Data Protection Policy

Policy last reviewed: Oct 2024

Reviewed by: Hannah Tulloch

Date of next review: Oct 2025

Signed off by: Charles Gibson

Date: 08.10.24

Role: Trustee

1. Policy Statement

This document sets out Carney's Community's policy regarding data protection in respect of all personal data held in relation to young people, member organisations or other third parties working with Carney's Community (the "Data Subjects").

This policy outlines the key requirements identified for Carney's Community by the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulations (GDPR) which came into effect in 2020. These regulations are the same as the previous EU GDPR, prior to the UK leaving the European Union.

This policy covers the collection, handling, storage and transmission of personal data received from the Data Subjects. This policy is in addition to other requirements, which may be necessary for specific operations and should be read together with the Carney's Community Confidentiality Policy.

Employee data is covered in more detail in the attached Employee Privacy Notice. Participant data is covered in more detail in the Participant Privacy Statement, attached at the end of this Policy. Sensitive information given voluntarily by participants/users of Carney's Community in the form of a disclosure is covered separately in the Safeguarding Children Policy.

All data Carney's Community collects and processes is listed in the Information Audit at the end of this Policy.

Carney's Community is registered with the Information Commissioner's Office (ICO), reference number ZA344951.

2. Aims and Objectives

Carney's Community adheres to the GDPR by following the guidelines laid out in this policy, and ensuring all staff are made aware of data protection issues and guidelines through in-house training.

The objectives of this policy are to ensure all data collected and held is:

- Processed fairly and lawfully with the lawful basis clearly communicated to Data Subjects;
- Obtained and processed only for specified and lawful purposes and not in any manner incompatible with those purposes;
- Adequate, relevant and not excessive;
- Accurate and kept up to date;
- Not kept for longer than is necessary;
- Processed in accordance with the individual's rights;
- Kept secure;
- Not transferred to countries without adequate protection;

Finally, that Carney's Community is transparent and clear in communicating to individuals our aims and objectives regarding the use and storage of data, and that we ensure as far as is practically possible Data Subjects are aware of their rights.

3. Context

3.1 What is data protection?

The basic principles of the Data Protection Act are designed to:

- Safeguard the handling and use of personal information;
- Respect a person's rights over his/her personal information; and
- Enable organisations such as Carney's Community to legitimately use personal information to operate its business.

Carney's Community needs to capture, obtain, store, access and disclose certain personal data in relation to the people and organisations that we work with when carrying out our activities to enable us to:

- Monitor and evaluate our reach and impact;
- Raise funds in order to continue our work;
- Employ staff and volunteers to carry out the work;
- Inform others of the work we are doing that may benefit them; and
- Ensure we effectively safeguard young people.

Carney's Community recognises the importance of the correct and lawful treatment of personal data and that the failure to do so can cause real harm and distress to the individual to which the information relates and also cause harm to Carney's Community's reputation.

3.2 What is personal data?

Any information which relates to and which can specifically identify an individual living person. This includes, but is not limited to, names and addresses, telephone numbers, email addresses, credit or debit card details, HR details and records of interactions between staff/volunteers and participants (eg mentoring sessions, records of any incidents). Data may constitute personal data even if the individual is only identifiable when the information is tied to other data which is held by Carney's Community.

3.3 When does the GDPR apply?

The GDPR applies whenever there is **processing** of personal data. This includes collecting, handling, storing, transmitting, using or doing anything else with the data, including accessing the data, whether such access is from inside or outside of the UK. The GDPR only applies to personal data which is stored (a) electronically (i.e. on a computer or server) or b) manually if in a filing system that is very sophisticated so that the data is readily accessible.

4. GDPR principles

Carney's Community fully endorses the data protection principles listed in the GDPR and complies with them by ensuring that any personal data held in respect of the Data Subjects is:

i. Processed fairly and lawfully

Carney's Community informs all Data Subjects of the following:

- How we collect information.
- The type of information we collect and hold
- The purpose for which it is kept
- How it is processed
- What our lawful basis is for collecting and retaining it
- How long we keep this information on file
- To whom it may be disclosed and why
- What their rights as a Data Subject are, and who to contact in the event of an enquiry or complaint.

Please see the Information Audit at the end of this policy which lists in detail all types of information collected by Carney's Community, and what we do with it.

Information about staff is also covered by our Employers Privacy Notice, attached at the end of this Policy. A copy of the Privacy Statement for participants is also included at the end of this Policy.

ii. Obtained and processed only for specified and lawful purposes and not in any manner incompatible with those purposes

Carney's Community must process personal data in a way which is compatible with the original purposes for which the data was obtained. Sensitive personal data is used for the purposes of providing our services to participants or if we need to comply with a legal obligation.

