GALACTICO COACHING

GDPR Policy

Contents

1. Introduction

Galactico Coaching (GC) is committed to the safety and well-being of all children and adults involved with GC. GC and all people associated with GC must adopt and implement this policy.

This policy establishes the commitment of GC to handling data safely and sensitively. The policy is intended to ensure any information held on individuals is accurate and is only collected and held for its intended purpose.

2. Definitions and Interpretations

Below are the meanings of words that this policy highlights:

GDPR stands for General Data Protection Regulations.

ICO stands for Information Commissioner's Office.

Personal Data refers to any information that relates to an individual. For example, their name, address, contact details etc. It can also include special characteristics such as information relating to a person's physical, physiological, genetic, mental, economic, cultural or social identity.

Personal Data Breach is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Abuse relates to any type of abuse, including physical, emotional, psychological, sexual, and inappropriate use of power, that has caused, is causing, or is likely to cause harm to a person's wellbeing.

Safeguarding and Promoting the Welfare of Children means:

- Protecting children from abuse and neglect.
- Preventing impairments of children's mental and physical health or development.
- Taking action to help all children to have the best outcomes.

3. Purpose of our Policy

The Galactico Coaching GDPR Policy aims to ensure that participants involved with GC know how their data will be handled, and that staff are aware of their responsibilities in handling participant's data. This policy seeks to inform everyone involved with GC about the expectations and requirements of effective GDPR practice to ensure all participants of GC are kept safe and protected from harm, without fear of their personal information being shared. The policy is intended to promote an environment and culture of data privacy. The policy will outline the processes to follow to ensure data is handled safely and sensitively.

4. Who our Policy Applies to

This policy applies to:

- Paid and unpaid employees, volunteers, or contracted personnel of GC.
- Board and Committee Members.
- Affiliated centres, clubs, organisations, and personnel.

5. The Extent of our Policy

Everyone affiliated with GC is expected to comply with this GDPR Policy. This GDPR policy applies to information stored in all forms including, but not limited to:

- Hard copy documents.
- Information/data stored electronically, including scanned images.
- Communications sent by post, email, text or electronic file transfer.
- Information or data stored on or transferred to DVD, USB storage device or memory card.
- Information stored on portable electronic devices including mobile phones, tablets, cameras and laptops.
- Speech, voice recordings and verbal communications, including voicemail.
- Published web content.
- Photographs.

Participants, parents and carers have the right to access any data that GC hold that relates to them and are encouraged to review it to ensure its accuracy. This is to reassure individuals that any data stored is reasonable and can be queried or altered if they wish.

It is crucial to prevent any data breaches and leaks as these can be detrimental to the security and safety of participants and staff, and cause reputational damage.

6. Responsibilities

The protection of data is the responsibility of GC staff.

The individuals to whom this Policy applies (Section 4) must:

- Monitor GDPR use in their setting.
- Store and process any personal data in accordance with GC procedures.
- Inform GC of any changes to their personal data.
- Ensure they understand GDPR and Data Protection.
- Read and understand this GDPR Policy, and consistently adopt, implement and comply with it.
- Ensure that the policy is easily accessible to all.
- Ensure that the existence and consequences of breaching this policy, are widely known.
- Be willing to undertake any training required by GC.
- Deal with any breaches or complaints concerning this policy, in a prompt, impartial

and sensitive manner.
- Follow the procedure outlined in this policy.
- Understand that failure to comply with this GDPR policy may result in disciplinary action.
- Be accountable for their own behaviour.
- Comply with any decisions and discipline imposed following this policy.
- Continually monitor and review this policy when required.
- All staff must read the Policy at the start of each year.
- Any new or returning staff must read the Policy within the first two weeks of employment.
- All staff must sign to say that they have read the Policy. This log must be retained.
- Review the policy annually as a minimum and ensure that the procedures are implemented, updated and reviewed regularly.

Individuals to whom this policy applies (Section 4) must contact the Director if:

- They have any questions about the procedures, data protection law, retaining personal data, or keeping personal data secure.
- They have any concerns that the procedures are not being followed, or not being followed accurately.
- They are unsure if they have a lawful basis to use personal data in a particular way.
- They have to rely on or capture consent or deal with data protection rights invoked by an individual.
- There has been a data breach.
- They are engaging in a new activity that may affect the privacy rights of individuals.
- They need to share personal data with third parties.

