DATA PROTECTION POLICY

SEPTEMBER 2020

CONTENTS

INTRODUCTION

The College has a responsibility to maintain its records and record keeping systems. When doing this, the College will take account of the following factors:

- The most efficient and effective way of storing records and information
- The confidential nature of the records and information stored
- The security of the record systems used
- Privacy and disclosure
- Their accessibility.

This policy does not form part of any team member's contract of employment and is not intended to have contractual effect. It does, however, reflect the College's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the College from time to time and any changes will be notified to team members within one month of the date on which the change is intended to take effect. The College may also vary any parts of this procedure, including any time limits, as appropriate in any case.

SCOPE

The College has several Creative Learning Studios (CLS) that provide appropriate, challenging, and meaningful study programmes, to increase employability skills. This policy relates to distance learning and e-safety across all aspects of the work of the College.

Any reference to 'College' in this policy means each of the above CLS'.

Any reference to the College 'team' in this policy means all staff and volunteers working at each of the above CLS'.

OUR VALUES

To be Respectful, Responsible, Safe and Kind, are at the core of our values. They are reflective of expected behaviours and set the foundation upon which the College builds its culture.

COMMUNICATION

This policy will be:

- Displayed on the College website
- Included as part of the induction pack for all new staff.

REVIEW AND MONITORING

The Board of Governors and the College Lead are responsible for overseeing, reviewing, and updating this policy, which will be reviewed annually.

We will monitor the effectiveness of this and all our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the College and all data subjects.

The College team will be informed or any updates or amendments.

RELATED POLICIES

This policy should be read in conjunction with the following policies:

Data Retention
Data Breach
Safeguarding

LEGISLATION & ACCOUNTABILITIES

The General Data Protection Regulation (GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed, or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

This policy is intended to be fully compliant with the Data Protection Act 1998 (DPA 1998), the General Data Protection Regulations 2018 and the 6 data protection principles set out in the GDPR. It is based on guidance published by the Information Commissioners Office (ICO), on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras

The College is committed to adhering to good practice guidelines in the handling of personal data and compliance with all relevant legislation.

INFORMATION COLLECTED BY THE COLLEGE

While running the College and providing educational provision, we collect the following personal information about our students:

- names, addresses, telephone numbers, e-mail addresses and other contact details for parents and next of kin;
- Information about members of your family, your family relationships and family circumstances (including eligibility for bursary funds and free college meals). We may also need information about any court orders or criminal petitions which relate to you so that we can comply with safeguarding obligations to protect students' welfare and well-being;
- Name, home address and date of birth of student;
- National Insurance Number (for students over the age of 19); Unique pupil number (UPN) or unique learner number (ULN) of student;
- Ethnicity and religion of student;

- References given or received by the College about students and information provided by other educational establishments and/ or other professionals or organisations working with students;
- Information about health and medical requirements, including personal care information;
- dietary requirements and allergies
- Copies of Education, Health and Care Plans (EHCPs) and Statement of Special Educational Needs (including information about learning difficulties or disabilities);
- Education, care, and therapy reports from previous education providers;
- Individual Learning Plans;
- Meeting minutes (regarding education, care and therapy, progress and behaviour);
- Case notes and clinical notes (regarding medical, care, behaviour and therapy);
- Annual review documentation;
- Social worker details and safeguarding information;
- Bank details and other financial information (where required);
- Attendance and behaviour records
- Assessment and attainment information including student work and marks;
- We may take pictures of students for the purpose of admission and/or reports to support their education and development;
- We may take pictures of you and/or your child at college events to use in marketing material. This is usually to show prospective parents and students what we do and to keep our current parents informed of events. This is always with your consent;
- We use CCTV at the college to ensure the site is safe;
- Trips and activities information;
- Progression data in terms of establishments attended after leaving the college such as educational institution or supported living services attended.

The College processes this information to enable the registration of a student, provide the educational study programme and for the purposes of management information, forecasting and planning activities.

REGISTRATION WITH THE INFORMATION COMISSIONER'S OFFICE (ICO)

Notification is the process by which the data controller's details are added to a public register. This register is maintained by the Information Commissioner and can be consulted by individuals to find out what processing of personal data is being carried out by a particular data controller. The College as data controller shall be registered with the Information Commissioner's Office (ICO) under the 1998 Data Protection Act and this will be renewed annually.

- The information that will be required for notification includes:
- Name and address of data controller
- Nominated representative (if applicable)
- Description of the personal data being processed and the category of data subject to which they relate.
- Description of the purpose(s) for which the data is/are being processed
- Description of any recipients to whom the data will be disclosed
- Names of any countries outside the EEA to which data is or will be transferred.

WHERE THE COLLEGE COLLECTS ITS PERSONAL DATA FROM

We collect and hold personal information relating to our students, much of which is collected via our application form process, but may also receive information about them from other sources, including:

- Parents/Guardians/ Carers
- Previous school/college
- Local Authority / Social Services
- Department for Education (DfE)
- Health professionals

WHO THE COLLEGE SHARES ITS PERSONAL DATA WITH

Routine data sharing

The College routinely shares personal information with:

- Past and future educational establishments – usually on request from other schools or colleges;
- Others with Parental Responsibility for a student;
- Local Authority (e.g. SEN Team, Adult Social Care Team, Health Team);
- Examination Awarding Bodies

Third party Suppliers

In accordance with the relevant data protection legislation, some of the College's processing activity is carried out on its behalf by third parties, such as IT systems, web developers and cloud storage providers.

There may also be occasions where data is shared with other contractors and suppliers, such as education software providers, document destruction services, consultants, and other experts such as educational psychologists or therapists.

This type of data sharing is always subject to contractual assurances that personal data will be kept securely and only in accordance with the College's specific directions. The College will need to share personal information relating to its community with third parties, such as professional advisors or relevant authorities, such as the Local Authority.

Other Data Sharing

We will share personal information with law enforcement or other authorities if required by applicable law.

The College may also be required to share information with:

- The Police, for example where we have safeguarding concerns of a serious nature;
- With other emergency services if there is an emergency while students are in our care;

- Consultants, experts and other professional advisors, eg Ofsted, to assist the College in properly running the college;
- Our insurance company, for example if there is an incident on the College site;
- Organisations that the College works with to support our students. For example some organisations may offer support regarding trips we organise or provide work experience activities; and
- Health professionals to effectively meet the health care needs of the student.

The above authorities will have their own policies relating to the protection of any data that they receive or collect.

DATA PROTECTION PRINCIPLES

- Personal data must be processed lawfully, fairly and in a transparent manner
- Personal data must be collected only for specified, explicit and legitimate purposes
- Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed (*Please refer to the College's Data Retention Policy for further guidance*).
- Personal data must be accurate and, where necessary, kept up to date
- Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (*Please refer to the College's Retention Policy for further details about how the College retains and removes data)*
- Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage

Personal Data

The College will only collect, process, and share personal data fairly and lawfully and for specified purposes. The College must have a specified purpose for processing personal data and special category of data as set out in the GDPR.

Before the processing starts for the first time, we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

The College may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or to carry out official functions as authorised by law;

- For the purposes of the College's legitimate interests where authorised in accordance with data protection legislation. This is if it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Personal Data Breaches

The GDPR requires the College to notify any applicable personal data breach to the ICO. We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so. If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the College Lead or the DPO. **Please refer to our separate Data Breach Policy for more detailed information.**

Special Category Data

The College may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the College in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing in necessary for archiving, statistical or research purposes.

The College identifies and documents the legal grounds being relied upon for each processing activity.

Personal data of the College Team

We will collect and use the following types of personal data about team members

- recruitment information, an application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments
- contact details and date of birth
- the contact details for emergency contacts

- gender
- marital status and family details
- information about contracts of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement
- bank details and information in relation to tax status including national insurance number
- identification documents including passport and driving licence and information in relation to immigration status and right to work for the College
- information relating to disciplinary or grievance investigations and proceedings (whether or not a particular member of staff was the main subject of those proceedings)
- information relating to performance and behaviour at work
- training records
- electronic information in relation to use of IT systems/swipe cards/telephone systems
- images (whether captured on CCTV, by photograph or video); and
- any other category of personal data of which we may notify from time to time.

Special categories of personal data of team members

We may hold and use any of the special categories of personal data of team members in accordance with the law.

Obligations of Team Members

Any team member may have access to the personal data of other team members, suppliers, parents or students at the College in the course of their employment or engagement. If so, the College expects those members of the team to help meet the College's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only view, and work on and save, documents on the College share-point systems, on College systems owned by Project Inc, and never on personal laptops or personal devices;
- Never download any documents to your own personal laptop or device;
- Only log onto, and access Project Inc social media from devices owned and operated by Project Inc;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example by complying with rules on access to college premises, computer access, password protection and secure file storage and destruction
- Not to remove personal data or devices containing personal data from the College premises unless appropriate security measures are in place (such as Pseudonymisation, encryption, password protection) to secure the information;
- Not to store personal information on local drives.

Consent

Where the College relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the College will normally seek another legal basis to process that data. However, if explicit consent is required the data subject will be provided with full information in order to provide explicit consent.

The College will keep records of consents obtained in order to demonstrate compliance with consent requirements under the GDPR.

Data Protection Officer: Lindsey Rhodes

Address: 71 Westholme close, Congleton, CW12 4FZ

Email: lindsey@projectinc.co.uk

Telephone: 07773776862

The DPO is responsible for overseeing this data protection policy, monitoring compliance with the data protection law and developing data-related policies and guidelines.

Responsibility for day to day compliance is delegated to the College Lead.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances: -

(a) If you are unsure of the lawful basis being relied on by the College to process personal data;

(b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);

(c) If you need to draft privacy notices or fair processing notices;

(d) If you are unsure about the retention periods for the personal data being processed;

(e) If you are unsure about what security measures need to be put in place to protect personal data;

(f) If there has been a personal data breach [*and would refer you to the procedure set out in the College's breach notification policy*];

(g) If you are unsure on what basis to transfer personal data outside the EEA;

(h) If you need any assistance dealing with any rights invoked by a data subject;

(i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;

(j) If you plan to undertake any activities involving automated processing or automated decision making;

(k) If you need help complying with applicable law when carrying out direct marketing activities;

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

DATA SUBJECT'S RIGHTS AND REQUESTS

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the College handles their personal data are set out below: -

(a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;

(b) Receive certain information about the College's processing activities;

(c) Request access to their personal data that we hold;

(d) Prevent our use of their personal data for marketing purposes;

(e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

(f) Restrict processing in specific circumstances;

(g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) Object to decisions based solely on automated processing;

(i) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;

(j) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(k) Make a complaint to the supervisory authority; and

(l) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the College to verify the identity of the individual making the request.

Subject Access Requests

A Data Subject has the right to be informed by the College of the following: -

(a) Confirmation that their data is being processed;

(b) Access to their personal data;

(c) A description of the information that is being processed;

(d) The purpose for which the information is being processed;

(e) The recipients/class of recipients to whom that information is or may be disclosed;

(f) Details of the College's sources of information obtained;

(g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct.

(h) Other supplementary information

Any Data Subject who wishes to obtain the above information must notify the College in writing of his or her request. This is known as a Data Subject Access Request.

The request should in the first instance be sent to the College Lead.

Transparency and Privacy Notices

The College will provide detailed, specific information to data subjects. This information will be provided through the College's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices sets out information for data subjects about how the College use their data and the College's privacy notices are tailored to suit the data subject.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the GDPR including the identity of the data protection officer, the College's contact details, how and why we will use, process, disclose, protect and retain personal data.

When personal data is collected indirectly (for example from a third party or publicly available source), we will provide the data subject with the above information as soon as possible after receiving the data. The College will also confirm whether that third party has collected and processed data in accordance with the GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the GDPR

RECORD KEEPING

The College is required to keep full and accurate records of data processing activities. These records include: -

- The name and contact details of the College;

- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the College's processing activities and purposes;
- Details of any third-party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

KEEPING PERSONAL INFORMATION SECURE

The College will use appropriate technical and organisational measures to ensure the security of personal data and has several policies and procedures in place in this regard. We have appropriate security measures in place to prevent personal information from being accidentally lost or used or accessed in an unauthorised way. The College limit access to personal information to those who have a genuine business need to know it. Data processors will do so only in an authorised manner and are subject to a duty of confidentiality.

All team members, Governors and Trustees are made aware of this policy, their duties under data protection law and all will receive the appropriate level of training in relation to the same. The College has procedures in place to deal with any suspected data security breach. We will notify data subjects and any applicable regulator of a suspected data security breach where we are legally required to do so.

Privacy by Design

The College adopts a privacy be design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the College considers the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

To achieve a privacy by design approach, the College conducts DPIAs for any new technologies or programmes being used by the College which could affect the processing of personal data. In any event the College carries out DPIAs when required by the GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data;
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and

- The risk mitigation measures in place and demonstration of compliance.

Audit

The College, through its DPO, regularly tests its data systems and processes in order to assess compliance. These tests are completed through data audits which take place annually in order to review use of personal data. The DPO will also provide an annual report to the College Board of Trustees, reporting activities, advices and recommendations on data protection issues.

Automated processing and automated decision making

The college will not undertake any Automated Processing and Decision making.

Training

The College will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

Direct Marketing

The College is subject to certain rules and privacy laws regarding marketing. For example, a data subject's prior consent would be required for electronic direct marketing (for example, by email, text or automated calls).

The College will not use personal data for direct marketing. The College will promptly respond to any individual queries about direct marketing.

TRANSFER OF DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

The College will not transfer your information out of the UK or outside of the EEA.

DATA INFORMATION RETENTION

The College will retain personal information securely and only for as long is necessary. Please refer to our data retention policy for further information

ANNEX A

DEFINITIONS

Automated Processing

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

Data Subject

An individual about whom such information is stored. It includes but is not limited to employees.

Data Controller

A person or organisation storing and controlling such information. For the purposes of this policy the College is the controller of information.

Data Processor

A person or body, other than an employee of the Data Controller, who processes data on behalf of the Data Controller

Data Protection Impact Assessment (DPIA)

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

Criminal Records Information

This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

Data Protection Officer

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines. The DPO is the first point of contact for individuals whose data the College processes, and for the ICO

ICO

The Information Commissioners Office

Parent

Parent refers to parents, carers and guardians of students in the care of the College.

ANNEX A

Personal data/information

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual (paper) filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Personal Data Breach

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

Processing

Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Special Category Data

Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs and opinions, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

Student

Student refers to any service user of the College, funded through a Local Authority, Social Services or privately.

The College

Project Inc. A company limited by guarantee; company number 10535404. The main site is located at Macclesfield Heritage Centre.

Version Number	
SLT Member Responsible for This Policy	
Board Approval Date	
Date of Next Review	