Cheshire College
South & West

Data Protection Policy

Key Information	
Policy Reference Number	CCSW - DPP
Published on Website	Yes
ELT Post responsible for policy update and monitoring	Chief Financial Officer
Date approved by ELT	23 February 2021
Date approved by committee (if applicable)	09 March 2021
Approved by	Audit and Risk Committee
Date of next review	09 March 2024

1. Introduction

1.1. Cheshire College South & West (the College) needs to process information about its learners and employees. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

1.2. The College and all staff or others who process or use any personal information must ensure that they always comply with Data Protection law.

1.3. To achieve this, the College shall:

- 1.3.1 ensure that personal data is processed lawfully, fairly and in a transparent manner in relation to individuals;
- 1.3.2 specify why the data is being collected and how it will be used *(through a Privacy Statement)*;
- 1.3.3 ensure that personal information is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- 1.3.4 only process personal information where the College has a specific legal basis to do so;
- 1.3.5 ensure that when dealing with the personal data of children the College complies with the law to ensure appropriate processing including appropriate processes for obtaining consent, including compliance with the Age-Appropriate Design Code where relevant;
- 1.3.6 ensure that, where the College asks for consent to use personal data, people are asked to positively opt in, using clear, plain language that is easy to understand;
- 1.3.7 tell individuals they can withdraw their consent at any time, the College shall ensure that individuals can refuse to consent without detriment and avoid making consent a precondition of a service;
- 1.3.8 ensure that all information is adequate, relevant and limited to what is necessary in relation to the purposes for which it is collected;
- 1.3.9 ensure that all information is kept accurate and, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay;
- 1.3.10 implement appropriate record keeping standards and keep information in an identifiable form for no longer than is necessary for the purposes for which the personal data is obtained;
- 1.3.11 Ensure information is protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and operational measures.
- 1.3.12 demonstrate accountability and compliance with these requirements through reports, appropriate documentation, training, spot checks and audits;
- 1.3.13 facilitate the rights of data subjects;
- 1.3.14 ensure that every instance where the College uses a data processor *(a third party with access to process personal data)* there is a written contract in place;
- 1.3.15 ensure that any transfers of personal data outside the UK comply with the law *(in line with the International Transfers of Data Procedure)*;
- 1.3.16 conduct a Data Protection Impact Assessment (DPIA) *(in line with the Data Protection Impact Assessment Policy and Procedure)* where required to do so by law or best practice; and
- 1.3.17 report any data breaches promptly *(in line with the Data Breach Management Procedure)* and inform the Information Commissioners Office (ICO) and data subjects where required.

2. Status of the Policy

2.1 This Policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failures to follow the Policy can therefore result in disciplinary proceedings.

2.2 Any member of staff who considers that the Policy has not been followed in respect of personal data about them, should raise the matter with the Data Protection Officer initially. If the matter is not resolved, it should be raised as a formal grievance.

2.3 Compliance with data protection law is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

3. Roles and Responsibilities

3.1 Overall accountability for data protection sits with the Executive Leadership Team (ELT).

3.2 The ELT will:

- 3.2.1 champion a data protection culture in the organisation;
- 3.2.2 ensure that adequate resources are devoted to meet the College's data protection obligations;
- 3.2.3 commission reports from the Data Protection Officer and take action to remedy deficiencies identified by the report in a timely manner; and
- 3.2.4 ensure the Data Protection Officer operates independently and is not dismissed or penalised for performing their task *(in relation only to their role as Data Protection Officer as defined in law)*;

3.3 Board of Governors

- 3.3.1 The Governors are responsible for holding the ELT to account to ensure compliance with the law.
- 3.3.2 The Data Protection Officer has a direct reporting line to the Governors where they can raise any data protection risks or compliance issues if necessary.

