Reference Number: *P27*

DATA PROTECTION POLICY

PURPOSE OF THE POLICY

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").

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.

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.

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.

RESPONSIBILITY & AUTHORITY

1. THE DATA PROTECTION PRINCIPLES

1.1 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:

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

1.1.2 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;

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

1.1.4 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;

1.1.5 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;

1.1.6 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;

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

1.1.8 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).

1.2 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:

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

1.2.2 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;

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

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

1.2.5 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;

1.2.6 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.

1.3 Processed for Specified, Explicit and Legitimate Purposes

1.3.1 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).

1.3.2 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.

1.4 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 1.2.6.

1.5 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.

1.6 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.

1.7 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.

2. ACCOUNTABILITY

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

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

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

2.2.2 the purposes for which the College processes Personal Data;

2.2.3 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;

2.2.4 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;

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

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

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

2.3 Privacy Impact Assessments

The College will carry out Privacy Impact Assessments when and as required under the Regulation. In general, data protection impact assessments are appropriate for projects where one or more of the following applies:

2.3.1 information about living individuals will be collected and processed for the first time;

2.3.2 information about living individuals will be shared with people or organisations that previously did not have access to it;

2.3.3 change of use of existing Personal Data;

2.3.4 the use of new technology that collects or uses data of a personal nature e.g. biometrics or artificial intelligence;

2.3.5 existing Personal Data will be used to reach decisions as part of an automated process;

2.3.6 it might reasonably be expected that an individual may find any aspect of the project intrusive or the data involved private.

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

2.3.7 the purpose(s) for which Personal Data is being processed and the processing operations to be carried out on that Personal Data;

2.3.8 details of the legitimate interests being pursued by the College;

2.3.9 an assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

2.3.10 an assessment of the risks posed to individual Data Subjects; and

2.3.11 details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of Personal Data, sufficient to demonstrate compliance with the Regulation.

Please refer to the Data Protection Officer Procedures for details about how to assess the need and process for completing a Privacy Impact Assessment

3. THE RIGHTS OF DATA SUBJECTS

3.1 The Regulation sets out rights applicable to Data Subjects, including:

3.1.1 the right to withdraw consent to processing at any time;

.

3.1.2 the right to be informed;

3.1.3 the right of access;

3.1.4 the right to rectification;

3.1.5 the right to erasure (also known as the 'right to be forgotten');

3.1.6 the right to prevent use of their Personal Data for direct marketing purposes;

3.1.7 the right to restrict processing in specific circumstances;

3.1.8 the right to data portability;

3.1.9 the right to object;

3.1.10 rights with respect to automated decision-making and profiling;

3.1.11 the right to challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

3.1.12 the right to request a copy of an agreement under which Personal Data is transferred outside of the UK;

3.1.13 the right to complaint to a 'supervisory authority' under the Regulation.

3.2 Keeping Data Subjects Informed

The College will ensure that the following information is provided to every Data Subject when Personal Data is collected:

3.2.1 details of the College including, but not limited to, the identity of its Data Protection Officer;

3.2.2 the purpose(s) for which the Personal Data is being collected and will be processed (as detailed in clause 4 of this Policy) and the legal basis justifying that collection and processing;

3.2.3 where applicable, the legitimate interests upon which the College is justifying its collection and processing of the Personal Data;

3.2.4 where the Personal Data is not obtained directly from the Data Subject, the categories of Personal Data collected and processed;

3.2.5 where the Personal Data is to be transferred to one or more third parties, details of those parties;

3.2.6 where the Personal Data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place (see clause 7 of this Policy for further details concerning such third country data transfers);

3.2.7 details of the length of time the Personal Data will be held by the College (or, where there is no predetermined period, details of how that length of time will be determined);

3.2.8 details of the Data Subject's rights under the Regulation;

3.2.9 details of the Data Subject's right to withdraw their consent to the College's processing of their Personal Data at any time;

3.2.10 details of the Data Subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);

3.2.11 where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the Personal Data and details of any consequences of failing to provide it;

3.2.12 details of any automated decision-making that will take place using the Personal Data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

3.2.13 The information set out above in clause 3.2 will be provided to the Data Subject:

3.2.13.1 where the Personal Data is obtained from the Data Subject directly, at the time of collection;

3.2.13.2 where the Personal Data is not obtained from the Data Subject directly (i.e. from another party):

a. if the Personal Data is used to communicate with the Data Subject, at the time of the first communication; or

b. if the Personal Data is to be disclosed to another party, before the Personal Data is disclosed; or

c. in any event, not more than one month after the time at which the College obtains the Personal Data.