We will use non-sensitive personal data to (i) register new participants, (ii) to manage our relationship with them, and (iii) to occasionally update them with information about Carney's Community sessions e.g. cancelled sessions. Our legal grounds for processing data are in relation to points (i), (ii) and (iii) above are for performance of a contract with participants.

We do not share any details with third parties for marketing purposes.

Data used in reports and for statistics is anonymised unless explicit consent has been obtained from the participant (if aged 18 or over) or their parent if they are under 18.

iii. Adequate, relevant and not excessive

Carney's Community seeks to ensure that the personal data it holds on a Data Subject is the minimum amount of data required to carry out its legitimate business, and to safeguard participants and staff.

iv. Accurate and kept up to date

Every effort will be made to ensure that data is accurate and up-to-date, and that inaccuracies are corrected quickly.

However, it is possible that we will not always hold data that is complete and/or entirely accurate. This is because our target participant group can be reluctant to pass on any personal information. The hardest to reach young people are often the ones most resistant to information sharing. Similarly, they often do not come from families willing to engage with any sort of authority or organisation, so verifying any data provided and confirming consent can be problematic.

Carney's Community will always prioritise engaging with young people over data collection, unless the data collection is required by law or for safeguarding purposes, with the aim of collecting the relevant data once trust has been established and the young people are engaging regularly with the Charity.

v. Not kept for longer than is necessary

Carney's Community will review the nature of the information being collected and held on a yearly basis to ensure there is a valid business reason for requiring the information to be retained.

As a result of this review, Carney's Community then takes steps to remove personal data which is no longer needed for the purposes for which it was obtained.

Files of Participants considered 'inactive' are pseudonymised. Out of date data or any information deemed unnecessary is securely and systematically destroyed by shredding or deleted from the online database.

See data retention schedule for more information in Appendix 1: Data Audit

vi. Processed in accordance with the individual's rights

Personal data should be processed in accordance with an individual's rights under the GDPR. These are:
The right to be informed;
The right of access;
The right to rectification;
The right to erasure;
The right to restrict processing;
The right to data portability;
The right to object;
The right to not be subjected to automated decision making including profiling.

These rights are communicated via our Website & Cookie Privacy Statement, and the Participant Privacy Statement.

vii. Kept secure

Carney's Community seeks to ensure that it has adequate measures in place to prevent unauthorised or unlawful processing of personal data and to prevent accidental loss, destruction or damage. All data is stored securely in lockable files, on our secure shared drive, and within the upshot database. More particularly, Carney's Community takes reasonable steps to ensure that:

- any doubt about a person's authorisation to be in any of our workplaces is challenged and if necessary reported;
- desks and cupboards are securely locked if they hold confidential information of any kind;
- paper documents which are no longer required are shredded and CD-ROMs and USBs are physically destroyed when they are no longer required;
- personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party;
- access to the upshot database is password protected and restricted to staff with a requirement to access the system;
- the security of our information systems is reviewed annually and updated as necessary.

viii. Not transferred to countries without adequate protection

Currently Carney's Community uses Dropbox and Mailchimp, based in the USA. Both companies are GDPR compliant. Carney's Community does not directly send participants or staff's sensitive information outside the UK.

5. Access to Personal Data

All Data Subjects have the right under the GDPR to be:

- told whether any of their personal data is being processed;
- given a description of the personal data, the reasons why it is being processed and whether it will be given to any third party organisation or other person;
- given a copy of the personal data (subject to such redaction as Carney's Community considers necessary to comply with its GDPR obligations and/or protect its commercial interests); and
- given details of the source of the data.

If the Data Subject wishes to exercise these rights they should contact the Carney's Community Data Protection Officer (DPO – Hannah Tulloch) via email: hannah.tulloch@carneyscommunity.org or by post: 30 Petworth Street, London SW11 4QW

Carney's Community will aim to comply with any subject access request as quickly as possible and will ensure that it is provided within 1 calendar month of the receipt of a written or emailed request.

6. Data Subject consent

- Whenever personal data is given to Carney's Community, the Data Subject should be asked to consent to their information being stored. If the Data Subject is under the age of 18, such consent should be obtained from that child's parent or guardian where possible.
- the nature of the data storage and any possible uses of the data is declared at the point of consent being given via the Participant Privacy Statement
- data will only be stored if consent has been given;
- all consent forms will be retained;
- the relevant personal data obtained should not be publicly accessible to anyone other than parties declared at the point of consent being given; and
- Any individual who has their personal data held by Carney's Community should be informed of their rights to access such data (as described above).

All of the above points are achieved via the informed consent option on the registration form. Carney's Community is working towards making all participants aware of the issue of consent & data protection. If participants do not consent to their data being stored, this will limit the amount of support that can be offered by the organisation due to our responsibilities for safeguarding and health and safety.

