA) and UK General Data Protection Regulation (the "Regulation").

1.2 The Regulation defines "Personal Data" as any information relating to an identified or identifiable living person (a "Data Subject"); an identifiable living 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 living person. Data Subjects may be nationals or residents of any country.

1.3 This Policy sets out the procedures that are to be followed when dealing with Personal Data. The procedures and principles set out herein must be followed at all times by the College, its employees, agents, contractors, or other parties working on behalf of the College. Any breach of this Policy may result in disciplinary action. This Policy does not form part of an employee's contract of employment and may be amended at any time.

1.4 The College is committed not only to legal compliance, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all Personal Data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

## 2. RESPONSIBILITY & AUTHORITY

2.1 Overview

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which anyone handling Personal Data must comply. All Personal Data must be:

2.1.1 processed lawfully, fairly, and in a transparent manner in relation to the Data Subject;

2.1.2 collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes will not be considered to be incompatible with the initial purposes;

2.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

2.1.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

2.1.5 kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the Data Subject;

2.1.6 processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

2.1.7 not transferred to another country without appropriate safeguards being in place in accordance with clause 8; and

2.1.8 made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

2.2 Lawful, Fair and Transparent Data Processing

The Regulation seeks to ensure that Personal Data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the Data Subject. The Regulation states that processing of Personal Data will be lawful if at least one of the following applies:

2.2.1 the Data Subject has given consent to the processing of his or her Personal Data for one or more specific purposes;

2.2.2 processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;

2.2.3 processing is necessary for compliance with a legal obligation to which the College is subject;

2.2.4 processing is necessary to protect the vital interests of the Data Subject or of another natural person;

2.2.5 processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the College;

2.2.6 processing is necessary for the purposes of the legitimate interests pursued by the College or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

2.3 Processed for Specified, Explicit and Legitimate Purposes

2.3.1 The College collects and processes the Personal Data set out in clause 4 of this Policy. This may include Personal Data received directly from Data Subjects (for example, contact details used when a Data Subject communicates with us) and data received from third parties (for example, School Partnerships, Safeguarding History, CVs from recruitment agencies and references).

2.3.2 The College only processes Personal Data for the specific purposes set out in clause 4 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process Personal Data will be communicated to Data Subjects at the time that their Personal Data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

2.4 Adequate, Relevant and Limited Data Processing

The College will only collect and process Personal Data for and to the extent necessary for the specific purpose(s) communicated to Data Subjects in accordance with clause 1.2.

2.5 Accuracy of Data and Keeping Data Up To Date

The College will ensure that all Personal Data collected and processed is kept accurate and up-to-date. The accuracy of Personal Data will be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date Personal Data is found, all reasonable steps will be taken without delay to amend or erase that Personal Data, as appropriate.

2.6 Timely Processing

The College will not keep Personal Data for any longer than is necessary in light of the purposes for which that Personal Data was originally collected and processed. When the Personal Data is no longer required, all reasonable steps will be taken to erase it without delay.

2.7 Secure Processing

The College will ensure that all Personal Data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which will be taken are provided in clauses 5 and 6 of this Policy.

## 3. ACCOUNTABILITY

3.1 The College's Data Protection Officer is the Vice Principal Finance & Resources who can be contacted on DataProtection@yeovil.ac.uk

3.2 The College will keep written internal records on a Data Register of all Personal Data collection, holding, and processing, which will incorporate the following information:

3.2.1 the name and details of the College, its Data Protection Officer, and any applicable third party data controllers;

3.2.2 the purposes for which the College processes Personal Data;

3.2.3 details of the categories of Personal Data collected, held, and processed by the College; and the categories of Data Subject to which that Personal Data relates;

3.2.4 details (and categories) of any third parties that will receive Personal Data from the College and on what basis. A copy of any agreement purporting to transfer Personal Data must be kept and reviewed prior to signing to ensure processing provisions are compliant with the Regulation. Please contact the Data Protection Officer before entering into any contract;

3.2.5 details of any transfers of Personal Data to non-UK countries including all mechanisms and security safeguards;

3.2.6 details of how long Personal Data will be retained by the College; and

3.2.7 detailed descriptions of all technical and organisational measures taken by the College to ensure the security of Personal Data.