3.3 Data Subject Access

3.3.1 A Data Subject may make a subject access request ("**SAR**") at any time to find out more about the Personal Data which the College holds on them. The College is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests and, in such cases, the Data Subject will be informed of the need for the extension).

3.3.2 All subject access requests received must be forwarded to the Vice Principal Finance & Resources at DataProtection@yeovil.ac.uk within 24 hours of receipt.

3.3.3 The College does not charge a fee for the handling of normal SARs. The College reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a Data Subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

3.4 Rectification of Personal Data

3.4.1 If a Data Subject informs the College that Personal Data held by the College is inaccurate or incomplete, requesting that it be rectified, the Personal Data in question will be rectified, and the Data Subject informed of that rectification, within one month of receipt the Data Subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the Data Subject will be informed of the need for the extension).

3.4.2 In the event that any affected Personal Data has been disclosed to third parties, those parties will be informed of any rectification of that Personal Data.

3.5 Erasure of Personal Data

3.5.1 Data subjects may request that the College erases the Personal Data it holds about them in the following circumstances:

3.5.1.1 it is no longer necessary for the College to hold that Personal Data with respect to the purpose for which it was originally collected or processed;

3.5.1.2 the Data Subject wishes to withdraw their consent to the College holding and processing their Personal Data;

3.5.1.3 the Data Subject objects to the College holding and processing their Personal Data (and there is no overriding legitimate interest to allow the College to continue doing so) (see clause 3.8 of this Policy for further details concerning Data Subjects' rights to object);

3.5.1.4 the Personal Data has been processed unlawfully; or

3.5.1.5 the Personal Data needs to be erased in order for the College to comply with a particular legal obligation.

3.5.2 Unless the College has reasonable grounds to refuse to erase Personal Data, all requests for erasure will be complied with, and the Data Subject informed of the erasure, within one month of receipt of the Data Subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the Data Subject will be informed of the need for the extension).

3.5.3 In the event that any Personal Data that is to be erased in response to a Data Subject request has been disclosed to third parties, those parties will be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

3.6 Restriction of Personal Data Processing

3.6.1 Data subjects may request that the College ceases processing the Personal Data it holds about them. If a Data Subject makes such a request, the College will retain only the amount of Personal Data pertaining to that Data Subject that is necessary to ensure that no further processing of their Personal Data takes place.

3.6.2 In the event that any affected Personal Data has been disclosed to third parties, those parties will be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

3.7 Data Portability

3.7.1 Where Data Subjects have given their consent to the College to process their Personal Data in such a manner or the processing is otherwise required for the performance of a contract between the College and the Data Subject, Data Subjects have the legal right under the Regulation to receive a copy of their Personal Data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

3.7.2 To facilitate the right of data portability, the College will make available all applicable Personal Data to Data Subjects in the format of emails on our electronic system or hard copy.

3.7.3 If requested by a Data Subject, Personal Data will be sent directly to another data controller.

3.7.4 All requests for copies of Personal Data will be complied with within one month of the Data Subject's request (this can be extended by up to two months in the case of complex requests or numerous requests and in such cases the Data Subject will be informed of the need for the extension).

3.8 Objections to Personal Data Processing

3.8.1 Data subjects have the right to object to the College processing their Personal Data based on legitimate interests, direct marketing including profiling and statistics purposes.

3.8.2 Where a Data Subject objects to the College processing their Personal Data based on its legitimate interests, the College will cease such processing forthwith, unless it can be demonstrated that the College's legitimate grounds for such processing override the Data Subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

3.8.3 Where a Data Subject objects to the College processing their Personal Data for direct marketing purposes, the College will cease such processing forthwith.