7. Responsibilities

Overall responsibility for the efficient administration of the GDPR lies with Carney's Community. Day-to-day responsibility for oversight of compliance with the GDPR is delegated to the Data Protection Officer for compliance with the GDPR provisions within their respective areas of authority. Carney's Community Data Protection Officer is Hannah Tulloch, Chief Operating Officer.

All employees and trustees of Carney's Community have a duty to observe the principles of the GDPR and the procedures referred to in this document and to comply fully with this policy and the principles of the GDPR. This policy will be shared and training given to support team members with these responsibilities.

Disciplinary action may be taken against any employee who breaches any of the instructions or procedures set out in this policy. Individuals who do not handle data as part of their normal work have a responsibility to ensure that any personal data they see or hear remains strictly confidential and is not disclosed to any third party. This includes personal data and information extracted from such data. For example, un-authorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or even inadvertently by reading a computer.

Trustees could be regarded as data controllers if they process personal data either manually or by computer, whether on their own equipment or on equipment provided to them by Carney's Community. Just as any other individual holding and processing personal information about others, Trustees need to comply with the GDPR, and need to notify the Data Protection Officer of all purposes for which they hold and process personal data.

7.1 Data relating to our participants

In addition to the procedures listed above, to ensure compliance with the principles of the GDPR and the procedures referred to in this document, Carney's Community ensures the following measures are in place and adhered to:

- Participants data will not be given out to third parties unless compliant with this Data Protection Policy;
- All consent forms will be retained by an appropriate member of staff and filed appropriately.

8. Guidelines on use of personal or non-Carney's devices for processing data

It is acceptable to use a personal device (i.e. phone, laptop, tablet or computer) to process data, as long as the following guidelines are adhered to:

- If a non carneys device is used to take a photo or scan a copy of paperwork, including contact sheets, to send to the administrator, you must delete the photo/scan off the storage on your device.
- If a non Carneys device is used to create or view documents these must be saved to the Carney's dropbox and not to the device itself.
- Any non carneys device must be password protected/fingerprint/pin, so that only authorised individuals can access information that may be stored on the drop box, emails, Upshot or other cloud storage systems.

9. Disclosure of Personal Data

Personal data may only be disclosed outside of Carney's Community to a third party with the written consent of the Data Subject, or in circumstances where young people are considered to be at immediate risk. Carney's Community will occasionally share anonymised information with our funders (for reporting purposes) and with other agencies that we consider might benefit young people or our members. The data protection statement on our registration forms explains how and why Carney's Community might share information, when appropriate.

Procedures with Police requests – see additional guidelines – Releasing Personal Data to Outside Agencies Sections 4a and 5.

10. Child protection in relation to this data protection policy

All children and young people, and their families, are entitled to respect for their privacy. However, where there are concerns about the safety or welfare of a child or young person, those concerns and the necessary personal information may have to be shared. It is the role of the Designated Safeguarding Officer (DSO – George Turner) to liaise with outside agencies regarding child protection issues. If a staff member has any safeguarding concerns or concerns about sharing information, they should speak to the DSO.

There is nothing in any legislation that prohibits the sharing of confidential and personal information where there are concerns about the safety or welfare of a child/young person, or where a criminal act may be, or may have been committed. However, the child's safety and welfare must be the overriding consideration.

This policy should be read in conjunction with;
Confidentiality Policy & Working Guidelines
Child Safeguarding Policy
Vulnerable Adults Safeguarding Policy

9.1 Information sharing: Working together to safeguard children

All records related to concerns about a child's or young person's safety or welfare will be held securely. Any records held on computer will comply with the GDPR.

These detailed records should be kept until Carney's Community is confident that the information is held accurately with the agency responsible for taking further action to safeguard the child i.e. partner agencies, social care children's services or the police. A chronology of decisions made and actions taken can then be kept on file, once the detailed records are deleted or destroyed. This record should not be held for longer than six years.

11. Making a complaint

In the first instance, if any participant or staff member feels uncomfortable about anything related to data protection at Carney's Community they can discuss with a member of the management team. If they do not feel their issue has been sufficiently dealt with they can put a request in writing to the DPO.

Carney's Community is registered with the ICO and they can be contacted with any enquiries or complaints relating to data. If a Data Subject does not want to go via the persons specified above, or feels an existing enquiry or complaint has not been dealt with to their satisfaction, they can contact the ICO directly.

These rights are clearly communicated via our Employees Privacy Notice and the Participant's Privacy Statement.