3.3 Data Protection Impact Assessments

The College will carry out Data Protection Impact Assessments (DPIA)for all new processes where data is collected, or where there is a change in process for data collection. The DPIA will be reviewed by the GDPR panel each term as required by the Regulation.

3.3.1 In line with UK GDPR, the college will always complete a DPIA in the following circumstances:

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

3.3.2 In line with ICO requirements, where the processing is likely to result in high risk, the college will carry out a DPIA in the following circumstances:

- use innovative technology (in combination with any of the criteria from the European guidelines);
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;

- process biometric data (in combination with any of the criteria from the European guidelines);
- process genetic data (in combination with any of the criteria from the European guidelines);
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
- track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
- profile children or target marketing or online services at them; o
- process data that might endanger the individual's physical health or safety in the event of a security breach.

3.3.3 Additional High-risk processing. Outside the mandatory list of DPIAs, a DPIA will be required where the proposed project/ initiative involves data processing which is likely to result in high risk.

3.3.4 Data Protection Impact Assessments (DPIA) will be overseen by the Data Protection Officer and will address the following areas:

- Identifying the need for a DPIA
- Describing the nature, scope and context of the processing;
- Consideration for how to consult with relevant stakeholders;
- Describing the compliance and proportionality measures, including lawful basis for the processing;
- an assessment of the risks posed to individual Data Subjects; and
- details of the measures in place to reduce or eliminate risks

Please refer to the Data Protection Officer for details about how to complete a Data Protection Impact Assessment. DataProtection@yeovil.ac.uk

## 4. DATA SUBJECT RIGHTS

4.1 Data Subject Rights

4.1.1 Data protection law gives individuals greater control over their personal data through several rights which the College strives to facilitate effectively.

4.1.2 Requests can be made verbally or in writing to DataProtection@yeovil.ac.uk As a member of College staff, if you receive a data subject rights request you should forward it to the DPO immediately and no later than within 24 hours of receipt. If the request is made verbally, please obtain as much information as possible, including contact details for the data subject, and pass them immediately to the DPO.

4.1.3 The College must respond to data subject requests within one calendar month. It is possible to extend the time to respond by a further two months if the request is complex or if we have received a number of requests from the individual. The College will let the individual know that the time limit needs to be extended within one month of receiving the request and will explain the reasons for the extension.

4.1.4 Generally, there is no fee for making a data subject rights request, however the College may charge a reasonable fee for the administrative costs of complying with a request if it is manifestly unfounded or excessive. Where the College charges a fee, we will contact the individual promptly to inform them. Please note that the College does not have to comply with the request until we have received the fee.

4.1.5 Some rights only apply in certain circumstances, depending on the lawful basis for processing. The College may refuse to comply with a request if an exemption applies or if a request is manifestly unfounded or excessive. Every request will be dealt with on a case by case basis.

4.1.6 If an individual has a complaint about the way in which their data subject right request has been dealt with they should contact the Data Protection Officer at DataProtection@yeovil.ac.uk

4.1.7 If an individual remains dissatisfied they have the right to complain to the Information Commissioner's Office[1].

4.1.8 Please contact the Data Protection Officer at DataProtection@yeovil.ac.uk if you wish to withdraw consent to processing.

[1] www.ico.org.uk

4.2 Keeping Data Subjects Informed – Privacy Information

4.2.1 Where the College collects personal data directly from individuals, the College will inform them about the nature and purpose of the processing in a[2] privacy notice published on the College's website. The full list of privacy information we must provide can be found here[3].

4.2.2 Where personal data is collected directly from the individual, this information will be provided at the time of collection. Where we obtain personal data from another source we will, subject to exemptions, communicate this information, as well as the source and the categories of personal data processed, at the time of the first communication with the individual, or before personal data is disclosed to another party or in any event not more than one month after obtaining the personal data.

4.2.3 Further information on the College's processing of special category data and criminal offences data can be found in the College's Appropriate Policy Document[4] which supplements the College's privacy notices.

4.3 The Right of Access

4.3.1 An individual may appoint another person to act on their behalf in making a subject access request (SAR). When this happens, we will need written evidence that the individual concerned has authorised a third party to make the application and may also require further identification for the person making the request so we can be confident of their identity.

4.3.2 On receiving a SAR asking for information held about a child, the College will consider whether the child is mature enough to understand their rights before we respond. If we are confident that the child understands their rights, we will usually respond directly to the child. However, if the child has authorised it or if it is evident that it is in the best interests of the child to do so, we will allow a parent or guardian to exercise the child's rights on their behalf. If they are competent to do so, a child may authorise a third party, other than a parent or guardian to act on their behalf. Further information on this can be found here[5].

---

[2] privacy notice
[3] Information Commission's Office
[4] Appropriate Policy Document.docx
[5] How do we recognise a subject access request (SAR)?

4.4 Right to Rectification

4.4.1 Individuals have the right to have inaccurate personal data rectified or depending on the purposes for processing, to have incomplete data completed. On receiving a request for rectification, the College will take reasonable steps to determine the accuracy of the data we hold and will restrict processing the personal data in question while we do this. Further information can be found here[6]

4.5 Right to Erasure

4.5.1 The right to have personal data erased is also known as the 'right to be forgotten'. This applies only to data the College holds at the time the request is made, and not to data that may be created in the future. The right is not absolute and only applies in certain circumstances. Further information can be found here[7].

4.6 Right to Restrict Processing

4.6.1 As an alternative to the right to erasure, an individual can request that the way an organisation uses their personal data is limited. This is not an absolute right and applies in certain circumstances. Further information can be found here[8].

4.7 Right To Data Portability

4.7.1 Individuals have the right to request personal data they have provided to a controller in a structured, commonly used and machine-readable format. Individuals can receive their data and store it for future re-use or can request that a controller transmits this data directly to another controller. The right to data portability only applies in certain circumstances. Further information can be found here[9].

4.8 Right to Object

[6] Right to rectification | ICO
[7] Right to erasure | ICO
[8] Right to restrict processing | ICO
[9] Right to data portability | ICO

4.8.1 Individuals have the right to stop or prevent processing of their personal data. Whether the right to object applies depends on the purpose for the data is processed and the lawful basis for processing.

4.8.2 The right to object to processing of personal data for the purposes of direct marketing is an absolute right. Therefore, when the College receives such a request it will suppress the personal data of the individual concerned retaining just enough to ensure that they do not receive direct marketing in future.

4.8.3 Further information on the right to object can be found here[10].

4.9 Rights Related to Automated Decision-Making Including Profiling

4.9.1 The College will not use personal data for the purposes of automated decision making that has legal or significantly similar effects on the individual unless the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by UK law; or
- based on the individual's explicit consent.

4.9.2 Where the College does use personal data in this way, individuals have the right to challenge such decisions, request human intervention in the process, express their own point of view and obtain an explanation from the College.

4.9.3 Where the College used automated decision making, including profiling, we will

- provide meaningful information about the way the decision-making process works, as well as explaining the significance and the envisaged consequences for the individual;
- use appropriate mathematical or statistical procedures;
- ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it;
- put appropriate technical and organisational measures in place, so that we can correct inaccuracies and minimise the risk of errors; and

[10] Right to object | ICO

- secure personal data in a way that prevents discriminatory effects and is proportionate to the risks to the individual's rights and interests.

## 5. DATA PROCESSING AND SHARING ACTIVITIES

5.1 Personal Data will be collected, held, and processed by the College and is specified in departmental registers setting out the type of data, data subjects, purpose of processing, type of recipient to whom personal data is transferred and retention period.

5.2 Where personal data that the college has collected is shared with a third party, this will be made clear to data subjects in the College Privacy Policy and the contractual obligations set out in a Data Sharing Agreement or Contract with that party. When the college uses a third-party data processor a written contract will be in place setting out the obligations, responsibilities and liabilities of both parties.

5.3 Where personal data and sensitive personal data is shared between the college and legitimate external agencies (such as a school, Local Authority, Law Enforcement Agencies) in the vital interest of the learner, then consent will not always be sought.

5.4 Where the college is collecting and sharing personal data of a child (under 18) the college will take extra care to ensure that the data is only processed in the best interest of the child. Where consent is required, the college will endeavour to ensure that the child understands the implications and necessity of sharing their personal data.

5.5 All third parties receiving personal data from the college are also subject to the obligations under the UK GDPR and the Data Protection Act 2018.

## 6. DATA PROTECTION MEASURES

All employees, agents, contractors, or other parties working on the College's behalf must comply with the following when working with Personal Data:

6.1 all emails containing Personal Data must be encrypted using password protected attachments only. The password must not be included in the same email and should be sent separately. Personal data should not be copied directly into the body of the email;

6.2 where any Personal Data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and

disposed of. Hardcopies should be put in a secure data bag or shredded and electronic copies should be deleted and also deleted from the recycle bin;

6.3 Personal Data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

6.4 where Personal Data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using registered post depending on the sensitivity of data.

6.5 no Personal Data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the College requires access to any Personal Data that they do not already have access to, such access should be formally requested from the Head of IT Services at Helpdesk@yeovil.ac.uk

6.6 all hardcopies of Personal Data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

6.7 consideration should be given to passing Personal Data to any college employees, agents, contractors, or other parties, whether such parties are working on behalf of the College or not.

6.8 Personal Data must be handled with care at all times and should not be left unattended or on view by unauthorised employees, agents, sub-contractors or other parties at any time;

6.9 if Personal Data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

6.10 no Personal Data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the College or otherwise without the formal written approval of the Vice Principal Finance & Resources at DataProtection@yeovil.ac.uk and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

6.11 no Personal Data should be transferred to any device personally belonging to an employee and Personal Data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the College where the party in question has agreed to

comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the College that all suitable technical and organisational measures have been taken);

6.12 all Personal Data stored electronically should be backed up daily with backups stored onsite and offsite. All backups should be encrypted using Windows security authentication and Veeaam password protection on hardware storage devices.

6.13 all electronic copies of Personal Data should be stored securely using Windows network authentication and only accessible by the IT Services security group; such access should be formally requested from Head of IT Services at helpdesk@yeovil.ac.uk

6.14 all passwords used to protect Personal Data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.

6.15 under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the College, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords but can reset them;

## 7. ORGANISATIONAL MEASURES

The College will ensure that the following measures are taken with respect to the collection, holding, and processing of Personal Data:

7.1 all employees of the College will be made fully aware of both their individual responsibilities and the College's responsibilities under the Regulation and under this Policy, and will have access to a copy of this Policy;

7.2 all agents, contractors, or other parties working on behalf of the College will do so under a written agreement setting out the obligations, responsibilities, and liabilities of both parties under the Regulation and under this Policy and will have access to a copy of this Policy.

7.3 only employees, agents, sub-contractors, or other parties working on behalf of the College that need access to, and use of, Personal Data in order to carry out their assigned duties correctly will have access to Personal Data held by the College;

7.4 all employees, agents, contractors, or other parties working on behalf of the College handling Personal Data will be appropriately trained to do so;

7.5 all employees, agents, contractors, or other parties working on behalf of the College handling Personal Data will be appropriately supervised;

7.6 methods of collecting, holding and processing Personal Data will be regularly evaluated and reviewed;

7.7 the performance of those employees, agents, contractors, or other parties working on behalf of the College handling Personal Data will be evaluated and reviewed regularly;

7.8 all employees, agents, contractors, or other parties working on behalf of the College handling Personal Data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;

7.9 all agents, contractors, or other parties working on behalf of the College handling Personal Data must ensure that any and all of their employees who are involved in the processing of Personal Data are held to the same conditions as those relevant employees of the College arising out of this Policy and the Regulation;

7.10 where any agent, contractor or other party working on behalf of the College handling Personal Data fails in their obligations under this Policy that party will indemnify and hold harmless the College against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

## 8. USE OF CLOSED-CIRCUIT TELEVISION (CCTV) (Appendix C)

8.1 The College is fully committed to operating a safe environment and has therefore placed a closed-circuit television (CCTV) system on campus. This is to assist in providing a safe and secure environment for students, staff and visitors. CCTV systems are based around digital technology and therefore need to be treated as information that will be processed under the Regulation.

8.2 For the purpose of the Data Protection Act 2018 Yeovil College is the data controller.

- CCTV digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act 2018.

- The College has registered its processing of personal data (including CCTV) with the Information Commissioner's Office (ICO).

8.3 All users of the data collected by the College's CCTV will follow the Use of CCTV Protocol set out at Appendix C, which is designed to regulate the management, operation and use of the CCTV system at the college to ensure the College complies with the Data Protection Act 2018, Human Rights Act 1998, UK GDPR and other legislation.

## 9. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE UK

9.1 The College may from time to time transfer ('transfer' includes making available remotely) Personal Data to countries outside of the UK.

9.2 In order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined, the transfer of Personal Data to a country outside of the UK will take place only if one or more of the following applies:

9.2.1 the UK has issued regulations confirming that the country to which the College transfers the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

9.2.2 appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the College's Data Protection Officer;

9.2.3 the Data Subject has provided informed consent to the proposed transfer after being informed of any potential risks; or

9.2.4 the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between the College and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent and, in some limited cases, for the College's legitimate interest;

9.2.5 the transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for Personal Data.

## 10. DATA BREACH NOTIFICATION

10.1 Individuals have a legal duty to report and record both data breaches and near misses, to the college Data Protection Officer. Failure to do so may result in the College taking disciplinary action on the individual.

10.2 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. All Personal Data breaches must be reported immediately to the College's Data Protection Officer who is the Vice Principal Finance & Resources at DataProtection@yeovil.ac.uk

10.3 If a Personal Data breach occurs and that breach is likely to result in a risk to the rights and freedoms of Data Subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

10.4 Where the personal data breach is not reported to the ICO, it will be recorded as such including the reasons for non-notification.

10.5 In the event that a Personal Data breach is likely to result in a high risk (that is, a higher risk than that described under clause 9.2 to the rights and freedoms of Data Subjects), the Data Protection Officer must ensure that all affected Data Subjects are informed of the breach directly and without undue delay.

10.6 Data breach notifications will include the following information:

10.6.1 the categories and approximate number of Data Subjects concerned;

10.6.2 the categories and approximate number of Personal Data records concerned;

10.6.3 the name and contact details of the College's Data Protection Officer (or other contact point where more information can be obtained);

10.6.4 details of the measures taken, or proposed to be taken, by the College to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

## 11. IMPLEMENTATION OF POLICY

This Policy will be deemed effective as of 25 May 2018. It has been updated on 3 August 2023. No part of this Policy will have retroactive effect and will thus apply only to matters occurring on or after this date.

## 12. CHANGES TO THIS POLICY

The College reserves the right to change this Policy at any time. Where appropriate, we will notify Data Subjects of those changes by mail or email.

## 13. RELATED POLICIES, PROCEDURES, DOCUMENTS, DEFINITIONS

Appendix A – Subject Access Request Form
Appendix B – Students with Additional Needs and/or Pastoral Care Needs Agreement for Disclosing Information
Appendix C – Use of CCTV Protocol
Retention of Records Policy
College's Appropriate Policy Document
www.ico.org.uk
privacy notice
Information Commission's Office
How do we recognise a subject access request (SAR)?
Right to rectification | ICO
Right to erasure | ICO
Right to restrict processing | ICO
Right to data portability | ICO
Right to object | ICO

# YEOVIL COLLEGE
# SUBJECT ACCESS REQUEST FORM

You have the right to ask for copies of your personal data we store and use. This is your right of access, also known as making a subject access request or SAR. We'll normally respond at the latest within one calendar month of receiving your request. There may be times where we need longer, or we may need to charge a reasonable fee for admin costs. We'll let you know if this is the case.