3.8.4 Where a Data Subject objects to the College processing their Personal Data for statistics purposes, the Data Subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The College is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

3.9 Automated Decision-Making

3.9.1 The College will not use Personal Data for the purposes of automated decision-making when those decisions have a legal (or similarly significant effect) on Data Subjects unless:

3.9.1.1 the decision is necessary for the entry into, or performance of, a contract between the College and the Data Subject;

3.9.1.2 the decision is authorised by law; or

3.9.1.3 the Data Subject has given their explicit consent.

3.9.2 Where the College using Personal Data in accordance with 3.9.1 above, Data Subjects have the right to challenge such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the College.

3.9.3 A DPIA will be carried out before any automated processing or automated decision-making activities are undertaken.

3.10 Profiling

Profiling is a form of automated processing which is intended to evaluate certain personal aspects of an individual in particular to analyse the performance at work, health, personal preferences, reliability, location, movements etc. Where the College uses Personal Data for profiling purposes, the following will apply:

3.10.1 clear information explaining the profiling will be provided, including its significance and the likely consequences;

3.10.2 appropriate mathematical or statistical procedures will be used;

3.10.3 technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected will be implemented; and

3.10.4 all Personal Data processed for profiling purposes will be secured in order to prevent discriminatory effects arising out of profiling.

4. DATA PROCESSING ACTIVITIES

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. 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:

5.1 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;

5.2 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;

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

5.4 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.

5.5 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

5.6 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;

5.7 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.

5.8 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;

5.9 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;

5.10 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;

5.11 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);

5.12 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.

5.13 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

5.14 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.

5.15 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;

6. ORGANISATIONAL MEASURES

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

6.1 all employees, agents, contractors, or other parties working on behalf 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;

6.2 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;

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

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

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

6.6 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;

6.7 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;

6.8 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;

6.9 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.

7. USE OF CLOSED CIRCUIT TELEVISION (CCTV) (Appendix D)

7.1 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.

7.2 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).

7.3 All users of the data collected by the College's CCTV will follow the Use of CCTV Protocol set out at Appendix D, 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.

8. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE UK

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

8.2 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:

8.2.1 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;

8.2.2 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;

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

8.2.4 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;

8.2.5 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.

9. DATA BREACH NOTIFICATION

9.1 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.

9.2 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.

9.3 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 9.1 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.

9.4 Data breach notifications will include the following information:

9.4.1 the categories and approximate number of Data Subjects concerned;

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

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

9.4.4 the likely consequences of the breach;

9.4.5 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.

10. IMPLEMENTATION OF POLICY

This Policy will be deemed effective as of 25 May 2018. It has been updated on 11 June 2021. No part of this Policy will have retroactive effect and will thus apply only to matters occurring on or after this date.

11. 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.

RELATED POLICIES, PROCEDURES, DOCUMENTS, DEFINITIONS

Appendix A – Subject Access Request Form
Appendix B – Data Breach Reporting Form
Appendix C – Students with Additional Needs and/or Pastoral Care Needs Agreement for Disclosing Information
Appendix D – Use of CCTV Protocol

Retention of Records Policy
Retention of Records Procedure
Data Protection Procedure
Home Working Policy

YEOVIL COLLEGE
SUBJECT ACCESS REQUEST FORM

Should you wish to access certain information held about you, please complete this form and return it to the Data Protection Officer by email. This is permitted under the UK General Data Protection Regulations (GDPR).

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

Name *Include all known names to assist with the request*		**Address**	
Daytime telephone number		**Department** *For staff only*	

By completing this form you are making a request under the DPA/UK GDPR for information held about you by the College that you are eligible to receive.

Required information

Please specify exactly what information you seek and any relevant dates, names of individuals who may hold the information, form of information (such as paper file) to assist us in locating the information you are seeking:

By signing below you indicate that you are the data subject named above. The College cannot accept requests from anyone else (such as family members) regarding your personal data. We may need to contact you for further identifying information before proceeding with your request (if needed). You warrant that you are the data subject 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 administration 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 will endeavour to process your request at the earliest opportunity. Please allow up to one month for a reply.

Data subject's signature		**Date**	

Please keep one copy and return one copy via email to the Data Protection Officer as above.