6.1 Affiliated Centres, Clubs and Organisations Responsibilities

Affiliated centres, clubs and organisations bound by this policy are responsible for:

- Implementing and complying with the GC GDPR policy.
- Promoting the policy and modelling the desired behaviours.
- Dealing with any breaches or complaints concerning this policy, in a prompt, impartial and sensitive manner.
- Seeking advice from and referring serious issues including unlawful behaviour to GC.

7. Process

GC will only collect personal data for specified, explicit and legitimate reasons as stated in Attachments 1 and 2. If personal data is used for purposes other than those, GC will inform the individuals concerned before using the data and will seek consent where necessary.

GC staff should only process personal data where it is necessary to enable them to do their jobs and GC will aim to ensure the data is accurate and up to date. Any inaccurate data will be rectified or erased where appropriate. Any personal data that is no longer needed will be deleted or anonymised.

7.1 Access Requests

Individuals have the right to obtain confirmation that their data is being processed, and to request access to personal information that GC holds about them. This can include:

- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data.
- Who the data has been, or will be, shared with.
- The source of the data if it was not the individual.
- How long the data will be stored for, and the criteria used to determine this.
- To request rectification, erasure or restriction of the data.

The Director should be notified of any requests that are made to gain access to personal information. Any access requests must be made in writing and include the following information:

- Individual's name.
- Contact address.
- Contact number and email address.
- Details of the information requested.

If the personal data relates to a child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent, if a parent/carer wants to request access to their data.

- If the child is below the age of 12, they are generally considered to not be able to understand their rights and the implications of a subject access request, so most access requests from parents/carers may be granted without express consent from the child.
- If a child is aged 12 and above, they are generally considered to be mature enough to understand their rights and the implications of a subject access request, so most access requests from parents/carers may only be granted with express written consent from the child.
- This is not a rule, and the child's ability to understand their rights will always be judged on a case-by-case basis.

When responding to access requests, GC will ensure the individual requesting the data can legally request the information. If the requester is a third party, GC will ensure that the subject of the data has provided written consent and will:

- Promptly contact the individual to confirm the request was made and ask the individual for identification.
- Respond within 1 month of receipt of the request or of receipt of the additional information needed to confirm identity. If the request is complex or numerous, GC will inform the individual at the 1-month mark that they will respond within 3 months of receipt of the request and provide an explanation for the extension.
- Provide the information free of charge.

GC may choose not to disclose information if it:

- Could cause harm to the physical or mental health of the individual.
- Would reveal that the child is being or has been abused, or is at risk of being abused, and the disclosure of the information would not be in the child's best interests.
- Would include another individual's personal data that cannot be anonymised, and the other person has not consented and it would be unreasonable to proceed without the consent.
- Is part of certain sensitive documents. For example, those related to crime, immigration, legal proceedings etc.

GC may refuse to act on a request for access if the request is unfounded, repetitive or excessive. Alternatively, they may choose to charge a reasonable fee to cover administrative costs. GC will provide explanations to the individual for any access requests that they have refused.

Individuals can:

- Withdraw their consent for GC to process their data at any time.
- Request to rectify, erase, or restrict the processing of their data.
- Prevent their data from being used for direct marketing.
- Be notified about a data breach that concerns their personal data.
- Make a complaint to the ICO.

7.2 Altering or Deleting Data

If an individual needs to alter the data that GC has processed for them, they need to request this in writing. If the data that has been altered has been disclosed to third parties, GC will inform them of the change. GC will then also inform the individual about the third parties with whom the data has been disclosed.

Individuals have the right to request the data that GC holds be deleted. This can be requested if:

- The data is no longer necessary for its original intended purpose.
- The individual withdraws their consent.
- The individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The data was unlawfully processed.
- The data is required to be deleted in order to comply with a legal obligation.

GC can refuse a request to delete data if the data is being processed for the following reasons:

- Exercising the right of freedom of expression and information.
- Complying with a legal obligation, for the performance of a public interest task, or exercising official authority.
- Public health purposes in the public interest.

- Archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- Exercising or defending legal claims.

If any data that has been erased was previously shared with third parties, GC will inform the third party unless it is impossible. If any data that has been erased was previously made public online, GC will inform any other organisation required to erase links and copies of the data in question.

7.3 Restricting data

Individuals have the right to block or suppress GC's processing of their personal data. If processing is restricted, GC will store the data but not process it further, to ensure that enough information about the individual has been retained so restriction is respected.

GC will restrict the processing of personal data when:

- An individual contests the accuracy of the personal data. This is restricted until GC has verified the accuracy of the data.
- An individual has objected to the processing of their personal data. This is restricted until GC has decided whether their legitimate grounds override those of the individual.
- Processing is unlawful and the individual has requested restriction rather than erasure.
- GC no longer needs the data, but the individual requires the data for a legal claim.

If any data which has been restricted was previously disclosed to third parties, GC will inform them about the restriction unless impossible to do so.

GC will inform individuals in writing when a restriction on processing has been lifted.

7.4 Objecting

Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest.
- Direct Marketing.
- Processing for purposes of scientific or historical research and statistics.

If the personal data is being processed for the performance of a legal task or legitimate interests, an individual's grounds for objecting must relate to their particular situation. GC will stop processing the individual's data unless the processing is for the establishment, exercise or defence of legal claims or, if GC can demonstrate compelling legitimate grounds to continue processing, which overrides the individual's interests, rights and freedoms.

If the personal data is being processed for direct marketing purposes, GC cannot refuse any objection regarding data used for marketing, and will stop processing personal data used for this purpose immediately.

If the personal data is being processed for research purposes, an individual's grounds for objecting must relate to their particular situation. If the processing of personal data is necessary for the performance of a public interest task, GC is not required to comply with an objection to the processing of the data.

7.5 Photographs and Videos

As part of GC activities, photographs and videos of individuals may be taken. Written consent will be obtained to use these photographs and videos for communication, marketing and promotional materials. For children below the age of 18, this written consent will come from their parents/carers. For individuals aged 18 and above, written consent will come from themselves. GC will ensure that it is known how these photographs and videos may be used and will issue a photo consent form to all participants. GC will not provide any identifiable personal information, such as full names, alongside the photo.

Consent can be refused or withdrawn in writing at any time. If consent is withdrawn, GC will delete the photograph or video and not distribute it further.

GC is not responsible for any photographs or videos that are taken by parents/carers for their own personal use and they are not covered by this policy. GC do ask that photographs and videos with other children are not shared publicly for safeguarding reasons unless agreed upon by all relevant individuals.

7.6 Data Security and Storage of Records

All personal data that GC holds will be kept safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. This is achieved by:

- Keeping all paper-based records that contain personal data, under lock and key when not in use.
- Electronic devices containing personal data, such as laptops and phones, are password-protected and not left unattended.
- If memory sticks are used to store personal information, they will be password-protected and kept under lock and key when not in use.
- Papers containing confidential personal data will not be left anywhere public.
- When circular emails are sent, Blind Carbon Copy (Bcc) will be used so that email addresses are not disclosed to other recipients.

7.7 Personal Data Breaches

GC will make all reasonable endeavours to ensure that there are no personal data breaches. As part of training, the Director will ensure that all staff are made aware of and understand,

what constitutes a data breach. In the unlikely event of a suspected data breach, staff must immediately report the breach to the Director.

The following information will be provided if there is ever a breach:

- The nature of the breach, including an estimate of how many individuals are concerned.
- An explanation of the likely consequences of the breach.
- A description of how the breach will be dealt with, including how any possible adverse effects will be mitigated.

If a breach is likely to result in a high risk of impacting an individual's rights and freedoms, GC will inform the individuals concerned directly in writing. GC will evaluate whether it would be beneficial to notify any relevant third parties who may be able to mitigate the loss to individuals. For example, the police, insurers, and banks. GC will make all reasonable efforts to contain and minimise the impact of any breaches that occur. GC will keep a record of any breaches.

7.7.1 Reporting to the Information Commissioner's Office (ICO)

GC will assess the potential consequences of any data breaches that may occur on a case-by-case basis, and based on the level of seriousness, may report it to the ICO.

If a breach is likely to result in a high risk of impacting an individual's rights and freedoms, the ICO must be informed via their "report a breach" webpage (https://ico.org.uk/for-organisations/report-a-breach/) within 72 hours of when they were first made aware of the breach where feasible. Any report should include:

- A description of the nature of the breach, including the estimated number of individuals and records concerned.
- The name and contact details of the person reporting, ideally the Director of GC.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on any individuals concerned.
- If any or all of the above are not yet known, the report must try to include as much information as possible within the 72 hours. Reports such as these must explain that there is a delay, the reasons for the delay and a timeframe for when the information is expected (which should be as soon as possible).

GC must keep a record of any breaches whether or not they were reported to the ICO. The record for each breach must include the facts, cause, effects, and any actions taken to contain it and prevent further breaches.

7.7.2 Minimising the impact of data breaches

In the case of a data breach, GC will review how it occurred and how it can be stopped from happening again. This will occur as soon as possible after the breach. The review will

include an attempt to identify any trends or patterns requiring action to reduce risks of future breaches.

The below should be considered to try and mitigate the impact of data breaches:

- If sensitive information is accidentally shared with unauthorised individuals via email, the sender must immediately attempt to recall the email as soon as they become aware of the error.
- If the recall is unsuccessful or cannot be confirmed as successful, GC should decide if it is appropriate to contact the unauthorised individuals who received the email and explain that it was an error, and request that they delete the information without sharing, publishing, saving or replicating it. GC must attempt to receive a written response from the unauthorised individuals saying that they have complied with this.
- GC will conduct an internet search to ensure the information has not been made public. If it has, GC will immediately contact the publisher/website administrator to request the removal and detention of the information.
- If any GC staff or affiliated centres, clubs, or organisations are aware they have received personal data in error, they must immediately alert the sender or the Director.

7.8 Data Retention

GC will ensure that personal data is not kept for longer than necessary and is deleted as soon as possible.

GC will dispose of any paper documents confidentially and securely by shredding them. Any electronic memories will be scrubbed clean.

All individuals mentioned in Section 4 will follow the guidance and protocols as set out in Attachment 3.

Attachment 1
Participant Privacy Notice
How We Use Participant Information

This Privacy Notice will set out how GC manages the personal data it uses.

GC collects the following information regarding its participants:

- The individual's name.
- If over the age of 18, the individual's address, email and phone number.
- If below the age of 18, the parent/carer's name, address, email and phone number.
- Any relevant medical information and/or special educational needs information.
- Attendance information (sessions attended, cancellations).
- Any complaint forms.
- Photography consent forms.
- Emergency contact details.

Why do we collect this information?

We use the participant's data:

- To ensure a safe environment.
    - We know who we are expecting at our sessions.
    - Emergency contact details in case anything happens.
    - Complaint forms so we know if we need to adapt our sessions in any way to support the participants.
- To enable efficient communication.
- To assess the quality of our service.
    - Statistics of what were the best sessions.
    - Statistics of how busy we are and how many places are left for each session.

GC holds the legal right to collect and use personal data relating to its participants. The information is collected to meet legal requirements and legitimate interests set out in UK laws regarding GDPR. This includes:

- Consent for GC to use images and videos of participants.
- The legitimate interest of providing a fun and safe environment for participants to enjoy sports.
- Compliance with a legal obligation, for example, safeguarding participants.

Storing Participant's data

GC does not store personal data indefinitely, and data is only stored for as long as is necessary to complete the task for which it was originally collected.

Sharing Participant's Information

We do not share information about our participants with anyone without consent unless the law and our policies allow us to do so, for example, due to safeguarding issues information may be shared with the police.

Decisions on whether GC shares the information with third parties are based on an evaluation of:

- Who is requesting the data?
- Why do they require the data?
- The level and sensitivity of data requested.
- The arrangements in place to store and handle the data.

Participants Requesting Access to Their Personal Data

Participants (and their parents/carers in the case of children) have a legal right to request access to information about them that GC holds. Any request will need to be made in writing to the Director of GC.

They also have the right to:

- Object to processing of any personal data that is likely to cause, or is causing damage or distress.
- Prevent any processing that is for the purpose of direct marketing.
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed.
- Withdraw consent to the processing of any data based on consent.

If participants (and their parents/carers in the case of children) have any concerns about the way we are collecting or using their personal data, they should first raise their concerns with GC.

Attachment 2
Staff Privacy Notice
How We Use Staff Information

This Privacy Notice will set out how GC manages the personal data it uses. It outlines what you can expect when GC collects your information if you are a current staff member or volunteer.

GC will collect the following data from staff:

- Personal Information - name, address, next of kin, National Insurance Number.
    - This is needed for the contract (payroll and tax etc).
- Other characteristics - gender, age, ethnic group.
    - This is only collected if consent has been obtained from the individual.
- Contract Information - start date, hours worked, role, salary.
    - This is needed for the contract (payroll etc).
- Bank Account Details.
    - This is needed for the contract (salary payments).
- Work Absence Information - number of absences, reasons.
    - This is needed for the contract (paying sick pay).
- Qualifications.
    - This is needed to ensure staff are appropriately qualified.
- Records concerning performance management and appraisal.
    - This is needed to ensure staff are working at an appropriate standard.
- References.
    - This is only collected if consent has been obtained from the individual.
- Records of grievances.
    - This is needed to comply with employment law.
- Investigations into breach of terms and conditions of employment.
    - This is needed to comply with employment law.
- Records of disciplinary proceedings.
    - This is needed to comply with employment law.
- Health and Safety records.
    - This is needed to comply with Health and Safety Regulations.
- Photographic ID.
    - This is needed to comply with a legal obligation. GC need to establish the identity of a person working with children in a position of trust.

Why do we collect this information?

We use this information to:

- Perform employment checks, for example, right to work in the UK.
- Review staff performance.
- Monitor absences and maintain sick records in accordance with HR policy.
- Enable staff to be paid.

Failure to provide this information may lead to serious consequences for the staff, including:

- Right to work: failure to provide this will prevent employment with GC. Any employees found to be working illegally could face legal prosecution.
- Tax codes: failure to provide accurate tax codes and National Insurance numbers could lead to delayed payments or overcharging tax.

Collecting this Information

Most of the information that GC collect is mandatory, but some is voluntary. GC will inform staff which information is mandatory and which is voluntary. Third parties will not be contacted to obtain staff members' personal data without their consent.

Storing this Information

GC does not store personal data indefinitely, and data is only stored for as long as is necessary to complete the task for which it was originally collected.

Who has access to staff data?

Access to personnel files is controlled by the Director. If the Director grants permission for another member of staff to see staff files, they will be bound by obligations of confidentiality.

Where necessary, third parties may have access to and may process staff members' personal information. GC places data protection requirements on third-party processors to ensure data is processed in line with staff members' privacy rights. Examples of these types of third parties are:

- Local and relevant authorities.
- Disclosure and Barring Service (DBS).
- Pension Services.
- Trade Unions.

Sharing Staff Information

GC only shares staff information if they have consent. The only exception to this is if the law or our policies require/allow us to share the information without consent.

GC may share staff information with third parties who require it to:

- Conduct research or analysis.
- Produce statistics.
- Provide information, advice or guidance.

Decisions on whether GC shares the information with third parties are based on an evaluation of:

- Who is requesting the data?
- Why do they require the data?

- The level and sensitivity of data requested.
- The arrangements in place to store and handle the data.

Staff Requesting Access to Their Personal Data

Staff have a legal right to request access to information about them that GC holds. Any request will need to be made in writing to the Director of GC.

They also have the right to:

- Object to processing of any personal data that is likely to cause, or is causing damage or distress.
- Prevent any processing that is for the purpose of direct marketing.
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed.
- Withdraw consent to the processing of any data based on consent.

If staff have any concerns about the way we are collecting or using their personal data, they should first raise their concerns with GC.

Attachment 3
Data Retention Guidance and Retention Periods

This guidance applies to all records created, received or maintained by GC.

Records refer to all documents, both hard copy and electronic copy, which facilitate the business carried out by GC and which are thereafter retained for a set period to provide evidence of its transactions and activities. Some records may be permanently preserved for GC's archives.

Safe disposal of records

Any records that have been identified for destruction will be disposed of appropriately. All records containing personal or sensitive information must be disposed of confidentiality and securely using a shredder for any hard copy records.

GC will maintain a list of any records which have been destroyed, and include the name of the person who authorised the destruction and the date the destruction took place.

Retention Periods

The retention periods that GC will follow are outlined below. We outline the retention periods for Participant Records, Staff Records, Health and Safety Records, Administrative Records, and Property Records.

Participant Records

File Description	Are there data protection issues?	Retention Period	Comments
Child protection allegation against a member of staff (including unfounded allegations).	Yes	Until the staff member retires or for 10 years from the date of the allegation. Whichever is the longest.	Used for references, DBS check, and resurfacing. Shred after the retention period.
Policy Documents	No	Until the policy expires.	Archive after the retention period.
Complaint forms	Yes	10 years from the date the complaint was resolved.	Shred after the retention period.
Attendance Registers	Yes	5 years from the date of the register.	Shred after the retention period.
Any other records created in the course of contact with the participants	Yes/no	5 years from the creation of the record.	Review at the end of the retention period and shred if no longer needed.
Parental permission forms	Yes	Until no longer needed. If there were any incidents related to what they permitted for, then keep them for 25 years from the DOB of the child.	Shred after the retention period.

