Lifeworks Charity Limited

General Data Protection Policy V7.1 (UK GDPR)

September 2025

Notice to staff using a paper copy of this guidance, the Intranet holds the most recent version of this guidance. Staff must ensure they are using the most recent guidance.

Owner: Operations Manager – Finance and Support Services

Contents		Page
1.0	Introduction	3
2.0	Purpose	3
3.0	Scope	3
4.0	Definitions	3
5.0	Responsibilities	4
6.0	Data Protection Principles	4
7.0	Lawful, fair and transparent processing	5
8.0	Purpose Limitation	5
9.0	Transparency procedures	5
10.0	Data minimisation	6
11.0	Systems – data protection by design & default	6
12.0	Record keeping procedures	6
13.0	Data quality	7
14.0	Information handling procedures	9
15.0	Storage limitation	9
16.0	Storage hard copy data	9
17.0	IT security	10
18.0	Retention schedule and disposal procedures	13
19.0	Destruction of records	13
20.0	Monitoring - Audit monitoring procedures	13
21.0	Data security audit procedures	14
22.0	Audit trail	14
23.0	Breach	14
24.0	Employee awareness training	15
Appendix A	Subject Access Request Procedure (GDPR compliant)	16
Appendix B	Subject Access Request Form	18
Appendix C	Privacy notice - For people that use our services	19
Appendix D	Privacy notice – Job applicants	22
Appendix E	Privacy notice – Lifeworks employees	25
Appendix F	Retention and disposals schedule	28
Appendix G	Incident Reporting Procedure for Breaches – Flow Chart	33
Appendix H	Policy Information Chart	34
	Document Review History	35

1.0 Introduction

1.1. Lifeworks is committed to all aspects of data protection and takes seriously its responsibilities in safekeeping of all records from creation to disposal, including our procedures for sharing information externally.

1.2. We acknowledge our duty and that of our employees, including agency workers under the General Data Protection UK Regulation (UK GDPR).

1.3. We will be open and transparent with those who use our services and those who lawfully act on their behalf and will adhere to our duty of candor responsibilities as outlined in the Health and Social Care Act 2012.

1.4. We are registered with the Information Commissioner's Office as an organisation that processes personal data.

2.0 Purpose

2.1. The purpose our Data Protection Policy is to support the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation.

2.2. This policy assists the Board of Trustees (BoT), staff, volunteers, contractors, and any other people working on behalf of Lifeworks, of their responsibilities in respect of UK GDPR when gathering, using or sharing personal data about individuals. This includes those who use our services, beneficiaries, employees, volunteers, donors, customers, and suppliers.

3.0 Scope

3.1 This policy applies to all personal data processed by Lifeworks, either in hard copy or digital copy, this includes special category data.

3.2 The policy applies to all staff, including temporary staff, agency staff and contractors.

3.3 This policy shall be reviewed at least annually.

4.0 Definitions

4.1 This policy uses the following definitions:

4.1.1 "Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier.

4.1.2 "Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership.

4.1.3 "Criminal offence data" is data which relates to an individual's criminal convictions and offences.

4.1.4 "Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

5.0 Responsibilities

5.1 The Board of Trustees

5.1.1 To have ultimate responsibility for the content of the Data Protection Policy, its implementation and review.

5.2 The Data Controller

5.2.1 To protect Lifeworks and all of its stakeholders from data security risks.

5.2.2 To take responsibility for on-going compliance with this policy.

5.2.3 To monitor compliance with the GDPR and Data Protection Act 2018 and report all incidents to the BoT.

5.2.4 To oversee changes to systems and processes and complete Data Protection Impact Assessments (DPIA) if required.

5.2.5 To liaise with the Information Commissioners Office (ICO).

5.2.6 To complete an annual data protection audit including the NHS requirement of the Data Security and Protection Toolkit submission.

5.2.7 To ensure that all staff receive training appropriate to their job role.

5.2.8 To undertake a review of the policy at least annually.

5.3 Managers' responsibility

5.3.1 To familiarise themselves with the UK GDPR Policy and other associated policies and guidelines.

5.3.2 To ensure that staff are aware of and comply with the UK GDPR Policy and other associated policies and guidelines.

5.3.3 To ensure that all data protection breaches, complaints/allegations are reported to the Data Controller.

5.3.4 To participate in appropriate training relating to UK GDPR.

5.4 Employee responsibility

5.4.1 To familiarise themselves with current UK GDPR policy and other associated policies, procedures, and guidance.

5.4.2 To participate in appropriate training relating to GDPR.

5.4.3 To report any breaches, suspected breaches or near misses in respect of Data Protection legislation.

6.0 Data Protection Principles

6.1 Lifeworks is committed to processing data in accordance with its responsibilities under UK GDPR.

6.2 Article 5 of the GDPR requires that data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7.0 Lawful, fair and transparent processing

7.1 To ensure its processing of data is lawful, fair and transparent, Lifeworks shall maintain a Register of Systems.

7.2 The register of systems shall be reviewed at least annually.

7.3 Subject Access Requests (SAR)

7.3.1 Individuals have the right to access their personal data and any requests made to Lifeworks shall be dealt with in a timely manner, without undue delay and at the latest within one month of receipt. Requests should be made using the guidance available in the SAR request guidance procedure.

7.4 National Data Opt-Out

7.4.1 If the National Data Opt-out applies this is recorded in our Record of Processing Activities (ROPA).

7.4.2 All new processing is assessed to see if the national data opt-out applies.

7.4.3 If any data processing falls within scope of National Data Opt-out, we use MESH to check if any the people that use our services have opted out of data being used for this purpose.

8.0 Purpose Limitation

8.1 We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation.

8.2 We will establish and maintain associated policies for the control and appropriate sharing information with other agencies, taking account all relevant legislation and citizen consent.

8.3 Where consent is required for processing of personal data, we will ensure that informed and explicit consent will be obtained, and documentation is in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time.

8.4 We will ensure that it is easy to withdraw consent.

9.0 Transparency Procedures

9.1 Our privacy notice/s outline to people why we hold their data, the lawful basis for doing so, and their rights in terms of how we process their data.

9.2 Our privacy notices are freely available to all individuals whose data we process and is part of our commitment to transparency and accountability. They satisfy the individual's right to be informed under GDPR.

9.3 Our privacy notices are available:

- For people who make contact with us on-line Lifeworks Privacy Notice - Lifeworks (lifeworks-uk.org).
- For people who use our services, or their representatives at the time we ask them to give us their personal data or receive it from an external source.
- For job applicants – as a part of our application process.
- For employees – at the start of their employment and by logging into our HR portal for subsequent updates.
- By request from Lifeworks Data Controller karendorow@lifeworks-uk.org or by telephone 01803 861062.

9.4 The privacy notices will be reviewed annually and updated as required.

10.0 Data minimisation

10.1 Lifeworks will ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

11.0 Systems - data protection by design and by default

11.1 We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

11.2 We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

11.3 Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA).

11.4 All new systems used for data processing will have data protection built in from the beginning of system change.

11.5 All existing data processing has been recorded on our Record of Processing Activities. Each process is reviewed annually.

11.6 We ensure that by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

11.7 In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for, and we only keep the information for as long as it is

12.0 Record keeping procedures – creation and use of records

12.1 When we create records, we use standardised structures and layouts for the contents of records.

12.2 All records are kept in accessible but protected locations. The location of these records is documented in the Information Asset Register (IAR).

12.3 Through the lifespan of the record, we will:

- For service user records - Ensure documentation reflects the continuum of care and is viewable in chronological order.
- For service user records - Provide a clearly written care plan when care is being delivered by several members of the team, and ensure records are maintained and updated, and shared with those who have a legal basis for seeing the information.
- For all records - Provide staff with guidance and training on the creation and use of records and their legal responsibilities to share and safeguard personal confidential information.
- For all records - Monitor access to the records.

12.4 At any point in the lifespan of the record, the data subject has the right to request that their record is correct. These procedures are detailed in 13.0 Data Quality.

12.5 At any point in the lifespan of the record, the data subject has the right to request the erasure ('Right to be forgotten') of their record in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and processed.
- When the individual withdraws consent.
- When the individual objects to processing and there is no overriding legitimate interest for continuing to process.
- The personal data was unlawfully processed (i.e. in breach of GDPR).
- The personal data has to be erased in order to comply with a legal obligation.

12.6 At any point in the lifespan of the record, the data subject has the right to request access to their data (SAR). See appendix A.

12.7 Records are only retained while they are necessary for the purposes for which they were originally collected. We will ensure that all records are retained and destroyed in-line with Retention & Disposal Procedures. See appendix E.

12.8 At least annually we guarantee that we will audit our record keeping procedures to ensure that they are adequate and continue to keep our records to the highest standards.

13.0 Data quality

13.1 The availability of accurate and timely data is vital for the safety of the people we care for and the safe and responsible running of our organisation. There are procedures in place for ensuring data accuracy and correcting errors. This applies to all of the data which we process either in hardcopy or digital copy, this includes special categories of data.

13.2 Data accuracy procedures demonstrate how we commit to ensuring that we comply with the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17 that we will "maintain securely an accurate, complete and contemporaneous record in respect of each person that uses our services, including a record of the care and treatment provided to the individual and of decisions taken in relation to the care and treatment provided.