YEOVIL COLLEGE
DATA BREACH REPORTING FORM

This form should be used to report details of an actual or suspected data breach. The form can be downloaded at Blank Data Breach Reporting Form

Please answer the questions below as fully as you can and then email this form to the Data Protection Officer at your earliest convenience and no later than 24 hours of the actual or suspected breach being identified. Please refer to the Data Protection Policy for further guidance.

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

If you believe the issue is urgent call the Data Protection Officer on 01935 845458

Person making the report		**Department**	
Contact telephone number		**Date of report**	
Date of actual or suspected breach			
Date of discovery of actual or suspected breach			
Summary of the facts *Provide as much information as possible, including the amount, sensitivity and type of data involved*			
Is there a breach of employee or customer/ client confidentiality?		**Yes/No** *If yes, provide more detail*	
Cause of the actual or suspected breach *Provide a detailed account of what happened*			
Is the actual or suspected breach on-going?		**Yes/No** *If yes, provide more detail*	
Who is or could be affected by the actual or suspected breach? *Include details of categories and approximate number of data subjects concerned. Do not notify affected data subjects. The Data Protection Officer will determine who should be notified and how.*			
Are you aware of any related or other data breaches?		**Yes/No** *If yes, provide more detail*	

YEOVIL COLLEGE
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: _____

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 D

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 and the UK GDPR.

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:

   - Deter crime, vandalism, damage or disruption.
   - Assist in prevention and detection of crime and to aid security of campus buildings.
   - Assist with the identification, apprehension and prosecution of offenders.
   - Assist with the identification of actions that might result in disciplinary proceedings against staff and students.
   - 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 IT Services is responsible for the day-to-day 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

- 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.
- 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.
- Should a download be required as evidence, an electronic copy may only be made by a holder of a SIA CCTV Licence or by the approved members of staff.
- Where this is to be released to the Police, it will only be released on completion of Data Release Form in the Digital Video Recorder Incident Management Book and sight of their warrant card.
  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..
- 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.
- Where this is requested by other parties, a CCTV Request Form will be completed by the an SIA college operative. A fee of up to £100 may be charged for this service.
- 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:

- Provide images to the world wide web.
- Record sound.
- 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:

- The appropriateness of and reasons for using CCTV will be assessed and documented;
- The purpose of the proposed CCTV system will be established and documented;
- 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:

- The reason for the request
- Who is requesting the recordings
- The date and time the images were recorded
- Information to identify an individual, group or situation.
- 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:

- Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry)
- Prosecution Agencies and their Legal Representatives
- 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, DE Home Office Surveillance Camera Code of Practice.

Policy Review				
Author/Owner Emma Cox	Position VP Finance & Resources	Approved by Corporation Signed: 	Approval date 07.07.22	Review Period 2 years

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	

Initial Equality Impact Screening

Have you consulted on this policy, service, strategy, procedure or function? Yes
Details: Clarke Willmott solicitors and the GDPR Panel

What evidence has been used for this assessment?

Could a particular group be affected differently in either a negative or positive way? Indicate Y where applicable

Group	Negative impact	Positive impact	Evidence
Age			
Disability			
Gender (incl. Transgender)			
Race (incl. Gypsy &Traveller)			
Religion or belief			
Sex			
Sexual orientation			
Marriage & civil partnership			
Pregnancy & maternity			
Other groups (see guidance)			

Please give details:

If any negative impacts are identified, are there any related polices, services, strategies, procedures or functions that need to be assessed alongside this screening? If yes, please detail below:

Should the policy proceed to a full Equality Impact Assessment? No
If no, please give reasons: the new GDPR enable individuals to understand how and why their data is being used; the policy reflects this and no-one is disadvantaged by it.

Declaration
We are satisfied that an initial screening has been carried out on this policy and a full Equality Impact Assessment is not required.

We understand that the Equality Impact Assessment is required by the College and that we take responsibility for the completion and quality of this assessment

Completed by Author: Emma Cox Position: Vice Principal Finance & Resources Date: 27.04.18

Reviewed by Safeguarding, Equality & Diversity Group: Date: 09.05.18

Comments from Safeguarding, Equality & Diversity Group Review: