Legacy Youth Zone
GDPR Policy

Reviewed by Management Team	October 2025
Agreed by the Board	October 2025
Implemented	At date of approval
Next review	October 2026
Dissemination	UKG Team meetings Website and application forms/JDs

Table of Contents

1. Introduction

Legacy Youth Zone is committed to protecting personal data and respecting the rights of the people whose personal data we collect and use (data subjects). This policy explains our responsibilities and how we will comply with the UK GDPR (as amended by the Data Protection Act 2018 and the Data Use and Access Act 2025).

Personal data is defined as that which relates to an identifiable living individual and includes any expression of opinion about that individual. Within Legacy Youth Zone, personal data includes information about job applicants, employees, volunteers, beneficiaries, donors, trustees, such as name and address.

We process personal data to:

1. maintain our contacts held on Salesforce (Legacy's CRM database)
2. recruit, support and manage staff and volunteers
3. safeguard children and young people at risk
4. maintain our HR and financial records
5. recruit and support trustees
6. provide services to our Youth Zones
7. undertake research
8. respond effectively to enquiries and any complaints
9. communicating with our supporters

This policy has been approved by Legacy's Trustees who are responsible for ensuring that we comply with all our legal obligations.

2. The Principles

We are committed to protecting personal data from being misused, shared inappropriately or being inaccurate.

We will ensure all personal data is:

1. processed lawfully, fairly and transparently;
2. collected for specified, explicit and legitimate purposes;
3. adequate, relevant and limited to what is necessary;
4. accurate and kept up to date, where necessary;
5. kept for no longer than is necessary where data subjects are identifiable;
6. processed securely and protected against accidental loss, destruction or damage;
7. processed in keeping with the rights of data subjects regarding their personal data.

Data subjects, including employees, have the:

1. right to be informed about the processing of their personal data;
2. right to rectification if their personal data is inaccurate or incomplete;
3. right of access to their personal data and supplementary information, and the right to confirmation that their personal data is being processed;
4. right to be forgotten by having their personal data deleted or removed on request where there is no compelling for an organisation to continue to process it;
5. right to restrict processing of their personal data, for example, if they consider that processing is unlawful or the data is inaccurate;
6. right to data portability of their personal data for their own purposes (they will be allowed to obtain and reuse their data);
7. right to object to the processing of their personal data for direct marketing, scientific or historical research, or statistical purposes.

These principles are applied in line with the updated definitions and interpretations introduced under the Data Use and Access Act 2025.

3. Application of the Policy

a. The Data Protection Policy applies to:
- successful and unsuccessful applicants, and former applicants (see appendix 3 for the Applicant Privacy Notice)
- current and former employees which includes full time, part-time, sessional, casual employees and contract workers, as well as volunteers
- young people – current and former members as well as visitors
- both manual and electronic records

b. Legacy Youth Zone employees, trustees and volunteers who process personal information are required to read, understand, and comply with this policy. Any individual who breaches the policy may be subject to disciplinary action. If you are unsure about whether anything you plan to do, or are currently doing, may breach this policy you must first speak to the Head of HR.

c. Data subjects of Legacy Youth Zone will have their personal data processed in line with this policy.

d. Organisations, consultants and other third parties appointed to undertake services for Legacy Youth Zone are required to comply with this policy as a condition of their contract. Any breach of the policy will be taken seriously and could result in Legacy Youth Zone terminating the contract.

e. Training will be provided by Legacy Youth Zone, as and when appropriate, for employees, trustees, and volunteers to ensure an understanding of the policy and its application to our work.

4. Personal Data

a. Legacy Youth Zone will collect and process personal data about a wide range of data subjects. This includes data received directly from individuals and from other sources. The personal data processed will be in both electronic and paper form and will include the following:

1. CVs, application forms, shortlisting and interview notes, references, etc. obtained during selection processes
2. terms of employment
3. payroll information including tax, national insurance details and dates of birth
4. emergency contacts
5. health and sickness absence records
6. information about performance
7. details of any disciplinary investigations and proceedings
8. training and development records
9. contact names, addresses, telephone numbers and email addresses
10. visual images
11. personal and demographic information (date of birth, age, gender, nationality, etc.)
12. professional information (organisation, title, Board memberships, connections, employment records, etc.)
13. support services (Looked After Children, Support/Key Workers, etc.)
14. safeguarding records (concerns, disclosures, meetings, etc.)
15. identification numbers
16. biometric data
17. financial information
18. information relating to a member's use of their membership and activities at Legacy Youth Zone

Regarding visits to our website, Legacy Youth Zone may collect the following information:

1. technical information including the internet protocol (IP) address used to connect a computer to the internet
2. user's login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform
3. full Uniform Resource Locators (URL), clickstream to, through and from our website (including date and time), pages viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks and mouse-overs), and methods used to browse away from the page

b. Legacy Youth Zone may also hold special categories of personal data which is considered sensitive personal data and includes information about an individual's race, ethnicity, religion or similar beliefs, trade union membership, health (including physical and mental health), genetic data, biometric data, sexual life, and sexual orientation. This sensitive information may be processed not only to meet Legacy Youth Zone's legal responsibilities but, for example, for purposes of personnel management and administration, suitability for employment and to comply with the Equality Act. The processing of criminal record checks is permissible when recruiting for a role which involves working with children or vulnerable adults.

c. GDPR rules for special category data do not apply to information about criminal allegations, proceedings or convictions. There are separate safeguards for personal data relating to criminal convictions and offences set out in Article 10. Legacy Youth Zone will not hold information relating to criminal proceedings or offences or allegations of offences unless there is a clear lawful basis to process this data such as where is fulfils one of the substantial public interest conditions in relation to the safeguarding of children and of individuals at risk. However, this processing will only ever be carried out by the Safeguarding Lead following legal advice.

5. Processing of Personal Data

Legacy Youth Zone will process personal data lawfully and transparently, providing individuals with an explanation of how and why we process their personal data at the point when the data is collected, as well as when we collect data about them from other sources.

For data to be processed lawfully, at least one of the following legal conditions, as listed in Article 6 of the GDPR, must be met:

1. the processing is necessary for a contract with the data subject;
2. the processing is necessary for Legacy Youth Zone to comply with a legal obligation.
3. the processing is necessary to protect someone's life;
4. the processing is necessary for Legacy Youth Zone to perform a task in the public interest, and the task has a clear basis in law.
5. the processing is necessary for the legitimate interests pursued by Legacy Youth Zone, unless these are overridden by the interests, rights and freedoms of the data subject;
6. if none of the other legal conditions apply, the processing will only be lawful if the data subject has given their clear consent.
7. In some cases, processing may also be based on Recognised Legitimate Interests as outlined in Schedule 1 of the Data Use and Access Act 2025 (e.g. safeguarding, crime prevention, and public interest purposes).

The processing of **special categories of personal data** is only lawful when the conditions above are met, together with one of the extra conditions set out in Article 9 of the GDPR. These include:

1. the processing necessary for carrying out Legacy Youth Zone's obligations under employment and social security and social protection law.

2. the processing is necessary for safeguarding the vital interests (in emergency situations) of an individual and the data subject is incapable of giving consent;
3. the processing is carried out in the course of Legacy Youth Zone's legitimate activities and only relates to individuals we are in regular contact with in connection with our purposes.
4. the processing is necessary for pursuing legal claims;
5. if none of the other legal conditions apply, the processing will only be lawful if the data subject has given their explicit consent.

When personal data is collected directly from an individual, we will refer them to the Legacy Youth Zone's Privacy Policy which explains how their data will be processed, stored, and retained. If personal data about an individual is collected from another source, the data subject will be referred to the Legacy Youth Zone's Privacy Policy and informed (verbally or in writing) about the type and source of the data. Should the data be required to be passed on to another organisation, this information will be provided to the data subject before the data is passed on.

Where processing relates to scientific or archival research, Legacy may rely on 'broad consent' as permitted under the Data Use and Access Act 2025, provided appropriate safeguards are in place.

6. Consent for Processing Data

a. Where none of the legal conditions for processing data apply, and consent is required from the data subject, Legacy Youth Zone will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it. Consent will be specific to each process for which we are requesting consent. Consent can be withdrawn at any time and should this be the case, the processing of the data will stop. Personal data will only be processed for the purposes set out in the Legacy Youth Zone's Privacy Policy or for other purposes specifically permitted by law.

b. Where data is further processed for a compatible purpose (such as research or statistical purposes), Legacy will ensure this complies with the compatibility test under the Data Use and Access Act 2025.

c. Personal data will only be collected and used for the specific purposes described above and Legacy Youth Zone will not collect any more than is required to achieve these purposes.

d. Legacy Youth Zone will ensure that any personal data held is accurate and, where appropriate, kept up to date.

e. Personal data will not be kept longer than is necessary. The data retention guidelines are set out in appendix 1, which cover statutory retention periods, recommended retention periods and retention periods required by Legacy's insurers, **Towergate Insurance**. The detailed conditions and requirements of **Towergate Insurance** are set out in appendix 2 and take precedence over the GDPR requirements for data retention. Legacy Youth Zone's privacy notice for job applicants can be found in appendix 3.

f. Legacy Youth Zone will ensure appropriate measures are in place to keep personal data secure, including protecting it from unauthorised or unlawful processing, or from accidental loss, destruction, or damage.

g. Legacy Youth Zone will keep clear records of our processing activities and of the decisions made concerning personal data.

7. Rights of Data Subjects

Legacy Youth Zone will process personal data in line with the rights of data subjects, including their right to:

1. request access to any personal data held by us (Subject Access Request);
2. ask to have inaccurate personal data changed;
3. restrict processing, in certain circumstances;
4. object to processing, in certain circumstances, including preventing the use of their data for direct marketing;
5. data portability, that is to receive some or all of their data in a format that can easily be used by another person or organisation;
6. withdraw consent when we are relying on consent to process their data;
7. Individuals retain the right not to be subject to a decision based solely on automated processing that has a significant effect on them. Legacy ensures human review and intervention in line with the amendments introduced by the Data Use and Access Act 2025.

8. Direct Marketing

Legacy Youth Zone will comply with the rules set out in the GDPR, the Privacy and Electronic Communications Regulation (PECR) and any laws which may amend or replace the regulations around direct marketing, which means the communication (by any means) of any advertising or marketing material which is directed, or addressed, to individuals. The forms of communication include making contact with data subjects by email, text message, social medial messaging, telephone and post.

Contact made by Legacy Youth Zone to individuals for the purpose of promoting our aims is defined as marketing, and therefore marketing does not need to be selling anything or be advertising a commercial product.

Any direct marketing material sent will identify Legacy Youth Zone as the sender and will clearly set out how data subjects can object to receiving similar communications in the future. Should an individual object to direct marketing, Legacy Youth Zone will stop the direct marketing as soon as possible.

Legitimate impact assessments have been completed, where appropriate.

Legacy will review direct marketing communications in line with forthcoming PECR amendments announced alongside the Data Use and Access Act 2025.

9. Subject Access Requests

Individuals have the right to access their personal data and can make a subject access request verbally or in writing. They have the right to obtain the following:

1. confirmation that Legacy Youth Zone is processing their personal data.
2. a copy of their personal data;
3. other supplementary information which mainly corresponds to the information provided in our Privacy Policy.

Legacy Youth Zone will respond to requests without undue delay and act on valid requests within one month, unless we have reason to, and can lawfully extend the timescale. This can be extended by up to two months in some circumstances. All data subjects' rights will be free of charge unless it is manifestly unfounded or excessive. Further information is set out in appendix 4 and the SAR form can be found in appendix 5. Legacy Youth Zone will follow the ICO guidance on Subject Access Requests (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/.

10. Sharing Information with Other Organisations and Transferring Data

Legacy Youth Zone will only share or transfer personal data where there is a lawful basis and adequate protection. For international transfers, Legacy follows the UK Secretary of State's approved 'adequacy decisions' or appropriate safeguards as outlined in the Data Use and Access Act 2025 ('not materially lower than UK standards').

11. Data Processors

Before appointing a contractor, who will process personal data on behalf of Legacy Youth Zone (a data processor), due diligence checks will be carried out to check the processor will use appropriate measures to ensure the processing will comply with GDPR.

12. Data Protection Impact Statements

Should Legacy Youth Zone plan to carry out any data processing which is likely to result in a high risk, a Data Protection Impact Assessment will be carried out. Any DPIA will be carried out using the ICO's Code of Practice.

Legacy applies a proportionate risk-based approach to DPIAs in accordance with the revised ICO guidance under the Data Use and Access Act 2025.

13. Dealing with Data Protection Breaches

Where employees, trustees or volunteers think that data may have been breached or lost, this must be reported as soon as possible to the Chief Executive. Breaches of personal data will be recorded, whether or not they are reported to the ICO in accordance with the UK GDPR and Data Use and Access Act 2025.

Contact details are:
Name: Myke Catterall
Role: Chief Executive
Email: Myke.Catterall@legacyyouthzone.org

Any data breach which is likely to result in a risk to any person will be reported to the ICO within 72 hours of the breach being reported. In addition, where a breach of personal data may cause a high risk to any individual, we will inform data subjects whose information is affected, without undue delay.

References

- **ICO – "The Data Use and Access Act 2025: What does it mean for organisations?"**
https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/the-data-use-and-access-act-2025-what-does-it-mean-for-organisations/

- **UK Government factsheet on DUAA and UK GDPR/DPA changes**
https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa

Legacy Youth Zone
GDPR Policy

Appendix 1: Data Retention Guidelines

Retention periods remain subject to ICO guidance and updates under the Data Use and Access Act 2025. Legacy will review these annually.

Statutory Retention Periods

Record	Retention Period	Start of Retention Period	Notes
Health & Safety			
Accident books, accident records/reports	3 years	From date of last entry	If the accident involves a child/young adult, then until that person reaches the age of 21
Medical records as specified by COSHH Regulations	40 years	From date of the last entry	
Medical records under the Control of Asbestos at Work Regulations: medical records containing details of employees exposed to asbestos and medical examination certificates	40 years (medical records) 4 years (medical certificates)	From date of the last entry 4 years from date of issue	
Records of tests and examinations of control systems and protective equipment under COSHH Regulations	5 years	From the date on which the tests were carried out	
Finance			
Accounting records	6 years		For Public Limited Companies
Income tax and NI returns, income tax records & correspondence with HMRC	Not less than 3 years	After the end of the financial year to which records relate	
National minimum wage records	3 years	After the end of the pay reference period following the one the records cover	
HR			
Statutory maternity pay records, calculation, certificates (Mat B1) or other medical evidence	3 years	After the end of the tax year in which the maternity period ends	
Salary records (also overtime, bonuses, expenses)	6 years		
Records relating to working time	2 years	From date on which they were made	
Young People			

Records relating to children and young adults	Until the child / young adult reaches the age of 21		

Recommended (non-statutory) Retention Periods (based on the time limits for potential UK tribunal or civil claims)

Record	Retention Period	Start of Retention Period	Notes
Health & Safety			
Assessments under H&S regulations and records of consultations with safety representatives and committees	Permanently		
HR			
Application forms and interview notes for unsuccessful candidates / CV and cover letters	6 to 12 months		
Inland revenue / HMRC approvals	Permanently		
Money purchase details	6 years	After transfer or value taken	Relates to pension schemes
Pension scheme investment policies	12 years	From the end of any benefit payable under the policy	
Parental leave	5 years	From birth/adoption of the child or 18 years if the child receives a disability allowance	
Pensioners' records	12 years	After benefit ceases	
Personnel files and training records (including disciplinary records and working time records)	6 years	After employment ceases	
Redundancy details, calculations of payment, refunds, notification to the Secretary of State	6 years	From the date of redundancy	
Senior executives' records (those on a senior management team)	Permanently	For historical purposes	
Shortlisting notes	6 to 12 months		
Statutory sick pay records, calculations, certificates, self-certificates	6 years	After employment ceases	
Time sheets	2 years	After audit	

Trade union agreements	10 years	After ceasing to be effective	
Equality and Diversity Form	Almost immediately	After data has been recorded	
Governance			
Trust deeds and rules	Permanently		
Trustees' minute books	Permanently		

Required Retention Periods as specified by Artemis Ltd (Legacy Youth Zone's insurance Brokers)

As incidents of abuse may only come to light after a long period of time, the long-term availability of relevant documents and related correspondence is of crucial important should allegations of abuse arise. In order to assist in the handling and defence of claims for abuse and to demonstrate that Legacy Youth Zone is compliant with Artemis Ltd Risk Management Condition, Artemis Ltd requires secure retention of all relevant personnel employment (employees & volunteers) and training records, safeguarding policies and other abuse-incident-related correspondence. Due to the potential for long latency periods, Artemis Ltd, on behalf of our insurers require such records to be kept for no less than 50 years.

Record	Retention Period	Notes
Application forms, all correspondence relevant to the applications including any correspondence in relation to gaps in employment	50 years	
Records that Legacy Youth Zone has obtained suitable references and details of any follow up enquiries carried out	50 years	Does not need to be a copy of the actual reference
Records that Legacy Youth Zone has carried out a suitable check to verify the identity of the applicant including the nature of the check	50 years	Does not need to be copies of passports/drivers licences/etc.
DBS or similar statutory disclosures i.e. DBS certificate reference number and any relevant follow up correspondence for all employees and volunteers for which they are obtained under the recruitment policy	50 years	In accordance with DBS Code of Practice, NOT a copy of the actual certificate
Safeguarding Policy including copies of previous versions; full details of all training delivered in relation to the policy including details of who attended and dates attended	50 years	
Records of abuse allegations or incidents and action taken including notifications to the appropriate authorities: • Record of all know abuse allegations and incidents • Details of the outcome of any investigation & any follow-up action taken by Legacy Youth Zone	50 years	

• Details of any notification made to relevant authorities; this could include Police, DBS and local safeguarding boards		
Copies of relevant information and accompanying correspondence relating to abuse, assault or molestation of or by Legacy Youth Zone's service users whilst in our care, contained in their referral assessment treatment and care plans	50 years	
Cause for concern forms and other paperwork required under Legacy Youth Zones Safeguarding Policy	50 years	

Appendix 2: Towergate Insurance Risk Management Conditions and Record Retention Requirements

As we know incidents of abuse may only come to light after a long period of time, in some cases as we have seen in the press many years and even decades. The long-term availability of relevant documents and related correspondence is of crucial importance should allegations of abuse arise. Acceptable safeguarding and risk management practices are critical when determining if a risk with exposure to abuse claims is acceptable to us.

In order to assist in the handling and defence of claims for abuse and to demonstrate that the Insured is compliant with our Risk Management Condition, we require secure retention of all relevant personnel employment and training records, safeguarding policies and other abuse-incident-related correspondence. Due to the potential for long latency periods, in most cases, we require such records to be kept for no less than 50 years.

Why do we use a Safeguarding Questionnaire and Risk Management Condition?
We provide some of the widest cover available in the market for abuse. To make this possible we must take a robust approach to risk selection and risk management. The Safeguarding Questionnaire aids us with risk selection. The condition reinforces this by making adherence to certain safeguarding practices part of the policy conditions.

Why do we have record keeping requirements?
The reasons we require certain records to be retained are:

1. They will provide evidence of compliance with our Risk Management Condition; this is a condition precedent to liability so compliance will ensure the policy responds to a claim.
2. They will allow us to verify whether or not the alleged perpetrator(s) was employed or otherwise engaged with the Insured at the relevant time and defend possible false claims.
3. They will assist in defence of abuse claims
4. They will secure vital evidence in situations where allegations are made many years after the abuse when key witnesses may be deceased or otherwise untraceable.

We therefore consider the 50-year retention requirement embodies a legitimate purpose, intended to benefit the Insured as well as Ecclesiastical, and is based upon our experience as to the longevity of some abuse claim notifications.

The Insured will be aware from the many high-profile cases in the news that abuse allegations may be subject to media attention. The document retention requirements are not purely for the benefit of **Towergate Insurance** – if we are able to provide a defence to liability claims this will also help to defend the Insured's **reputation** in the event of abuse allegations. Failing to securely retain records will prejudice our ability to defend a claim which will in turn jeopardise the personal and professional reputations of those involved.

Which specific records are required to be retained?
The Risk Management Condition contains the requirement that the Insured securely retain certain records for a period of at least 50 years. The following provides some explanation of the specific records we are asking to be retained:

a) Employment engagement applications, references, identity verification records, Disclosure and Barring Service or similar	• Copies of the original application forms, all correspondence relevant to the application including any correspondence in relation to gaps in employment. • A record that the Insured has obtained suitable references and details of any follow up enquiries carried out. This does not need to

statutory disclosure, reference numbers, pertinent related correspondence in respect of all of YOUR personnel	be a copy of the actual reference as this will often contain personal information of other individuals/organisations. • A record that the Insured has carried out a suitable check to verify the identity of the applicant including the nature of the check. This does not need to be copies of passports/drivers' licences/birth certs/etc. • DBS or similar statutory disclosures - We only require the Insured to retain details that are in accordance with DBS Code of Practice. This means they retain the certificate reference number and any relevant follow up correspondence only; NOT a copy of the actual certificate. • The Insured should retain details mentioned above for all employees or volunteers for which they are obtained as part of their recruitment policy.
b) YOUR protection policy and revisions thereof together with records of YOUR protection policy training delivered to all of YOUR relevant personnel	• Copies of the protection policy including copies of previous versions. • Full details of all training delivered in relation to protection policy including details of who attended and dates attended.
c) YOUR records of abuse allegations or incidents and action taken including notifications to the appropriate authorities	• Record of all known abuse allegations and incidents. • Details of the outcome of any investigation and any follow up action taken by the Insured. • Details of any notification made to relevant authorities. This could include Police, DBS, CQC, Ofsted, professional bodies and local safeguarding boards.
d) Copies of relevant information and accompanying correspondence relating to abuse assault or molestation of or by YOUR service users whilst in YOUR care contained in their referral assessment treatment and care plans	• This means in circumstances where there has been abuse of, or by, service users whilst in the Insured's care. • We only need them to retain relevant information contained in referral assessments and care plans for those service users involved in known abuse circumstances. What is relevant will be case specific so should be left to the Insured to make the judgement call. • We are not expecting them to retain these records where service users have not been subject of abuse or carried out abuse whilst in the Insured's care.

Does the 50-year retention requirement breach the Data Protection Act?

Concerns are often raised that by complying with our record retention requirements they will be in contravention of the Data Protection Act 1998 (DPA). This is incorrect. To be sure on this point, **Towergate Insurance** has obtained the specific advice of the Information Commissioners Office (ICO) which states that our requirements are in line with DPA rules.

The DPA contains eight personal data protection 'principles'; two of which are principally relevant here:

1. DPA Principle 3 states that: "*personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed*"
2. DPA Principle 5 states: "*personal data shall not be kept for longer than is necessary for that purpose or those purposes*"

The information that we ask to be retained is only that information that may be used in the handling and defence of a claim and as such ***we regard it as relevant and not excessive*** for that purpose. Therefore, the requirements are not in breach of the DPA. *For the legislative guidance please see here:* http://www.legislation.gov.uk/ukpga/1998/29/schedule/1.

As some of the information we require to be retained is regarded as 'personal data' (as defined by the DPA), the Insured will need to treat it in accordance with their DPA responsibilities. These responsibilities include informing data subjects that their information is being retained; keeping it secure; and not transferring it overseas unless adequate provisions are in place. The individuals concerned should be notified that information about them may be held for a long period of time as part of a safeguarding risk management programme. The Insured could address this by using a general statement in their employment contracts and published service-user/member information literature.

Disclosure & Barring Service – Record retention requirements
The only specific requirement we make in respect of DBS disclosure information is that the Insured retain the ***certificate reference numbers***.

The Risk Management Condition *does not* state that DBS certificates or certificate information need be retained. This is consistent with the DBS Code of Practice relating to disclosure information.

We do make the general statement in our policy condition that the pertinent related correspondence is retained. The Code of Practice is quite specific about the circumstances where disclosure information is permitted to be retained; again we would only expect the Insured to retain information if this is in accordance with the Code of Practice or indeed any other statutory provision, such as the Data Protection Act.

For the Code of Practice for DBS Registered Persons see here:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/474742/Code_of_Practice_for_Disclosure_and_Barring_Service_Nov_15.pdf

Storage of Records
Policyholders are often understandably concerned about the practical and cost implications of long-term record keeping. Whilst we do not specify the method of storage, clearly it must be in a form which will be accessible in the future if needed. We don't insist that information is kept in hard paper copy and would in fact expect much of it to be stored electronically; such as some form of imaging system. Electronic storage should come at a much lower relative cost.

Contingency Arrangements for Record Retention
The Safeguarding Questionnaire asks the Insured to describe their contingency arrangements for the retention of records in the event they cease to operate/trade. Abuse claims can emerge many years after the alleged incidents took place and the liability of the organisation will certainly not cease if the company/charity is wound up. It therefore remains crucial that long term records are not destroyed or lost in the event that the Insured ceases to operate/trade.
Please note that it is not a specific policy condition that the Insured have a formal arrangement in place for the retention of records. We do not require the Insured to make a formal provision in advance by entering into a contractual arrangement or incurring unnecessary expense. However, we would ask that they make a consideration for this as part of their normal business contingency planning. The generally acceptable methods of storage in these circumstances would be at the office of a solicitor, accountant or at a professional secure storage company.

Appendix 3: Legacy Youth Zones Applicant Privacy Notice

Legacy Youth Zones

As part of any recruitment process, Legacy Youth Zones collects and processes personal data relating to job applicants. Legacy Youth Zones are committed to being transparent about how we collect and use that data and to meeting our data protection obligations.

What information do we collect?
Legacy Youth Zones collects a range of information about you. This includes:

- Your name, address and contact details, including email address and telephone number where this has been supplied on your CV/Cover Letter
- Details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements; where this has been supplied on your CV/Cover Letter
- whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process; where this has been supplied on your CV/Cover Letter
- information about your entitlement to work in the UK; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health, and religion or belief – where this has been supplied

Legacy Youth Zone collects this information in a variety of ways. For example, data might be contained in application forms, CVs, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment, online or face to face.

Legacy Youth Zone will also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks. Legacy Youth Zone will seek information from third parties only once a job offer to you has been made and will inform you that it is doing so.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Why does Legacy Youth Zone process personal data?
Legacy Youth Zone needs to process data to take steps at your request prior to entering into a contract with you. We also need to process your data to enter into a contract with you. In some cases, Legacy Youth Zone needs to process data to ensure that we are complying with our legal obligations. For example, we are required to check a successful applicant's eligibility to work in the UK before employment starts.

Legacy Youth Zone has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. Legacy Youth Zone may also need to process data from job applicants to respond to and defend against legal claims.

Legacy Youth Zone processes health information only if we need to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to carry out our obligations and exercise specific rights in relation to employment.

Where Legacy Youth Zone processes other special categories of data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is for equal opportunities monitoring purposes, but only with the consent of job applicants, which can be withdrawn at any time. For some roles, we are obliged to seek information about criminal convictions and offences. Where this is the case, we do so because it is necessary for it to carry out our obligations and exercise specific rights in relation to employment.

If your application is unsuccessful, Legacy Youth Zone do not habitually keep personal data on file in case there are future employment opportunities for which you may be suited. Nevertheless, if it is so required, Legacy Youth Zone will ask for your consent before we keep your data for this purpose and you are free to withdraw your consent at any time.

Who has access to data?
Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

Legacy Youth Zone will not share your data with third parties, unless your application for employment is successful and we make you an offer of employment. We will then share your data with former employers to obtain references for you, and the Disclosure and Barring Service to obtain necessary criminal records checks. Legacy Youth Zone will not transfer your data outside the European Economic Area.

How does Legacy Youth Zone protect data?
Legacy Youth Zone takes the security of your data seriously. We have internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties, and is stored in a confidential electronic format, or locked physical storage with limited access.

For how long does Legacy Youth Zone keep data?
If your application for employment is unsuccessful, Legacy Youth Zone will hold your data on file for 12 months after the end of the relevant recruitment process. If you request or agree to allow Legacy Youth Zone to keep your personal data on file, we will hold your data on file for a further 12 months for consideration for future employment opportunities. At the end of that period, or once you withdraw your consent, your data is deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. The periods for which your data will be held will be provided to you in an organizational privacy notice.

Your Rights
As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require Legacy Youth Zone to change incorrect or incomplete data;
- require Legacy Youth Zone to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where Legacy Youth Zone is relying on its legitimate interests as the legal ground for processing, you also have the right to request human review of any automated decision that may significantly affect you, as outlined in the Data Use and Access Act 2025.
- ask Legacy Youth Zone to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override Legacy Youth Zone legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact:

Name: Myke Catterall
Role: Chief Executive
Email: Myke.Catterall@legacyyouthzone.org

If you believe that Legacy Youth Zone has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?
You are under no statutory or contractual obligation to provide data to Legacy Youth Zone during the recruitment process. However, if you do not provide the information, we may not be able to process your application properly or at all. You are under no obligation to provide information for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such information.

Appendix 4: Subject Access Requests
Under Article 15 of the GDPR an individual has the right to access the information that Legacy Youth Zone holds about them. Accessing personal data in this way is known as making a subject access request, which can be made in whatever format an individual may wish but for individuals' convenience, the standard Subject Access Request Form (see appendix 5) can be completed and emailed to emma.blakiston@legacyyouthzone.org. Using the form will help Legacy Youth Zone to verify an individual's identity and give a timely and accurate response to their request. There is no charge to make a subject access request, unless the request is manifestly unfounded or excessive.

An individual is entitled:
- to be informed whether their personal data is being processed by Legacy Youth Zone;
- to be sent a copy of their personal data, subject to any applicable exemptions and the removal of other people's personal data as appropriate;
- to other supplementary information which mainly corresponds to the information provided in Legacy Youth Zones Privacy Policy.

Any individual is only entitled to their own personal data, and not to information relating to other people.

On receipt of a Subject Access Request, Legacy Youth Zone will respond to requests without undue delay and act on valid requests within one month, unless there is reason to, and Legacy Youth Zone can lawfully extend the timescale. This can be extended by up to two months in some circumstances.

it is not compulsory to use this form but it will help Legacy Youth Zone to give a timely and accurate response to your subject access request under Article 15 of the GDPR. Please complete the form below and return it be post or email to the contact details below.

Subject Access Request Form

Date	
Name	
Other name(s) by which you have been known (if applicable)	
Address	
Email address	
Preferred response format (post or email)	
Relationship to Legacy Youth Zone	
Description of your request including information to help us locate the personal data you require	