3.4 Operational responsibility for data protection sits with the College's Data Protection Officer

3.5 The Data Protection Officer will:

- 3.5.1 inform and advise all members of staff on their data protection obligations;
- 3.5.2 monitor compliance with data protection requirements;
- 3.5.3 contribute to the development and maintenance of all data protection policies, procedures and processes in relation to the protection of personal data;
- 3.5.4 advise and inform the College on any data protection impact assessment (DPIA), including monitoring performance of DPIAs;
- 3.5.5 report and advise ELT on the allocation of their responsibilities to support ongoing compliance Data Protection law;
- 3.5.6 provide data protection training and awareness to all members of staff;
- 3.5.7 conduct audits of processes relating to personal data;
- 3.5.8 be the point of contact for data subjects about the processing of their personal data and respond to all data subject access request;
- 3.5.9 advise senior management on the allocation of information security responsibilities;
- 3.5.10 develop/advise on formal procedures for reporting incidents and investigations;
- 3.5.11 contribute to the risk management, business continuity and disaster recovery planning process;
- 3.5.12 advise on and monitor organisational record management and retention arrangements;
- 3.5.13 ensure that records of the processing are kept and the College Notifies the ICO;
- 3.5.14 advise on the issuing of privacy notices to data subjects at the point of collection of their personal data;
- 3.5.15 be the first point of contact for any enquiries from the Information Commissioners Office *(and any EU supervisory authorities, where relevant)*;

3.6 All staff also have responsibility for data protection. All staff must:

- 3.6.1 ensure any personal data which they hold is kept securely;
- 3.6.2 ensure personal information is not disclosed either orally or in writing, accidentally or otherwise unlawfully to any unauthorised party;
- 3.6.3 only access personal data that is applicable and required for them to undertake their role;
- 3.6.4 report a data breach immediately when any data breach occurs;
- 3.6.5 undertake all required data protection/cyber security training;
- 3.6.6 always maintain data protection awareness reporting any data protection risks or concerns to their

Line Manager or the Data Protection Officer;

3.6.7 ensure that records are accurate, kept up to date kept securely and disposed of safely in accordance with the timescales set out in this and other relevant record keeping procedures;

3.6.8 only send marketing information if they have approval from the Marketing Department and Data Protection Officer;

3.6.9 not process Special Categories of data or Criminal offence data without first ensuring they have a legal basis to do so and recording this processing with the Data Protection Officer;

3.6.10 ensure they have an appropriate contract in place *(approved by the Data Protection Officer)* with any third-party organisation that will have access to personal data;

3.6.11 where staff are required to sending personal data to another country or international organisations, they must seek advice from the Data Protection Officer;

3.6.12 check that any information that they provide to the College in connection with their employment is accurate and up to date and inform the College of any changes to information which they have provided, e.g., change of address or name;

3.6.13 follow all guidance relating to information sharing; and

3.6.14 comply with the College Data Protection Requirements set out as follows.

4. Data Protection Requirements

4.1 Physical Security:

4.1.1 staff must always wear their ID badge;

4.1.2 staff must never allow others to use their swipe cards or pin numbers to gain entry;

4.1.3 staff must not allow others to 'tailgate' e.g., follow a staff member through secure areas;

4.1.4 staff must report to security personnel if they encounter unescorted visitors or anyone not wearing appropriate visible identification, *(i.e., an ID badge)*; and

4.1.5 boards displaying person identifiable data should be sited in areas not accessible to learners or the public.

4.2 Paper Records:

4.2.1 all paper and files containing data subject details to be securely locked away when not in use a clear desk policy should be adopted; and

4.2.2 data that is no longer required must be disposed of securely. The College uses a secure shredding company to dispose of data securely.

4.3 Working Remotely/Offsite:

4.3.1 physical records must only be taken off-site where absolutely necessary;

4.3.2 only take the minimum necessary personal information off site;

4.3.3 ensure that staff members have a secure place to protect manual information;

4.3.4 never leave personal information in an unsecure area in the home, i.e., in garages, sheds, boots of cars, near open doors or windows;

4.3.5 never work on personal information in a public place where it could be seen by a third party; and

4.3.6 prevent access to information by other members of the household and by visitors. Staff members working at home should ensure they adopt a clear desk policy when leaving their work unattended.

4.4 Transporting Paper Records:

4.4.1 keep information in a sealed container/bag;

4.4.2 public transport should not be used for transporting personal information, if an exception to this rule is identified the information must be transported in a locked briefcase or similar;

4.4.3 never leave information unattended in the car for an extended length of time; and

4.4.4 never leave information in the boot of a car overnight. Information must be taken inside a property and secured.

4.5 Moving Offices/Relocation of Working Area:

4.5.1 all records should be either: transferred to a secure area for continued storage in the new location, archived or destroyed in line with the College Retention Schedule;

4.5.2 all filing/storage cabinets should be transferred to the new office, or those remaining for removal or disposal must be checked to ensure they are empty of all paperwork and IT devices;

4.5.3 all desk draws should be opened and the desks inspected to ensure they are empty of all paperwork and IT devices;

4.5.4 all rooms including cupboards, kitchens and other storage spaces must be checked to ensure they are empty of all paperwork or IT devices;

4.5.5 all confidential waste must be shredded or placed in clearly marked confidential waste collection bins/bags and a collect must be arranged; and

4.5.6 all IT equipment including laptops, desktops, DVDs, floppy disks, memory sticks etc. has been transferred to the new work area or returned to IT for secure disposal.

4.6 Post:

4.6.1 all external post should be delivered to the Post Room which must be locked when not staffed;

4.6.2 sensitive information should be posted using tracked services;

4.6.3 post should not be left in unsupervised areas that are open to learners or the general public; and

4.6.4 post containing personal or confidential information should be sent in sealed envelopes.

4.7 IT Security:

4.7.1 screens of computers must always be locked when left unattended;

4.7.2 if electronic data is stored on removable media, these must be encrypted and kept locked away securely when not in use; and

4.7.3 electronic data should only be stored on the College's designated drives and servers and should only be uploaded to an approved cloud computing services that the College has a contract with *(e.g., do not use Dropbox, Google Drive etc.)*.

4.8 Email:

4.8.1 staff should always consider if email is the best communication method;

4.8.2 staff should always consider whether the e-mail going to just one person. If so, is it the correct person where similar names exist in the e-mail directory or address book;

4.8.3 staff should always consider whether to use the 'reply all' function. If so, does every person on the list need to receive the reply and any attachment;

4.8.4 staff should carefully check the recipients of all e-mails prior to sending regardless of content. Staff members should be extra vigilant where personal, sensitive personal or confidential information is included;

4.8.5 always delete emails which they have reached their retention period;

4.8.6 only send email from another member of staff's email account or under an assumed name if they have the specific authority. This is generally reserved for the Executive Leadership Team.

4.8.7 manage email appropriately, clearing the deleted items folder and using appropriate archiving facilities; and

4.8.8 use password protect the content of any email when sending sensitive/confidential/special categories of data.

4.9 Telephone:

4.9.1 staff should generally not give any information about a learner, not even confirmation that an individual is a learner at the College, in response to any telephone enquiry, even if the query is from the parents unless they have taken steps to verify the caller such as asking for specific information, such as learner date of birth, course attending etc;

4.9.2 wherever possible it is recommended that staff:

4.9.2.1 take the name and telephone number of the person calling;

4.9.2.2 ask the nature of the enquiry;

4.9.2.3 tell the caller that you will pass on the enquiry or telephone them back;

4.9.2.4 seek advice from their line manager or the Data Protection Officer; and

4.9.2.5 enquiries about a learner's progress or attendance should be passed on to the Personal Development Tutor (PDT).

4.10 Marketing:

4.10.1 there are specific rules around sending advertising or marketing material which is directed to specific individuals. Routine service messages do not count as direct marketing, such as correspondence to provide information they need about the College *(e.g., information about College closures due to bad weather, safety announcements, changes to term dates etc.)*. General branding, logos or straplines in these messages do not count as marketing;

4.10.2 when sending specific marketing messages, staff should have obtained consent to send any emails, texts, picture messages, video messages, voicemails, direct messages via social media or any similar electronic messages; and

4.10.3 all uses personal data to directly target individuals for marketing purposes should be reviewed with the Data Protection Officer.

4.11 Retention:

4.11.1 the College must ensure that personal data is kept no longer than is necessary;

4.11.2 records which have reached the end of their life *(whether held in electronic or paper format)* should generally be destroyed under confidential conditions. Once a document reaches its retention period it should be reviewed to ensure it does not need to be kept for longer as some records need to be kept for historical purposes and these will be transferred to a place of deposit by the Data Protection Officer. Any staff wishing to retain a record for longer than the specified retention period should contact the Data Protection Officer for advice and guidance;

4.11.3 a Document Retention Procedure has been produced and staff must review this policy and ensure records are kept in line with the timescales specified. Staff must ensure that once data has reached its retention period it is destroyed securely. All personal data held in paper form must be disposed of by shredding or in the shred bins provided on College premises; and

4.11.4 electronic media will be disposed of securely by the Network Services.

5. Disclosing/Sharing Personal Data

5.1 Data Sharing General Principles

5.1.1 personal data must generally not be disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party; and

5.1.2 the College must ensure that individuals are informed if their data is to be shared with another organisation. Where sharing is to take place on a regular basis a data sharing agreement may be required. Data sharing agreements can be obtained from the Data Protection Officer.

