

Data Protection GDPR Policy

Cultural Capital is committed to a policy of protecting the rights and privacy of individuals, including learners, staff and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

The new regulatory environment demands higher transparency and accountability in how organisations manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

The GDPR contains provisions that The company will need to be aware of as data controllers, including provisions intended to enhance the protection of student's personal data. For example, the GDPR requires that:

We must ensure that our company privacy notices are written in a clear, plain way that staff and students will understand.

The company needs to process certain information about its staff, students, parents and guardians and other individuals with whom it has a relationship for various purposes such as, but not limited to:

- The recruitment and payment of staff.
- The administration of programmes of study and courses.
- Student enrolment.
- Examinations and external accreditation.
- Recording student progress, attendance and conduct.
- Collecting fees.
- Complying with legal obligations to funding bodies and government including local government.

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) The company must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Compliance

This policy applies to all staff and students of The company. Any breach of this policy or of the Regulation itself will be considered an offence and the Company's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with The company and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

The Code of Practice on GDPR for The company gives further detailed guidance and The company undertakes to adopt and comply with this Code of Practice.

General Data Protection Regulation (GDPR)

This piece of legislation comes in to force on the 25th May 2018. The GDPR regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

The GDPR also sets out specific rights for students in relation to educational records held within the state education system. These rights are set out in separate education regulations 'The Education (Pupil Information) (England) Regulations 2000'. For more detailed information on these Regulations see the Data Protection Data Sharing Code of Practice (DPCoP) from the Information Commissioner's Office (ICO). Please follow this link to the ICO's website (www.ico.gov.uk)

Responsibilities under the GDPR

The company will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data. The company appoints a Data Protection Officer (DPO), currently the Executive Manager who is available to address any concerns regarding the data held by the company and how it is processed, held and used. The company also has a nominated governor who oversees this policy.

The Senior Leadership Team is responsible for all day-to-day data protection matters, and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within The company.

The Senior Leadership Team is also responsible for ensuring that the company's notification is kept accurate. Details of The company's notification can be found on the Office of the Information Commissioner's website. Our data Registration Number is ZA475679

Compliance with the legislation is the personal responsibility of all members of The company who process personal information. Individuals who provide personal data to The company are responsible for ensuring that the information is accurate and up-to-date.

Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. More detailed guidance on how to comply with these principles can be found in the DPCoP. Please follow this link to the ICO's website (www.ico.gov.uk)

In order to comply with its obligations, The company undertakes to adhere to the eight principles:

1 Process personal data fairly and lawfully.

The company will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant. For example,

2 Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.

The company will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3 Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

The company will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

4 Keep personal data accurate and, where necessary, up to date.

The company will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify The company if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of The company to ensure that any notification regarding the change is noted and acted on.

5 Only keep personal data for as long as is necessary.

The company undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means The company will undertake a regular review of the information held and implement a weeding process.

THE COMPANY will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

6 Process personal data in accordance with the rights of the data subject under the legislation.

Individuals have various rights under the legislation including a right to:

- be told the nature of the information The company holds and any parties to whom this may be disclosed.
- prevent processing likely to cause damage or distress.
- prevent processing for purposes of direct marketing.
- be informed about the mechanics of any automated decision taking process that will significantly affect them.
- not have significant decisions that will affect them taken solely by automated process.
- sue for compensation if they suffer damage by any contravention of the legislation.

- take action to rectify, block, erase or destroy inaccurate data.
- request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

The company will only process personal data in accordance with individuals' rights.

7 Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

The company will ensure that all personal data is accessible only to those who have a valid reason for using it.

The company will have in place appropriate security measures e.g.

- ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):
- keeping all personal data in a lockable cabinet with key-controlled access.
- password protecting personal data held electronically.
- archiving personal data which are then kept securely (lockable cabinet).
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.
- ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, The company will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed.

This policy also applies to staff and students who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data.

8 Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The company will not transfer data to such territories without the explicit consent of the individual.

This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - so The company will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If The company collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

Consent as a basis for processing

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when THE COMPANY is processing any sensitive data, as defined by the legislation.

The company understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via the enrolment form) whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

“Personal Details

For the purposes of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) you consent to the The company holding and processing personal data including sensitive personal data of which you are the subject, details of which are specified in The company's data protection policy.

This will include marketing images and The company CCTV.

The company will ensure that any forms used to gather data on an individual will contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.

THE COMPANY will include the specified statement from the DfE on the student enrolment form and update when required following the ESFA's technical guidance:

How We Use Your Personal Information

This privacy notice is issued by the Education and Skills Funding Agency (ESFA), on behalf of the Secretary of State for the Department of Education (DfE). It is to inform learners how their personal information will be used by the DfE, the ESFA (an executive agency of the DfE) and any successor bodies to these organisations. For the purposes of the Data Protection Act 1998, the DfE is the data controller for personal data processed by the ESFA. Your personal information is used by the DfE to exercise its functions and to meet its statutory responsibilities, including under the Apprenticeships, Skills, Children and Learning Act 2009 and to create and maintain a unique learner number (ULN) and a personal learning record (PLR).

Your information may be shared with third parties for education, training, employment and well-being related purposes, including for research. This will only take place where the law allows it and the sharing is in compliance with the Data Protection Act 1998.

The English European Social Fund (ESF) Managing Authority (or agents acting on its behalf) may contact you in order for them to carry out research and evaluation to inform the effectiveness of training.

You can opt out of contact for other purposes by ticking any of the following boxes if you do not wish to be contacted:

About courses or learning opportunities. For surveys and research.

By post. By phone. By email.

Further information about use of and access to your personal data, and details of organisations with whom we regularly share data are available at: <https://www.gov.uk/government/publications/esfa-privacy-notice>

The company will ensure that if the individual does not give his/her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them which are held by The company. Any individual wishing to exercise this right should apply in writing to the Executive Manager. Any member of staff receiving a SAR should forward this to the Executive Manager.

The company reserves the right to charge a fee for data subject access requests (currently £20).

Under the terms of the legislation, any such requests must be complied with within 40 days.

For detailed guidance on responding to SARs, see the CoP.

Disclosure of Data

Only disclosures which have been notified under The company's DP notification must be made and therefore staff and students should exercise caution when asked to disclose personal data held on another individual or third party.

The company undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and in some circumstances, the police.

Legitimate disclosures may occur in the following instances:

- The individual has given their consent to the disclosure.
- The disclosure has been notified to the OIC and is in the legitimate interests of The company.
- The disclosure is required for the performance of a contract.

There are other instances when the legislation permits disclosure without the consent of the individual.

For detailed guidance on disclosures see the Code of Practice (Cop).

In no circumstances will The company sell any of its databases to a third party.

Publication of company Information

The company publishes various items which will include some personal data, e.g.

- internal telephone directory.
- event information.
- photos and information in marketing materials.

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential or restricted access only. Therefore it is The company policy to offer an opportunity to opt-out of the publication of such when collecting the information.

Email

It is the policy of The company to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information Legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on The company's email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from The company may be accessed by someone other than the recipient for system management and security purposes.

CCTV

There are some CCTV systems operating within The company for the purpose of protecting staff, students and property. The company will only process personal data obtained by the CCTV system in a manner which ensures compliance with the legislation.

Procedure for review

This document is subject to a scheduled annual review. This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.