You don't have to use this form to ask for copies of your data, but it's helpful for us to know what you're looking for so we can respond fully and promptly.

Please send your completed form to us using the contact details at the bottom of the page.

You can read more about your right of access by visiting: https://ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data/

If you have any queries on this form, please contact the Data Protection Officer at DataProtection@yeovil.ac.uk

## 1. Who's making this request?

We're asking for your contact details so we can send your response and discuss your request with you (if needed). You only need to give us relevant details. We may ask you for proof of ID if we feel it's reasonable and proportionate. The timescale for responding to your request will start when we receive this. We usually respond via email.

**Your name** **Contact number** **Email address**

**Postal address (inc postcode)**

Are you making this request on behalf of someone else?

☐ **Yes**

☐ **No (Please move to section three)**

## 2. Please provide contact details of the person you are making the request for.

If you're making the request on behalf of someone else, we need to know who they are and their contact details in case we need to get in touch.

**Name of other person** **Contact number** **Email address**

**College ID No (if known)** **College Course (if known)**

**Postal address (inc postcode)**

**Other contact information for the person you are making the request for**

You also need to give us proof of your authority to act on their behalf. For example, this could be written authorisation from them or a relevant power of attorney.

Please send proof of authority together with this form when you make your request.

☐ Yes, I've got proof of my authority to act on someone else's behalf and I'll include it with my form. (Please move to section three.)

☐ No, I haven't got any proof of authority yet, but will send it at a later date. I understand you can't action my request until you receive this information.

## 3. What personal data are you requesting?

If you know exactly what personal data you're looking for, it's helpful if you let us know.
For example, names of individuals who may hold the information, form of information (such as paper file or email), this will assist us in locating the information you are seeking.

**Briefly describe your request**

## 4. Is there a date range of the personal data you're asking for?

It's helpful if you're as specific as possible about your request. For example, if you've been a customer for several years, but you only need data about your recent purchase history, you could ask for data about thing you've bought only in the last few months.

**Date from** **Date to**

## 5. Can you tell us anything else to help us with our search?

If there's anything else of relevance you can tell us to help us identify you or the data you're requesting, please include this here. For example, any aliases, date of birth, order number or a customer reference number.

**Further information to help us find the data you need**

By signing below you indicate that you are the data subject named above, or have authority from the data subject. We may need to contact you for further identifying information before processing with your request (if needed). You warrant that you are the data subject, or are authorised to act on their behalf and will fully indemnify us for all losses, cost and expenses if you are not.

Please note, if your request for data access is deemed excessive, an administrative charge may be required. You will be notified if this is the case given details of the amount payable and how to pay. Whilst we endeavour to process your request at the earliest opportunity, please allow up to one month for a reply.

**Data Subjects Signature** **Date**

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data and the following information:

2. The purpose of the processing;

3. The categories of personal data concerned;

4. The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

5. Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

6. The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
7. The right to lodge a complaint with a supervisory authority;

8. Where the personal data are not collected from the data subject, any available information as to their source;

9. The existence of automated decision making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

**Please keep one copy and return one copy via email to the Data Protection Officer at:**
**dataprotection@yeovil.ac.uk**

**Appendix B**

# YEOVIL COLLEGE
# ADDITIONAL NEEDS CONSENT FORM

**STUDENTS WITH ADDITIONAL NEEDS AND/OR PASTORAL CARE NEEDS**
**AGREEMENT FOR DISCLOSING INFORMATION**

**Student name:** _____ **ID number:** _____

☐ I have discussed the guidelines on disclosure of information and understand that any relevant information about my needs may be passed to appropriate professional people in order to ensure my needs are met.

☐ I consent to information about my needs being passed to funding bodies and relevant people who may include:

- Learning Link Team
- Student Support Services (emotional support and counselling team)
- College staff (Tutors, Lecturers as appropriate)
- Appropriate external agencies such as Children's Social Care, Youth offending Team, Team CAT 8, CAMHS, Adult Mental Health Services, GPs and Police. This list is not exhaustive and if there is another agency that is working with you then the Student Support and safeguarding team may need to contact them to share/gain information to keep you safe.
- Local Authority funding commissioners
- Local Authority SEND departments

| | | | |
|---|---|---|---|
| **Signed Student** | | **Print Student Name** | |
| **Signed Staff** | | **Print Staff Name** | |
| **Date** | | **Date** | |

This form will be kept electronically, and the paper version will be destroyed. We will hold this information for as long as you are a student with the college and in safeguarding situations this can be indefinitely.

Article 6(1)(a,c,d,e) - consent, legal obligations, vital interests, public interest Article 9(2)(h) - Management of Health or Social Care systems.

**Appendix C**

## USE OF CCTV PROTOCOL

1. This document sets out the accepted use and management of the CCTV system and images to ensure the College complies with the Data Protection Act 2018, Human Rights Act 1998, the UK GDPR and other legislation and relevant codes of practice.

2. This covers the use of surveillance technologies which record identifiable images of people on college premises, including facial recognition. CCTV is defined as: fixed and portable cameras designed to capture and record images of individuals, groups and areas on the college site.

3. Surveillance System is defined as: any electronic system or device that captures images of individuals, information relating to groups or areas on the college site. This term is used to refer to any surveillance technology including CCTV. It also includes CCTV technology, such as automatic number plate recognition (ANPR), body worn cameras or aerial surveillance systems.

4. The College system comprises of a number of fixed and portable cameras located both internally and externally around the College site. All cameras may be monitored and are only available for use by Security Industry Authority trained and approved members of staff.

5. The college has in place video surveillance systems to provide a safe and secure environment for students, staff and visitors, and to protect college property.

6. The college has evaluated where there is a requirement for video surveillance technology. Reasons for a decision to install may include but are not limited to the following:

    a. Deter crime, vandalism, damage or disruption.
    b. Assist in prevention and detection of crime and to aid security of campus buildings.
    c. Assist with the identification, apprehension and prosecution of offenders.
    d. Assist with the identification of actions that might result in disciplinary proceedings against staff and students.
    e. Identify vehicle movement problems around the campuses.

7. The system will be provided and operated in a way that is consistent with an individual's right to privacy.

**Responsibility and Authority**

Operation

8. The CCTV surveillance system is owned by Yeovil College.

9. The Head of Infrastructure is responsible for the operation of the system and ensuring compliance with this policy. The College has one member of staff, who is SIA trained and additional approved members of staff who can review CCTV footage.

10. The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and will seek to comply with the requirements both of the Data Protection Act 2018 and the Commissioner's Code of Practice.

11. Static cameras will not focus on private homes, gardens and other areas of private property.

12. Materials or knowledge secured as a result of CCTV system will not be used for any commercial purpose. Downloads will only be released to the police to assist in an investigation.

13. The planning and design of the existing CCTV system has endeavoured to ensure that the CCTV system will give maximum effectiveness and efficiency, but it is not possible to guarantee that the CCTV system will cover or detect every single incident taking place in the areas of coverage.

14. Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at access routes and areas covered by the college CCTV System. These must state that monitoring is in use, the name of the organisation responsible, the reason for the monitoring and give contact details for any enquiries.

15. Image Viewing and Download Procedure

    a. All reviewed CCTV systems must be fully recorded in the Digital Video Recorder Incident Management Books (DVRIM). The fix camera CCTV system DVRIM book is located in the Kingston Server room, and the body camera DVRIM book is located in the Student experience room. Approved members of staff will be listed in the DVRIM booklets.