12.Monitoring and review

This policy will be monitored periodically to judge its effectiveness and will be updated in accordance with changes in the law. We will report to the Board of Trustees on any serious issues that arise in relation to data protection. The policy will be reviewed annually and updated if necessary. Any questions about the policy should be directed to the COO, Hannah Tulloch, who is the person responsible for Data Protection in the organisation.

Appendix 1. Information Audit

PARTICIPANTS Type of data	Collected via	Stored in*	Used for	Communicated via	Lawful basis for processing the data	Kept for:	How are data subjects made aware?	Shared with?	How is data transferred
Name, DOB	Registration form	Upshot database, paper form in filing cabinet	Identifying participant, tracking their attendance	Privacy Statement	The consent of the individual, necessary for carrying out legitimate company business	4 years from their last engagement with Carney's Community	Privacy Statement attached to Registration form	Staff, Outside agency 'as needed' usually only 121 mentored participants Some funders require initials and DOB and some require name.	Verbally, in meetings In reports to funders
Email, address	Registration form	Views database, paper form in filing cabinet	Occasional contacting of participants and Mentor program.	Privacy Statement	The consent of the individual, necessary for carrying out legitimate company business	4 years from their last engagement with Carney's Community	Privacy Statement attached to Registration form	Admin. Outside agency as needed, usually only 1:1 mentees. Some funders ask for postcodes.	Verbally, in meetings, request via internal email Reports to funders
Phone number	Registration form	Views database,	Occasional contacting of participants and Mentor program.	Privacy Statement	The consent of the individual, necessary for carrying out legitimate business	4 years from their last engagement with Carney's Community	Privacy Statement attached to Registration form	Admin team and managers, outside agency as needed. Other participants can see on what's app groups – with verbal consent	Email
Gender, ethnicity, religious beliefs, country of birth	Registration form	Views database, paper form in filing cabinet	Anonymised reporting	Privacy Statement	Individual consent, necessary for carrying out legitimate business	4 years from their last engagement with Carney's Community	Privacy Statement attached to Registration form	Outside agency 'as needed' usually only 121 mentored participants,	In meetings Anonymised reports
Health questionnaire, information on mental & physical disabilities	Registration form	Views database, paper form in filing cabinet	Anonymised reporting, information shared on a 'need to know' basis necessary to ensure safety & wellbeing of all participants	Privacy Statement	Individual consent, necessary for carrying out legitimate business, to ensure safety & wellbeing of participants, necessary for safeguarding in the public interest.	4 years from their last engagement with Carney's Community	Privacy Statement attached to Registration form	Outside agency 'as needed' usually only 121 mentored participants, CC staff on a need to know basis	In meetings, internal email Anonymised reports
Risk factors	Registration form	Views database, paper form in filing cabinet	Anonymised reporting, info shared on a 'need to know' basis, to ensure safety & wellbeing of all participants, to identify participants to target services.	Privacy Statement	Individual consent, necessary for carrying out legitimate business, necessary to perform safeguarding in the public interest.	4 years from their last engagement with Carney's Community	Privacy Statement attached to Registration form	Outside agency 'as needed' usually only 1:1 mentees. CC staff as needed	In meetings, internal email Anonymised reports
Emergency contact details, GP	Registration form	Views database, paper form in filing cabinet	Contacting participant next of kin in an emergency; details of parent/ carer (under 18's)	Privacy Statement	The consent of the individual, necessary for carrying out legitimate business	4 years from their last engagement with Carney's Community	Privacy Statement attached to Registration form	CC staff	In person, or obtained from file