Staff Records

File Description	Are there data protection issues?	Retention Period	Comments
Timesheets, sick pay	Yes	6 years after the current year.	Shred after the retention period.
Staff Personal Files	Yes	10 years after the termination of their employment.	Shred after the retention period.
Interview notes and recruitment records	Yes	1 year after the date of their interview.	Shred after the retention period.
Pre-employment vetting information (eg/ DBS)	No	1 year after the date of the check.	Shred after the retention period.
Disciplinary proceedings	Yes	Dependent on warning. Child protection issue = until the staff member has retired or for 10 years (whichever is longest). Oral warning = for 6 months. 1st written warning = for 6 months. 2nd written warning = for 1 year. Final warning = for 2 years.	Shred after the retention period.
Records relating to accidents/injuries at work	Yes	10 years after the date of the accident.	Shred after the retention period.
Salary cards	Yes	100 years from the last date of employment.	Shred after the retention period.
Maternity Pay Records	Yes	5 years from the current year.	Shred after the retention period.
Records held under retirement benefits schemes	Yes	5 years from the current year.	Shred after the retention period.
Proofs of identity	Yes	May feel necessary to keep a copy of these.	Archive after the retention period.

Health and Safety Records

File Description	Are there data protection issues?	Retention Period	Comments
Accessibility plans		10 years from the current year.	Shred after the retention period.
Accident Reporting	Yes	If relating to an adult, for 10 years from the date of the incident. If relating to a child, for 25 years from the DOB of the child.	Shred after the retention period.
Incident Reports	Yes	20 years from the current year.	Shred after the retention period.
Policy Statements		1 year from the date of expiry.	Shred after the retention period.
Risk Assessments		5 years from the current year, or until needed (whichever is longest)	Shred after the retention period.
Fire Precautions Log Books		10 years from the current year, or until needed (whichever is longest)	Shred after the retention period.

Administrative Records

File Description	Are there data protection issues?	Retention Period	Comments
Employer's Liability Certificate	No	40 years after the closure of GC.	Shred after the retention period.
Inventories of equipment and furniture	No	5 years from the current year or until needed (whichever is longest).	Shred after the retention period.
Circulars	No	1 year from the current year or until needed (whichever is longest).	Shred after the retention period.
Leaflets/brochures	No	5 years from the current year or until needed (whichever is longest).	Shred after the retention period.
Newsletters	No	1 year from the current year or until needed (whichever is longest).	Shred after the retention period.
Annual Accounts, statements	No	6 years from the current year.	Archive after the retention period.
Loans and grants		12 years from the date of the last payment.	Review to see if they need a further retention period. Archive after the retention period.
Contracts		Contracts under seal: 12 years from the contract completion date. Contracts under signature: 6 years from contract completion date. Contracts monitoring records: 2 years from the current year.	Shred after the retention period.
Copy Orders		2 years from the current year.	Shred after the retention period.
Budget Reports		3 years from the current year.	Shred after the retention period.
Invoice and receipts		6 years from the current year.	Shred after the retention period.
Annual budget		6 years from the current year.	Shred after the retention period.

Delivery Documentation		6 years from the current year.	Shred after the retention period.
Debtors' Records		6 years from the current year.	Shred after the retention period.
Service Level Agreements		Until superseded.	Shred after the retention period.
Work Experience Agreements		18 years from the DOB of the child or 5 years from when they start work experience (whichever is longest).	Shred after the retention period.
Claims made against insurance policies	Yes	For property damage: 3 years from when the case was concluded. For personal injury: 6 years from when the case was concluded.	
Training records	Yes	General training records: 2 years from the current year. Certificates etc: 7 years.	

Property Records

File Description	Retention Period	Comments
Title Deeds	Permanent	Archive if the deeds are no longer required.
Plans	Permanent	Retain whilst GC is operational. Archive if no longer required.
Maintainance and contractors	6 years from the current year.	Shred after the retention period.
Leases	6 years from the expiry of the lease.	Shred after the retention period.
Lettings	3 years from the current year.	Shred after the retention period.
Burglary, theft and vandalism reports	6 years from the current year.	Shred after the retention period.
Maintenance log books	10 years from the last entry.	Shred after the retention period.
Contractors' reports	6 years from the current year.	Shred after the retention period.