5.2 Parents/Guardians/Carers

5.2.1 learners are advised that it is College policy that staff may contact named parents/guardians of learners under the age of 18 at the start of the course to discuss academic progress, attendance and conduct. Learners who do not wish the College to make such contact may be granted an exemption by writing to the Principal at the commencement of their course;

5.2.2 learner Administration will provide a list of such learners which will be circulated to faculty managers and appropriate College Team Leaders. If the learner has requested that the College does NOT contact their parents/guardians, then no information can be given;

5.2.3 the learner will have indicated on the enrolment form the name of the parent/guardian with whom contact can be made. Learners can change these details on the system; and

5.2.4 enquiries can be dealt with, generally by the Personal Development Tutor (PDT), but only with the person given by the learner using the contact details on the learner record.

5.3 Other Family Members, Friends etc

5.3.1 staff should not respond to any enquiries from other family members or friends and should not even confirm that someone is a learner at the College. If the reason for the enquiry is stated to be an emergency, then the matter should be referred to the duty manager/member of the Senior leadership Team (SLT).

5.4 Potential Employers and Education Institutions *(Reference Requests)*

5.4.1 these should be dealt with by the Personal Development Tutor (PDT). All reference requests and responses should be in writing. The learner is entitled to see copies of any reference written about them. Copies of all references should be kept in the learner file.

5.5 Government Agencies

5.5.1 government agencies can include, but not be limited to, Social Services, Police, Benefits agencies, probation service, tax etc;

5.5.2 the College is legally bound to provide information to various government agencies. All requests for information and all responses should be in writing. Copies of all requests should be kept, preferably in the learner file; and

5.5.3 staff should seek advice from the Data Protection Officer when responding to any such requests.

5.6 Data Controllers

5.6.1 a data controller is a third party which the College shares to process personal data and the third-party choses how to use this data; and

5.6.2 a list of Data Controllers will be maintained by the Legal Advisor / Data Protection Officer.

> *For Example:*
>
> *Where a learner is undertaking a work experience placement details about the learner are provided to the employer. The employer is themselves a Data Controller and is responsible for how it handles this information and must do so in line with data protection law.*

5.7 Data Processors

5.7.1 a data processor is a third party which the College uses to process personal data. In every case where the College uses a data processor it will ensure it has a written contract in place. The contract is important so that both parties understand their responsibilities and liabilities. A list of contracts will be maintained by the Legal Advisor/Data Protection Officer.

5.7.2 the contract must include the following:

5.7.2.1 subject matter and duration of the processing;

5.7.2.2 nature and purpose of the processing;

5.7.2.3 type of personal data and categories of data subject; and

5.7.2.4 obligations and rights of the controller.

5.7.3 the contract will require that the processor must:

5.7.3.1 only act on the written instructions of the organisation (unless required by law to act without such instructions).

5.7.3.2 ensure that people processing the data are subject to a duty of confidence.

5.7.3.3 take appropriate measures to ensure the security of processing.

5.7.3.4 only engage a sub-processor with the prior consent of the data Society and a written contract.

5.7.3.5 assist the organisation in providing subject access and allowing data subjects to exercise their rights.

5.7.3.6 assist the organisation in meeting its obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments.

5.7.3.7 delete or return all personal data to the organisation as requested at the end of the contract.

5.7.3.8 submit to audits and inspections, provide the organisation with whatever information it needs to ensure that they are both meeting their data protection obligations and tell the organisation immediately if it is asked to do something infringing the law.

6. Key Definitions

Term	Definition
Personal Data	'Personal data' means any information relating to an identifiable person *('data subject')*; an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Special Categories of Personal Data	'Special categories of personal data' are racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation. *Note: This was previously referred to as Sensitive Personal data.*
Data Protection Principals	Data Protection law sets out seven key principles: • lawfulness, fairness and transparency; • purpose limitation; • data minimisation; • accuracy; • storage limitation; • integrity and confidentiality *(security)*; and • accountability.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Controller	'Controller' any person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
UK Data Protection Law	Refers to the applicable laws of the land including the UK Data Protection Act 2018 and the UK General Data Protection Regulations.
EU Data Protection Law	Refers to the EU General Data Protection Regulations which may be applicable to the College in the event that we process personal data of data subjects who are in the European union

(Table 1: Key Definitions)