STAFF and volunteers Type of data	Collected via	Stored in*	Used for	Communicated via	Lawful basis for processing the data	Kept for:	How are data subjects made aware?	Shared with?	How is data transferred
Name	Application	Dropbox Airtable	Identification	Application process	Carrying out legitimate company business	Successful applicants – 6 years after ending employment. Unsuccessful applicants 6 months	On applying	Staff involved in selection process and administrator	Face to face, via application form
Contact details	Application	Airtable	Identification	Application process	Carrying out legitimate company business	Successful applicants – 6 years after finishing employment, unsuccessful applicants 6 months	On applying	Staff involved in selection process/administrator	via application form
GP, emergency contact details	Forms given on accepting job	Airtable	Only in event of an emergency	Application process	Carrying out legitimate company business	Successful applicants – 6 years after finishing employment	On accepting job with CC	CC Administrators only	During induction process
Health status (allergies, conditions)	Forms given on accepting job	Airtable,	Safety & wellbeing of staff member	Application process	Carrying out legitimate company business	Successful applicants – 6 years after finishing employment,	On accepting job with CC	CC Administrator, other staff on a 'need to know basis'	During induction process
Interests	Application	Airtable	For recruitment selection only	Application process	Carrying out legitimate company business	Staff – 6 years after finishing employment, unsuccessful applicants 6 months	On applying	Staff involved in selection process/administrator	via application form
Qualifications	Application	Airtable	For recruitment selection only	Application process	Carrying out legitimate company business	Staff – 6 years after ending employment, unsuccessful applicants 6 months	On applying	Staff involved in selection process/administrator	via application form
DBS certificate	Forms given on accepting job	Airtable	Safeguarding	Application process	Carrying out legitimate company business, Safeguarding	Staff – deleted after 6 months	On accepting job with CC	Admin and Managers	DBS website, staff member brings in hard copy
References	Requested after job offer made	Airtable	Verifying application info	Employers Privacy Notice	Carrying out legitimate business	Staff – 6 years after ending employment	On accepting job with CC	Admin and Managers	Phone calls/email
Permission to work in UK	Passport seen		Verify ability to work in UK	Employers Privacy Notice	Legitimate business	Staff – 6 years after ending employment	On accepting job with CC	Admin and Managers	Email/ in person
Payroll forms (P45, P60) Staff only	Sent automatically via HMRC	Airtable	payroll	Employers Privacy Notice	Legitimate company business	Staff – 6 years after ending employment	During induction	Admin and Managers, payroll provider	Dropbox
Bank account details Staff only	Requested after job offer made	Airtable	payroll	Employers Privacy Notice	Carrying out legitimate business	Staff – 6 years after ending employment	Verbally, emails, signed form	Admin, payroll provider, managers	Dropbox
HMRC form/NI no.	Requested after job offer made	Airtable	payroll	Employers Privacy Notice	Legitimate business	Staff – 6 years after ending employment	Emails, signed form	Admin, payroll accountant	Dropbox
Passport	Requested after job offer made	Airtable	payroll	Employers Privacy Notice	Carrying out legitimate business	Staff – 6 years after ending employment	Verbally, emails, signed form	Admin	Dropbox
Other ID documents	Requested after job offer made	Airtable	Carrying out legitimate business	Employers Privacy Notice	Carrying out legitimate business	Staff – 6 years after ending employment	Verbally, emails, signed form	Admin	Dropbox
Supervision notes	Done periodically during employment	Dropbox	HR purposes	Employers Privacy Notice	Carrying out legitimate business	Staff – 6 years after ending employment	Verbally, emails, signed form	Senior staff, Admin	Not transferred outside
Disciplinary notes	When needed	Dropbox	HR purposes	Employers Privacy Notice	Carrying out legitimate business	Staff – 6 years after ending employment	Verbally, emails, signed form	Senior staff, Admin	Not transferred outside
Payroll summaries, payslips, pension info	Monthly payroll	Dropbox	Payroll and finance management	Email	Legitimate business	7 years	Employee privacy notice	Admin staff, managers	Not transferred outside

Other data held by Carney's Community

Type of data	Collected via	Stored in*	Used for	Communicated to data subject via	Lawful basis for processing the data	Kept for:	How are data subjects made aware of this?	Shared with?	How is data transferred
Case studies – named & anonymised	Interviews, staff's knowledge of participant	PC hard drive, (GT) Dropbox	Report writing, charity publicity	A consent form signed & filed to demonstrate participants agreement to be the subject	Carrying out legitimate business, consent	Unspecified	Verbal agreement, consent form will be given	All interested parties	Various including press and reports
Email address	Link to email sign up	Mail chimp	Distributing Newsletter	Website Privacy & Cookie Policy	Carrying out legitimate company business	Until user unsubscribes	Website/ Mailchimp	Mailchimp/ administrators	Auto-transfer
Non-personal info e.g. browser name, type of computer and technical info about Users means of connection to our website, such as OS and ISP	Website (cookies)	Website	Improve website	Website Privacy & Cookie Policy	Carrying out legitimate company business	Unspecified	Website	N/A	N/A
Photos	Staff, journalists	Various Dropbox	Publicity	Participants consent via tick box on registration, special events have one off forms. Consent from under 16's sought from parent/carer	Consent	Unspecified	Consent forms, verbal communications from staff	All interested parties, website, press	n/a
Quotes/ testimonies	Staff, journalists, Social media	Various	Publicity	Participants consent via tick box on registration, special events have one off forms. Consent from under 16's sought from parent/carer	Consent	Unspecified	Consent forms, verbal communications from staff	All interested parties, website, press	n/a
Incident report forms	Staff, reporting/ interviews with relevant participants	Filing cabinet (participant files) plus central folder on Dropbox	Monitoring incidents	Staff/ participant interaction	Carrying out legitimate company business, safeguarding	6 years after participant has left	At time (staff/participant interaction)	Managers/ Admin & Mentors. Social services & other safeguarding agencies.	Verbally, on Dropbox.
Mentoring/key working records, Outcomes	Hard copy reports written by mentors/ key workers & emailed to Admin. GT emails reports by email with names initialised	Reports on Participant Views record, hard copies shredded or filed in Participant file.	Recording & Monitoring participant progress within CC Mentoring programme. Annual accounts	Staff/ participant interaction	Consent, Carrying out legitimate business, safeguarding	6 years after participant has left	Consent forms, verbal communications from staff	Admin staff, Managers, Mentors Companies House and charity commission	Only anonymised information is transferred outside of CC Reports to funders.

SLA Type of data	Collected via	Stored in*	Used for	Communicated via	Lawful basis for processing the data	Kept for:	How are data subjects made aware of this?	Shared with?	How is data transferred
Name	ID's	Dropbox, Airtable	Identification	Application process	Carrying out legitimate business	SLA holders- 6 yrs after finishing SLA, unsuccessful applicants 6 months	On applying	Staff involved in selection process/administrator	Face to face, email / via ID's
Contact details	ID's	Airtable	Identification	Application process	Carrying out legitimate business	SLA holders –6 yrs after finishing SLA, unsuccessful applicants 6 months	On applying	Staff involved in selection process/administrator	Email / via ID's
GP, emergency contact details	Forms given on accepting SLA	This info will be collected from 2021	Only in the event of an emergency	Application process	Carrying out legitimate business	Successful applicants – 6 years after finishing SLA	On accepting SLA with CC	Administrators only	During induction process
Health status (allergies, conditions)	Forms given on accepting SLA	This info will be collected from 2021	Safety & wellbeing of staff member	Application process	Carrying out legitimate company business	Successful applicants – 6 years after ending SLA	On accepting SLA with CC	Administrator, other staff on a 'need to know basis'	During induction process
Qualifications	Application	Airtable	Insurance purposes	Application process	Carrying out legitimate business	Successful applicants – 6 years after finishing SLA	On applying	Staff involved in selection process/ HR & admin staff	During induction process
DBS certificate**	DBS forms	Airtable	Safeguarding Insurance purposes	Application process	Legitimate business, Safeguarding	6 months.	During the SLA process	CC Administrators and Managers	DBS website or in hard copy
Permission to work in UK	Passport seen	Airtable	Verify ability to work in UK. For insurance	SLA	Legitimate business	Staff – 6 years after finishing SLA.	During the SLA and DBS process	CC Administrators and Managers	Email/ in person
ID documents	Email/ in person	Airtable	Carrying out legitimate business	SLA	Carrying out legitimate business	Staff – 6 years after finishing SLA.	In person / email	CC Administrators / Managers	Dropbox

Appendix 2. Accessible privacy notice for participants Privacy Statement for participants:
This statement is included with all registration forms for new participants and must be reviewed by the parent or carer who signs this form. Participants can access the full version online, following the link at the bottom of the notice.

Privacy Notice

Why are we asking for this information?
We need to collect information to help us do our job, to keep you safe and to follow the law. The information we collect from you on this form and from your parent/carer is used to register you as a participant and to keep in touch with you about the activities we're running, e.g. new activities or cancelled sessions.

Who looks after your information?
Carney's Community looks after the information, we're called a "data controller". We keep your information on a secure online system, which is password protected and only accessible by staff at Carney's who need the information.

Will your information be shared?
We only share personal information with anyone outside of Carney's if we're required to by law. For example, to protect you if there are safeguarding concerns. When your data is shared with someone else, they must keep it safe. To keep our work going, the information we collect from all participants is gathered, we make it anonymous and then share this with the people and organisations who donate money to Carney's. For example, we tell them how many young people attended a session or the number of young people who are doing better in school because of our work. No one will know who this is when we share this.

How long do we keep your information for?
We will keep hold of your information whilst you're still coming to our sessions or keeping in contact with us. Once you've left we'll hold onto your information for 4 years and then delete it. To keep our information up to date we may contact you to confirm that the information you've given is still accurate.

Your Rights
In some situations you can ask us to delete the information we keep. You can also ask us what information we keep about you. You have to do this by email or in a letter and it can take one month for us to get the information to you. If you have any questions about this, speak to one of the staff or email us at info@carneyscommunity.org.

This is a short version of our privacy statement, for the full version go to www.carneyscommunity.org/policies

Appendix 3. Full Privacy Statement for participants:

This Version is available online for participants to access.

1. How we use your personal data

We are committed to protecting your personal data. The data we collect from you includes that submitted by you on the form overleaf, details of your attendance at Carney's sessions, and occasional feedback from you about our services.

We will use your sensitive personal data (that is the data you completed in the attached form) for the purposes of providing our services to you or if we need to comply with a legal obligation. We will use your non-sensitive personal data to (i) register you as a new client, (ii) to manage our relationship with you, (iii) to occasionally update you with information about Carney's Community sessions e.g. cancelled sessions. Our legal grounds for processing your data are in relation to points (i), (ii) and (iii) above are for performance of a contract with you.

2. Disclosure of your personal data

We may have to share non-sensitive and sensitive personal data with (i) other professionals/agencies where we are working in partnership with them to engage and support specific young people with specific needs, (ii) staff/coaches for the purpose of ensuring safeguarding of young people and safe practice during boxing fitness sessions. All information (both sensitive and non-sensitive) is treated as confidential and only shared where a 'need to know' basis has been established.

Personal data is disclosed to third parties in an anonymised (so that individuals cannot be identified), statistical format to provide evidence of Carney's Community's work, reports to funders, Trustees and other interested parties, and to make funding applications. Data in this anonymised format may be used indefinitely without further notice to you.

We require all of these third parties to whom we transfer data to respect the security of your personal data and to treat it in accordance with the law. They are only allowed to process your personal data on our instructions.

We will not share any of your details with third parties for marketing purposes.

3. International transfers

Data provided on this form is not shared internationally.

4. Data security

Protecting your data is important to us and we have put in place security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We also limit access to your personal data to employees, and/or other third parties who have a business need to know such data. They will only process personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breaches and will notify you and any applicable regulator of a breach where we are legally required to do so. In certain circumstances you can ask us to delete your data. See the section entitled 'your rights' below for more information.

5. Data retention

We will only keep your personal data for as long as is necessary to fulfil the purposes for which we collected it. We may retain your data to satisfy any legal, accounting, or reporting requirements. You have the right to ask us to delete the personal data we hold about you in certain circumstances. See section 6 below.

6. Your rights

You are able to exercise certain rights in relation to your personal data that we process. These are set out in more detail at: www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

In relation to a Subject Access Right request, you may request that we inform you of the data we hold about you and how we process it. We will not charge a fee for responding to this request unless your request is clearly unfounded, repetitive or excessive in which case we may charge a reasonable fee or decline to respond.

We will, in most cases, reply within one month of the date of the request unless your request is complex or you have made a large number of requests in which case we will notify you of any delay and will in any event reply within 3 months.

If you wish to make a Subject Access Request, please send the request to the DPO, Carney's Community, 30 Petworth Street, London SW11 4QW or email info@carneyscommunity.org marked for the attention of the Data Protection Officer.

7. Keeping your data up to date

We have a duty to keep your personal data up to date and accurate so from time to time we will contact you to ask you to confirm that your personal data is still accurate and up to date.

If there are any changes to your personal data (such as a change of address) please let us know as soon as possible by writing to or emailing us, using the details set out in section 6 above.

8. Complaints

We are committed to protecting your personal data but if for some reason you are not happy with any aspect of how we collect and use your data, you have the right to complain to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk).

We should be grateful if you would contact us first if you do have a complaint so that we can try to resolve it for you. Please contact the Data Protection Officer: info@carneyscommunity.org.

We may change this Privacy Notice from time to time and shall notify you of any changes.

Appendix 4: Privacy notice for Employees

INTRODUCTION
Carney's Community ("we" or "us") take the privacy and security of your personal data very seriously. In this privacy notice, we set out how we collect and use your personal data before, during and after your working relationship with us, in accordance with the UK General Data Protection Regulation (GDPR). It applies to all of our current and former employees, volunteers, workers and contractors and it does not form part of any employment contract or any other services contract with us.

We may update this notice at any time and we may provide you with additional privacy notices from time to time.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

DATA PROTECTION PRINCIPLES
We will comply with data protection law including the 6 principles of GDPR which are:
1. To process your personal data lawfully, fairly and in a transparent way.
2. To collect your personal data only for valid purposes that we have advised you about and to not use your personal data in any way that is incompatible with those purposes (unless we have notified you and explained the lawful ground that allows us to do so).
3. To only process your personal data to the extent necessary for the purposes we have advised you about.
4. To keep your personal data accurate and kept up to date.
5. To keep your personal data only as long as necessary for the purposes we have told you about.
6. To keep your personal data secure.

PERSONAL DATA THAT WE PROCESS
Personal data means any information about an individual from which that person can be identified. It does not include anonymous data where the identity has been removed. There are "special categories" of more sensitive personal data which require a higher level of protection such as your ethnicity and whether you are a member of a trade union.