b. Recordings may be viewed by the police and authorised officers, if authorised by a College SIA Operative and the Principal or Vice Principals of the college.
c. Should a download be required as evidence, an electronic copy may only be made by a
d. holder of a SIA CCTV Licence or by the approved members of staff.
e. Where this is to be released to the Police, it will only be released on completion of
f. Data Release Form in the Digital Video Recorder Incident Management Book and sight of their warrant card.
g. Where this is requested by the Principal, Vice Principals or the Head of Student experience, a CCTV Request will be sent via email to the SIA college operative or approved members of staff..
h. Where this is requested by Principal / Duty Manager / Investigating Officer investigating into a student incident, a CCTV Request Form will be completed and given to the SIA college operative or approved members of staff.
i. Where this is requested by other parties, a CCTV Request Form will be completed by the
j. an SIA college operative. A fee of up to £100 may be charged for this service.
k. All requests for downloads on the fixed CCTV system, will be retained in the Kingston Server room by the SIA college operative for 12 months or after the incident that the download relates to has been closed. All requested downloads on the body cameras, will be downloaded securely and kept within the Student Experience SharePoint site. Review access will be controlled by the Head of Student Experience and archived in accordance with the student records archive procedure.

16. CCTV and Surveillance System will not be used to:

a. Provide images to the world wide web.
b. Record sound.
c. Disclose to the media.

**Breaches of this Policy**

17. Any suspected breach of this protocol by College staff or students will be considered under the relevant College Disciplinary Policy.

**Overview of System**

18. The CCTV system runs 24 hours a day, 7 days a week and images are recorded continuously for 30 days after which the data overwrites itself. The CCTV system comprises fixed position cameras; portable body cameras, monitor; digital recorder and public information signs. CCTV fixed cameras are located at strategic points on site, principally at the entrances and exit points for the site and various buildings.

19. Although every effort has been made to ensure maximum effectiveness of the CCTV systems; it does not cover all areas and it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

20. Where new cameras are to be installed on College premises, Part 4 of the ICO's CCTV code of Practice will be followed before installation:

    a. The appropriateness of and reasons for using CCTV will be assessed and documented;
    b. The purpose of the proposed CCTV system will be established and documented;
    c. Responsibility for day-to-day compliance with this policy will be established and documented.

**Access to Images**

Individual Access Rights

21. The Data Protection Act 2018 gives individuals the right to access personal information about themselves, including CCTV images.
    All requests for access to view/copy CCTV footage by individuals should be made in writing to the Data Protection Officer.

Requests for access to CCTV images must include:

    a. The reason for the request
    b. Who is requesting the recordings
    c. The date and time the images were recorded
    d. Information to identify an individual, group or situation.
    e. The location of the CCTV camera

22. The College will respond promptly and at the latest within 30 calendar days of receiving the request processing fee, determined by the Data Protection Officer and sufficient information to identify the images requested.

23. If the College cannot comply with the request, the reasons will be documented. The requester will be advised of these in writing, where possible.

**Access to Images by Third Parties**

24. Unlike Data Subjects, third parties who wish to have a copy of CCTV images (i.e. images not of the person making the request) do not have a right of access to images under the (Data Protection Act (DPA), and care must be taken when complying with such requests to ensure that neither the DPA, Human Rights Act (HRA) or the CCTV Policy are breached. As noted above, requests from third parties will only be granted if the requestor satisfies the following criteria:

    a. Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry)
    b. Prosecution Agencies and their Legal Representatives
    c. Insurance Companies and their Legal Representatives

25. All third-party requests for access to a copy of CCTV footage should be made in writing to the Data Protection Officer. If a law enforcement or prosecution agency is requesting access, they should make a request under Section 29 of the Data Protection Act 1998 using a Section 29 Data Protection Request form.

**Retention and Disposal**

26. Recorded images will be retained for no longer than 30 days from the date of recording, unless required for evidential purposes or the investigation of crime or otherwise required and retained as a download with the requisite approval form.

27. All images on electronic storage will be erased by automated system overwriting. All downloads, still photographs and hard copy prints will be securely disposed of as confidential waste. The date and method of destruction will be recorded on the bottom of the original approval to copy held by the Data Protection Officer.

## RELATED POLICIES, PROCEDURES, DOCUMENTS

Home Office Surveillance Camera Code of Practice