DCC Interactive Limited (DCC-i) - Data Protection and Confidentiality Policy

Date Ratified	20/12/2023
Signed by	Daisy Long / Chloe Whittall
Next Review	January 2025 or as required by law/change of business model
Version No	4

Contents

Purpose of Policy

This Policy relates to the activity of DCC Interactive Limited (Company No: 13075266), known as DCC-i. Any GDPR or Data Protection claim, complaint or concern against the company when it was previously known as Daisy Bogg Consultancy Ltd - (Company No: 7300621) will be dealt with under the version 1 of this policy which has been archived but remains available if required.

The purpose of this combined Data Protection and Confidentiality Policy is to ensure that all services provided DCC-i regarding the storing, processing and sharing of data is clear and adheres to both legislation and best practice guidelines. This policy is an integral part of ensuring that DCC-i provides a safe environment where individuals are treated with respect.

DCC-i has a separate GDPR/Data Protection Policy in relation to DCC-I Employees which can be found in the DCC-I Staff Handbook. This Policy relates to our customers and any other 3rd parties.

The main reasons for producing a policy are:

- to comply with legislation;
- to provide practical guidelines;
- to protect people providing and using DCCi services;

Legal Context of Policy

- The Human Rights Act 1998 guarantees respect for a person's private and family life, home and correspondence.
- The Data Protection Act 2018 (DPA) concerns personal information, which includes facts and opinions about an individual which might identify them.
- Other UK legislation may at specific times over-ride the Human Rights Act and the UK General Data Protection Regulations, Eg suspected terrorist activity or in relation to specific safeguarding concerns; DCC-i will always ensure that the appropriate legislative framework is followed for the specific situation.

- The Privacy and Electronic Communications Regulations 2003 – updated 2016 (PECR) provide the legislative framework in relation to all electronic Direct Marketing.
- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 which enshrines the European General Data Protection Regulations 2018 (GDPR) following the UK exit from the EU on 31/12/2020 –The principles and requirements of these regulations (UK GDPR) provides the basis for this policy.
- At the current time DCC-i does not have any Overseas Customers other than the Isle of Man. The Isle of Man is covered for the purposes of Information Sharing by an 'Adequacy Agreement' between the UK and IOM that confirms that any organisation complying with its respective legislation is operating at a standard high enough to protect the sharing of data between the UK and IOM. This policy will be reviewed if DCC-i expands its customer base to include any customers outside the UK and IOM.
- The Directors of DCC-i are legally responsible for ensuring all the activities of DCC-i are compliant with this policy. The named Director is Chloe Whittall. All DCC-i staff and associates are individually responsible for complying with the law and are expected to read this policy as part of their induction to DCC-i and on each occasion that it is updated. This instruction will be given by email or recorded in Team Meeting notes and compliance will be checked via the Supervision Policy.

Statement on Confidentiality

Information shared in Confidence:

DCC-i offers confidentiality in respect to sensitive information shared with any member of DCC-i Staff. Confidential information will not be passed on except in circumstances where this is explicitly agreed as part of a contract, it is necessary to protect a vulnerable person or property from immediate danger or harm, comply with professional registration requirements (Eg Social Work England) or to comply with the law (EG: As required by the Counter Terrorism & Security Act 2015 or The Counter-Terrorism and Border Security Act 2019).

In such circumstances, the information will only be passed on with the permission of a Director of DCC-i or a senior member of staff with delegated authority. Wherever possible and appropriate, any person whose information has been shared, will be informed that this action has been taken.

Personal Data:

Personal Data is information entrusted by an individual in confidence, where there is a general obligation not to disclose or use that information without a clear legal basis.
Confidential information may include any attributable information such as name, age, address, contact details or electronic identifiers; as well as sensitive personal information such as protected characteristics under the Equalities Act 2010, health or criminal records. This includes information known or stored in any format, including photographs, videos and all electronic communications. For the purposes of this policy the GDPR 2018 definitions of Personal Data, Special Category Data and Criminal Offence Data and adopted by the UK GDPR Regulations 2019 are adhered to by DCC-i.

Information that identifies individuals personally is assumed to be confidential and will only be used when necessary and for the intended purpose for which it has been shared. The information will be stored and processed in line with legislation and best practice guidance as set out in this policy.

All individuals and companies providing DCC-i with personal data will be given clear information on how their information will be used, processed and stored, and if, how and when information will be archived or deleted.

Where consent is the legal basis for use of data, information will also be provided regarding how to withdraw consent and rights to erasure. This information will be provided by means of a clear privacy notice as set out in this policy.

Whenever possible, anonymised data—from which personal details have been removed and which therefore cannot identify the individual, will be used; this will also only be used for justified purposes.

Compliance with Data Protection Regulations.

ICO Code of Practice:

The Information Commissioners Office issued a new Code of Practice in December 2020 which is a statutory code of practice made under section 121 of the Data Protection Act 2018. DCC-i will comply with the Code as set out on the ICO Website (Summary | ICO).

In compliance with the Code of Practice we will:

- Be responsible for our compliance and be able to demonstrate it.
- Share personal data fairly and transparently.
- Identify at least one lawful basis for sharing data before sharing starts.
- Process personal data securely, with appropriate measures in place.
- Have policies and procedures that allow data subjects to exercise their rights.
- Share data in an emergency if it is necessary and proportionate.
- Only share children's data if there is a compelling reason, taking account of the best interests of the child.
- Follow the framework for the sharing of personal data, for defined purposes across the public sector, under the Digital Economy Act 2017 (DEA).

UK GDPR:

For the purposes of this policy, the GDPR 2018 Principles adopted by the UK GDPR Regulations 2019 (The principles | ICO) are adhered to by DCC-I in respect to the collection, storage, processing and sharing of all data.

Principles:

All information will be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals.

b) 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 shall not be considered to be incompatible with the initial purposes.

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 UK GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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.

Legal Basis:

Prior to obtaining any Personal Data, DCC-i will ensure that we are clear under which legal basis the information is being obtained and processed, this will be made clear to the individual and/or company providing the data.

The six available bases are:

- Consent
- Contract
- Legal Obligation
- Vital Interests
- Public Task
- Legitimate Interests

Rights:

DCC-i will ensure that all individuals and companies providing data to DCC-i are aware of their rights as set out in the UK GDPR.

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure (where applicable).
- The right to restrict processing.
- The right to data portability (for automated data).
- The right to object.
- Rights in relation to automated decision making and profiling (If carried out).

Means for Achieving Compliance with UK GDPR

DCC-i achieves compliance with GDPR by:

1. *Policy:* Ensuring this policy remains compliant and is reviewed annually, or more frequently if changes to data protection legislation occur. The current review period for this policy is 12 months.

2. *ICO Registration:* Ensuring DCC-i maintains up-to-date registration with the Information Commissioners Office and that this information is readily available to all DCCi Customers. The current reference number for DCC-i ICO Registration is ZA839281, DCC-I was first Registered on the 3rd January 2021 and the current registration is Valid until 2nd January 2024.

3. *Data Protection Officer:* Ensuring DCC-i has a Data Protection Officer (DPO) to deal with all queries in relation to Data Protection. The current DPO is Chloe Whittall –Director for People and Practice.

4. *Responses to Data Breach:* Any Data Breach identified by any member of staff will be immediately reported to the Data Protection Officer (DPO) who is available by mobile and email out of hours in emergency situations. When the DPO is on leave or unavailable, another senior member of staff will assume this role.

   All possible remedial action to secure the data or reduce the impact of its loss will be undertaken at the earliest possible time. Information breaches will be reported to the ICO in line with ICO Procedures within 72 hours, and a full investigation will be launched.

   Any parties whose data has been affected will be appropriately informed of the data breach and all actions to reduce the impact of the data loss will be taken. All parties will be informed of their right to complain and inform the ICO or other relevant authority. Where the data subject lacks the capacity to understand the implications of a data breach in respect of their data, the commissioning body will be notified. The commissioning body can act on behalf of the data subject and pursue a complaint if they assess this to be in the best interest of the individual.

   An investigation of learning points will be undertaken, and actions implemented following the completion to ensure the likelihood of any further data breaches is reduced.

5. *Information Storage:* Ensuring that all information stored electronically is protected by the use of a secure cloud-base system, encryption where appropriate, and a robust IT Policy for all staff to follow to maintain system security.

   DCC-i does not routinely store sensitive data in hard copy. On the rare occasions this is necessary, the staff member will agree with their line manager a suitable confidential storage arrangement that is secure. On the rare occasions that information is in transit, it is the responsibility of the DCC-i staff member or associate transporting it. Information will be kept secure and minimal personal data will be transported to reduce the likelihood of data loss. Staff can be provided with a lockable box for any required storage and/or transportation.

6. *Provision of Privacy Notice*: Providing a Privacy Notice to all DCC-i Customers that covers all the routine DCC-i Business Areas (See Relevant Section of this Policy) and the key principles. The DCC-i Privacy Notice also contains details of the emergency circumstances under which the organisation would use the 'Vital Interests' basis for using and sharing personal data.

7. *Audits:* Undertaking an annual review of the DCC-i UK GDPR compliance.

8. *Routine Deletion of Information:* Undertaking routine deletion of information that is no longer required (See Relevant Section of this Policy).

9. *Data Protection Impact Assessments:* Undertaking DPIA's on all time-bound DCC-i Projects as part of the Project Initiation Documentation for each Project and ensuring Data processing is discussed and agreed with the commissioning organisation as part of the contract. DCC-i will require commissioning Organisations to be GDPR compliant when providing contact details for DCC-i to undertake research and evaluation functions, which is shared in order for DCC-i to deliver against a contract.

10. *Legitimate interests' assessments:* undertaking and recording LIA's for all business areas where 'Legitimate Interests' is the legal basis for using, retaining and processing data. This will be recorded in the DCC-i GDPR Information Audit Spreadsheet, which will be reviewed annually.

11. *Staff Compliance:* Ensuring all DCC-i staff are able to clearly identify any data collected which meets the GDPR Special Category Data / Criminal Offence Data. Staff identifying the collection of Special Category Data / Criminal Offence Data will report this to the Data Protection Officer who will undertake a DPIA or LIA and ensure the appropriate consents and safeguards are in place for the data collection. All staff are required to undertake initial training in respect of this policy and confirm their understanding – staff will undertake an annual internal refresher.

All associates must confirm that they have read, understood and will comply with this policy. Training will be provided to associates on request if required, this training will specifically relate to GDPR requirements for the work they undertake for DCC-i.

12. *Right to Access Request Response Procedures:* DCC-i operates a clear system for responding to **'right to access'** requests within 1 month, unless grounds for extension or refusal applies – All DCC-i staff are able to recognise a request for access made verbally, by electronic means or in writing. The staff member receiving the request will record the request within 24 hours and report it to the Data Protection Officer within 3 working days.
The request will be reviewed and evaluated within 10 working days. The request will be responded to within 1 month, if retrieving the data requires additional time due to the volume or complexity of the data, the applicant will be informed of the need for an extension, which will not exceed 2 months.

The information will be provided in a clear and accessible format. If the applicants right to access is being refused, the Data Protection Officer will inform the applicant of the reason for this and ensure they are aware of their right to complain to the ICO, other relevant supervisory body or to seek judicial remedy.

13. *Right to Rectify Request Response Procedures*: DCC-i operates a clear system for responding to requests to **rectify information** within 1 month, unless grounds for extension or refusal applies - All DCC-i staff are able to recognise a request for rectification made verbally, by electronic means or in writing. The staff member receiving the request will record the request within 24 hours and report it to the Data Protection Officer within 3 working days.
No further processing of the information will take place whilst the request is evaluated.
The request will be reviewed and evaluated within 10 working days. If it is assessed that the information is incorrect and does need to be rectified, remedial action will be undertaken within 1 month and the applicant informed of the action taken. If rectifying the information is a lengthy or complex process, the applicant will be informed of the need for an extension, which will not exceed 2 months.

The information will be provided in a clear and accessible format. If the applicants request to rectification is being refused, the Data Protection Officer will inform the applicant of the reason for this, and ensure they are aware of their right to complain to the ICO, other relevant supervisory body or to seek judicial remedy.

14. *Request to restrict or object request response procedures:* DCC-i operates a clear system for responding to requests to **restrict or object to the processing of information** within 1 month, unless grounds for extension or refusal applies - All DCC-i staff are able to recognise a request for restriction or objection made verbally, by electronic means or in writing.

The staff member receiving the request will record the request within 24 hours and report it to the Data Protection Officer within 3 working days. No further processing of the information will take place whilst the request is evaluated.

The request will be reviewed and evaluated within 10 working days. If it is assessed that the information should be restricted, or the objection is valid, remedial action will be undertaken within 1 month and the applicant informed of the action taken. If the remedial action is a lengthy or complex process, the applicant will be informed of the need for an extension which will not exceed 2 months.

The information will be provided in a clear and accessible format.

If the applicants request to restrict or object to the processing of data is refused, the Data Protection Officer will inform the applicant of the reason for this and ensure they are aware of their right to complain to the ICO, other relevant supervisory body or to seek judicial remedy. The information will be archived or deleted in line with DCC-i Retention and Deletion Procedures (See Relevant Section of this Policy)

If the objection relates to an individual or company information being utilised for Marketing Process, this right will be respected unequivocally, and the information will no longer be used for Marketing.

15. *Request to erase request response procedures:* DCC-i operates a clear system for responding to requests to **erase information** within 1 month, unless grounds for extension or refusal applies - All DCC-i staff are able to recognise a request for data erasure made verbally, by electronic means or in writing. The staff receiving the request will record the request within 24 hours and report it to the Data Protection Officer within 3 working days. No further processing of the information will take place whilst the request is evaluated.
The request will be reviewed and evaluated within 10 working days. If it is assessed that the request for erasure is valid, this action will be taken in line with the DCC-i erasure and retention policy. The request will be responded to within one month and the applicant will be informed within what timeframe the data can be erased, if necessary, the information will be archived and scheduled for deletion at the earliest appropriate opportunity. (See Relevant Section of this Policy).

The information will be provided in a clear and accessible format. If the applicants request to restrict or object to erase data is refused, the Data Protection Officer will inform the applicant of the reason for this and ensure they are aware of their right to complain to the ICO, other relevant supervisory body or to seek judicial remedy.

If the erasure request relates to the individual or company information being erased from Marketing lists, this right will be respected unequivocally, a record of the request will be maintained for suppression purposes, i.e. to ensure further marketing requests are not sent. The information will be deleted in line with DCC-i Deletion Procedures.

16. *Opt-Out of Marketing Request Response Procedures:* DCC-i Customers will all be informed of their right to withdraw consent/object to Direct Marketing in each communication, any requests to opt-out of Marketing will be acted on promptly.

17. *Automated Data Sharing Procedures:* At the current time DCC-i does not use automated processing methods, therefore there are not specific procedures for portability, automated decision-making and profiling contained within this policy, should this change the UK GDPR guidance will be adhered to and the policy refreshed.

18. *Procedures of responding to GDPR breaches by other organisations:* If DCC-I become aware of a GDPR breach by a customer, the member of staff will inform the DPO immediately and the DPO or the appropriate member of staff will immediately inform the customer of the breach and delete the information sent in error from all elements of our system.

Privacy Notices

DCC-i will provide a Privacy Notice for all main areas of the business, the Privacy Notice will contain the underpinning principles for all data processing. The Privacy Notice will be publicly available on the DCC-i Website.

The Privacy Notice will be included in the DCC-i Terms and Conditions for new customers. The Privacy Notice will include specific named business functions where there is a data processing function, in particular how data provided for delivering training is used. Salient points on the Privacy Notice will be included in DCC-i email communications, particularly in relation to Marketing, which will notify customers of their right to object.

What we provide:

- The name and contact details of our organisation.
- The contact details of our data protection officer.
- The purposes of the processing.
- The lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if the data is obtained from 3rd party).
- The recipients or categories of recipients of the personal data.
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the data is obtained from 3rd party).

- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).

The majority of the information received or shared for the purposes of training and consultancy services is obtained and shared under the legal basis of 'legitimate interest' and the majority of the information received or shared for Independent Social Work Commissions is under the basis of 'legal basis or public task' *and therefore consent is not required and opportunities for the data subject to apply for restriction or erasure will be limited*; however we will ensure all data subjects are aware of the information held and how it will be used and/or shared.

Where the data subject lacks capacity in relation to understanding the implications of the privacy notice in respect of how their personal data will be stored, used or shared, the privacy notice will be made available to the organisation responsible for commissioning the service in order that they can raise any concerns or respond to any data breaches on behalf of the data subject if they assess this to be in the individuals Best Interest.

As an organisation which provides virtual training, it is a regular occurrence that our delegates are accessing the training from their home rather than their place of work. On rare occasions it can be the case that a DCC-i trainer becomes aware of an emergency situation where there is an immediate risk to life for the delegate (accident, medical emergency, harm from another person). In order to respond to this eventuality, all customers are asked to provide DCC-i with the contact details for a person or department that can provide an individual's home address in order for it to be passed onto the emergency services.

If time and circumstances allow, the information can be passed on directly by the customer, however where there is a live call in progress to an emergency call handler, the customer is asked to provide the delegates details to DCC-i to communicate. This circumstance is covered by the legal basis for sharing information defined as 'Vital Interests' which permits any relevant party to share information that is necessary to protect someone's life.

DCC-I also requests essential information directly from delegates via an MS TEAMS Form for responding to emergency situations, this information is provided under the legal basis of 'Consent' and would be shared under the legal basis of 'Vital Interests'. Further information can be found in our 'Emergency Procedures Protocol' which is on our website. This information is deleted at the end of each working day.

When we provide it

- We provide individuals with privacy information at the time we collect their personal data from them.

- If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information:
    - Within a reasonable of period of obtaining the personal data and no later than one month;
    - If we plan to communicate with the individual, at the latest, when the first communication takes place;
    - Or if we plan to disclose the data to someone else, at the latest, when the data is disclosed.

How we provide it

We provide the information in a way that is:

- Concise.
- Transparent.
- Intelligible.
- Easily accessible.

Use, Retention, Archiving and Deletion of Information

DCC-i understands the requirement not to retain personal information longer than is necessary and operates procedures to comply with this, whilst still ensuring that data is available for legitimate interests, legal requirements and contractual purposes.

Below is a list of common areas of DCC-i business and the associated retention and deletion policy, however this list is not exhaustive and all requests for deletion will be considered.

Emails – As data should not be kept for longer than it is needed, we ask that employees maintain good housekeeping of their email accounts, including the routine deletion of emails that are no longer required. Email that may relate to matters of finance, complaints, contract disputes, evidence services delivered and/or legal matters can be kept for up to 7 years if required. If contracts have ended the emails will be archived. Contact information will not be used for any other purposes than those they were originally initiated for.

Emails containing registers and/or details of individuals who have additional learning needs to allow for reasonable adjustments, are considered to contain sensitive personal information, and will be deleted after 6 months unless relevant to a complaint or legal process. To comply with this requirement all emails containing registers or information regarding delegates additional needs, the DCC-i administrator will perform a rolling monthly deletion of emails that are over 6 months old.

Any other requests for immediate email deletion will be considered by the Data Protection Officer on a case-by-case basis and will carried out, unless there is a legitimate, exceptional or legal reason not to.

Delegate Information for Training Courses / Email Addresses – Delegate lists are all electronic – there are no printed registers. **This information is obtained under the category of legitimate interests or by contract, rather than consent, as it is required to offer the training being commissioned. Therefore, individual consent for holding the data is not required, the organisation providing the data is responsible for ensuring they comply with their own GDPR Policy in doing so**.

We strongly recommend that customers do provide us with email addresses to facilitate the coordination of training courses. Email addresses enable us to send out invites, reminders and training materials direct to the delegate, we can provide updates to the delegates on additional

resources live and after the delivery of the course, we can provide tech support to delegates that are struggling and if a delegate leaves the training unexpectedly, we can check on their welfare. Providing email addresses is not a breach of most standard organisational GDPR Policies and this use of the 'legitimate interest' basis for data collection and use is robust, our DPO can discuss this further with you if necessary.

Email addresses are hidden in diary invites; however, Organisations are still recommended not to provide personal email addresses wherever possible, and to ensure that they comply with their own GDPR Policy if they do so.

Delegate Lists will be kept for 12 months to allow DCCi to respond to attendance queries that occur; this is considered a sufficient time-frame and the data will be considered obsolete after this point. To comply with this requirement all registers will be saved in monthly folders on sharepoint and the DCC-i administrator will perform a rolling monthly deletion of registers, applications and any course records that are over 12 months old. This excludes data connected to certification which are kept indefinitely.

Access to MS Teams Chat – We strongly recommend that customers do allow delegates access to the chat with DCC-i, this enables us to provide the delegates with slides and links they may find useful, enables delegates to give their input into the course and keep the trainer updated if they are unable to be present for all of the session for any reason, and allows the trainer to check on the welfare of any delegates that may have been affected adversely by the content of the course. Our IT system is robust and there is no organisational risk to the customer from allowing access. If customers are using the chat function as part of a consultation or project, we will seek permission before downloading any information in the chat, and the project platform will be archived on completion.

Delegate information utilised for MS Teams Guest Accounts – Some contracts include the opportunity for their staff to have a guest account in the DCC-i MS Teams Platform, this gives the person access to additional resources. These emails are provided by consent. If the person

ceases to use their account, email addresses may remain dormant in the administrative area of the site unless deletion is requested or that area of the platform is deleted.

Evaluation Forms – Delegates can choose to provide their name and/or demographic data as part of the evaluation process – this is done on the basis of consent. All evaluation data used for the purposes of marketing, tenders or research is anonymised prior to use and is not attributed to individuals. Concerns raised about the course will be shared with the commissioner of the course if appropriate.

Contact Lists for Marketing Purposes – Contact lists are internal and generated following specific requests for the provision of services. Utilising the legal basis of 'legitimate interests', individuals will be contacted in respect of similar services only. All communications will inform the customer that they can object to their data being processed for this purpose at any point, and a simple mechanism will be in place to enable customers to have their data erased from marketing purposes. This request will be recorded to ensure further marketing is not sent and to record the actions taken.

OCN and Internal Certifications – These records will be maintained indefinitely, as it is common for individuals to lose their certificates and ask for them to be re-issued many years after completion, this can only be done if a record of the original certificate exists.
This is deemed to be in the interests of the individual. The information is archived and not used for any other purposes other than to respond to requests for replacement certification.

Research and Evaluation Projects – Information received for research and evaluation policies is anonymised for the purposes of the final report, unless express permission has been obtained to name participants. Original data will be archived indefinitely and not accessed for any other purpose other than to clarify information relating to the original research or evaluation programme, or for further research or evaluation with the same parameters. Any requests for deletion will be considered and carried out unless there is a legitimate, exceptional or legal reason not to.

Independent Social Work / Health and Social Care Commissions – DCC-i offer independent Social Work / Health and Social Care Services such as independent assessments and expert reports, RCA's, SCR's and SAR's. Information obtained regarding these pieces of work come under the categories of Legal Obligation and/or Public Task and therefore this information is retained indefinitely. Customers are advised that they must comply with their own GDPR Policy when providing the information to DCC-i. Information will be exchanged using secure methods as agreed with the customer.

DCCi provides independent supervision services, much information is given by 'Consent' therefore is eligible for consideration of erasure, however the data is ultimately recorded under the 'Legitimate Interest' UK GDPR definition (detailed above), as we may need to refuse any request for refusal if it is essential for DCC-i to be able to evidence services provided or actions taken.

DCCi also provide Practice Education/ASYE Assessment and PE Mentoring and Assessment Services. This is service is agreed by contract, however the information will be held under the 'Public Task' UK GDPR definition, as this information relates to the achievement of a professional qualification/completion of an assessed period of employment it may be required in verifying or querying of the relevant award and therefore will be kept indefinitely and is not eligible for deletion. The information will be archived securely once the award and moderation is confirmed. This is in line with the expectations of Social Work England and the BASW Code of Ethics.

Appendix 1 – Compliance Checklist

Action Required	Person Responsible	Date for completion or frequency of action
Make Updated Policy available to all staff and associates – with date to reply confirmation of reading policy.	DPO	31/01/2024
Provide all staff and associates with updated Policy Training.	DPO	1/02/2024
All staff to ensure regular deletion of emails that are no longer required	All staff	Minimum requirement to check annually.
Emails containing Registers or delegate information over 6 months old in all shared inboxes to be deleted, or request exception to DPO	Deputy Director of Business and Governance	Rolling monthly task.
Registers, records & applications over 12 months old to be deleted from Sharepoint, or request exception to DPO (Excluding certificates and records for certificate which are kept indefinitely)	Administrator	Rolling monthly task
Deletion of MS Teams Areas at end of contract or if no bookings in the previous/next 6 months on 1st April each year.	Deputy Director of Operations	Within 14 days of formal notification of a contract end. Annually on closest working day to 1st April

Undertaking Data Protection Impact Assessments (DPIA's) to be completed on all Research or Evaluation Projects	Project Lead	Commencement of Project
Undertaking Legitimate Interests' Assessments (LIA's) for all key areas of the business.	DPO	Annually
Reporting, Recording and responding within timescales to all requests for right to access data, to rectify or erase data or restrict or object to processing of data that is classified as personal or sensitive.	Reporting & Recording – staff member receiving request, Response by DPO	At time of request in line with the timescales of this policy
Responding within timescales to remove individuals from marketing correspondence on request.	Deputy Director of Business and Governance	At time of request in line with the timescales of this policy
Responding within timescales to any occurrences of Data breaches.	Reporting & Recording – staff member receiving request, Response by DPO	At time of breach in line with the timescales of this policy
Ensuring all delegates are informed in the joining instructions that their data has been provided to us by their employer and informing them where the Privacy Notice is located in respect of this data.	Deputy Director of Operations.	Included in all invites
Maintaining ICO Registration	DPO	Annually

Maintaining compliance with ICO requirements and reviewing compliance with this Policy including updating Privacy Notice if required.	DPO	Annually
Ensuring delegates are given the opportunity to provide emergency details via MS Forms and understand how/when this data or data provided by their organisation will be used.	Trainer	At the beginning of all courses