We will collect, store, and use the following categories of personal data about you:
- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses;
- Date of birth;
- Gender;
- Marital status and dependants;
- Next of kin and emergency contact information;
- National Insurance number, bank account details, payroll records and tax status information;
- Salary, annual leave, pension and benefits information;
- Start and finish dates;
- Location of employment or workplace;
- Copy of driving licence and other ID;
- Recruitment information, including copies of right to work documentation, references, CV or application form or other details we collect as part of the application process;
- Employment records, including job titles, work history, working hours, training records and professional memberships;
- Performance information including details of any disciplinary and grievance procedures;
- CCTV footage;
- Information about your use of our information and communications systems;
- Photographs;

We may also collect, store and use the following "special categories" of more sensitive personal information:
- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions;
- Trade union membership;
- Information about your health, including any medical condition, health and sickness records;
- Information about criminal convictions and offences;

HOW WE COLLECT YOUR PERSONAL DATA
We collect personal data about you through the recruitment process, either directly from you or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

When you start your employment with us, you will directly provide us with certain personal data such as your bank account details and next of kin information. We may collect further personal data about you in the course of your employment.

HOW WE USE YOUR PERSONAL DATA

We will only process your personal data if we have a lawful ground for processing such data. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the employment contract between us or any other contract between us.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal data in the following situations, but these are not likely:

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest or for official purposes.

PURPOSES FOR WHICH WE PROCESS YOUR PERSONAL DATA

We will process your personal data for the following purposes:

- Making a decision about your recruitment or appointment;
- Determining the terms on which you work for us;
- Checking you are legally entitled to work in the UK;
- Paying you and, if you are an employee, deducting tax and National Insurance contributions;
- Providing certain benefits to you e.g. pension;
- Liaising with your pension provider;
- Administering the contract we have entered into with you;
- Business management and planning, including accounting and auditing;
- Conducting performance reviews, managing performance and determining performance requirements;
- Making decisions about salary reviews and compensation;
- Assessing qualifications for a particular job or task, including decisions about promotions;
- Gathering evidence for possible grievance or disciplinary hearings;
- Making decisions about your continued employment or engagement;
- Making arrangements for the termination of our working relationship;
- Education, training and development requirements;
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work;
- Ascertaining your fitness to work;
- Managing sickness absence;
- Complying with health and safety obligations;
- To prevent fraud;
- To monitor your use of our information and communication systems to ensure compliance with our policies;
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
- Equal opportunities monitoring.

If you decide not to provide us with certain personal data that we have requested, we may not be able to perform contracts between us (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

We may from time to time use your personal data without your knowledge or consent where this is required or permitted by law.

HOW WE USE SENSITIVE DATA

"Special categories" of sensitive personal data require higher levels of protection than non-sensitive data. In order to process such sensitive data we need to have further justification. We may process special categories of personal data in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.

Occasionally, we may process sensitive personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We will use your sensitive personal data in the following ways:

- In relation to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.

- In relation to your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to administer benefits.
- In relation to your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- In relation to your trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

DBS CHECKS AND CRIMINAL CONVICTIONS

We may only process data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations. Rarely, we may use your personal data relating to criminal convictions where necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Once a recruitment (or other relevant) decision has been made, we do not keep certificate information for any longer than is necessary. This retention will allow for the consideration and resolution of any disputes or complaints, or be for the purpose of completing safeguarding audits.

Once the retention period has elapsed, we will ensure that any DBS certificate information is immediately destroyed by secure means, for example by shredding. While awaiting destruction, certificate information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack). We will not keep any photocopy or other image of the certificate or any copy or representation of the contents of a certificate. However, not withstanding the above, we may keep a record of the date of issue of a certificate, the name of the subject, the type of certificate requested, the position for which the certificate was requested, the unique reference number of the certificates and the details of the recruitment decision taken.

AUTOMATED DECISION-MAKING

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.
2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights. You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

TRANSFERS TO THIRD PARTIES

We may have to share your personal data with third parties, including third-party service providers for example because it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Third party providers may carry out the following services: payroll, pension administration, benefits provision and administration, IT services.

We may also transfer your personal data to other entities as part of our regular reporting activities on our performance, for example to our funders, for system maintenance support and hosting of data.

We may share your personal information with other third parties, for example in the context of the possible merger or restructuring of the charity. We may also need to share your personal information with a regulator or to otherwise comply with the law.

We require third parties to respect the security of your data and to treat it in accordance with the law. They must act only in accordance with our instructions and they agree to keep your personal data confidential and secure.

DATA SECURITY

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

DATA RETENTION

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

It is important that the personal data we hold about you is accurate and up to date. Please keep us informed if your personal information changes.

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Protection Officer in writing via hannah.tulloch@carneyscommunity.org

You will not have to pay a fee to access your personal data or to exercise any of the other rights under data protection laws. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please email us at george@carneyscommunity.org. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

If you have any questions about this privacy notice, please contact the DPO: hannah.tulloch@carneyscommunity.org