13.3 We ensure accuracy in our data in both hardcopy and digital records by making sure all data has the following characteristics:

- Authentic - – i.e. the data is what it claims to be, has been created or sent by the person who said that they created or sent it, and that this was done at the time claimed.
- Reliable - i.e. the data is complete, accurate, has been created close to the time of the activity it records, and has been created by individuals with direct knowledge of the event it records.
- Integrity – i.e. the data is complete and unaltered, it is also protected from being changed or altered by unauthorised persons, any alterations are clearly marked and the person who made them can be identified.
- Useable – i.e. the data can be located when it is required for use and its context is clear in a contemporaneous record.

13.4 The principal purpose of service user records is to record and communicate information about the individual and their care and or educational needs.

13.5 The principal purpose of staff records is to record employment details for payroll and business planning purposes.

13.6 We have implemented a procedure that enables service users and staff to have easy access to their records where appropriate. This is outlined in our Privacy Notice.

13.7 All staff who record information – whether hardcopy or electronic - have a contractual responsibility to ensure that the data is accurate and as complete as possible. This responsibility extends to any system the staff member has access to.

13.8 Procedures for the correction of errors:

- In-line with national legislation, individuals have the right to have access to their personal data which we process and store. Individuals have the right to the rectification of said records in the instance that their records are inaccurate or incomplete.
- Where at all possible, in the instance that we have appropriately shared that individual's records with any third-party we will inform this third-party of the rectification if appropriate.
- In all cases we will respond to a request for rectification within one month. Should the request be complex this may be extended to two months, however, we will inform the individual in writing of the extension and the reasons why it is required within one month.
- To request for records to be rectified contact us with the request for rectification either verbally or in writing. If the rectification is due to the record being incomplete, then the individual should also provide the supplementary information to update the record.
- While we are assessing the request to rectify records, we will restrict processing of the data in question.
- In the instance where the rectification request is refused, the reason will be explained in full and in writing within one month of the original request having been received.
- All requests for rectification must be notified to the Data Protection Lead who will, maintain a log along with outcomes.
- All individuals who have their rectification request refused will be informed of their legal rights to complain to the ICO and to seek a judicial remedy.
- All staff will be informed of this policy in the staff handbook.
- All people who use our services, or their legal representative, will be informed of this policy, as well as their other rights as regards their personal data, prior to using our services.
- In order to process your request for rectification, you might be asked to provide identifying documents so that we can authenticate that it is appropriate for you to update your data.
- Staff are aware that data accuracy and security is a contractual and legislative requirement, and that breach of this policy might result in disciplinary action.

14.0 Information handling procedures

14.1 Information handling procedures ensure that personal information is protected and that it is not disclosed inappropriately, either by accident or design, whilst in use or when it is being transferred.

14.2 In line with legislation, personal information is not processed without a lawful basis being identified. The Record of Processing Activities (ROPA) records all processing of personal data and identifies the legal basis for it being processed.

14.3 These procedures cover all records which contain data or information which can be said to contain personal data whether stored in hardcopy or digitally.

14.4 Guidelines for staff on the secure use of personal information are outlined in the staff handbook.

14.5 We ensure that there are secure points for the receipt of personal information transferred to us and we have applied the following measures to safeguard personal information during receipt and transfer/transit.

14.6 Staff members have been provided with training in verbal communications. They know that they must take appropriate precautions not to reveal confidential information e.g. to avoid being overheard when making a phone call or not to have confidential conversations in public places or open offices. The staff handbook and their training inform them that breach of this procedure may be a disciplinary or legal offense.

14.7 We will ensure that all confidential information we transfer by post or courier is done so as securely as is practicable. All records transferred in this manner are addressed to a named individual and marked “Private and Confidential”. All records which are posted will be done through signed-for delivery so that it is guaranteed that the correct person receives the record.

15.0 Storage limitation

15.1 To ensure that personal data is kept no longer than is necessary, Lifeworks has a Retentions & Destruction schedule for each area in which personal data is processed and review this process annually.

15.2 We consider the retention of what data should/must be retained, for how long, and why.

16.0 Storage of hard copy data

16.1 We ensure that there are secure points for the receipt of personal information transferred to us and we have applied the following measures to safeguard personal information during receipt and transfer:

- We operate a clear desk policy; hard copy personal data is kept in lockable cupboards and keys are stored securely.
- Staff are not permitted to take hard copy records off-site that contains personal sensitive data without prior authorisation from a senior manager.
- Where data is taken off-site it must not be left unattended outside of a lockable cupboard.
- Records for people who use our services and employee personal records must be segregated from that of others, i.e. individual files will be held for each individual.
- Hard copy personal data that is still required under retention scales but no longer in use will be stored externally in local storage facilities operated by an ISO accredited company.
- Visitors are not left unattended whilst on-site.

17.0 IT Security

17.1 Cloud storage

17.1.1 The majority of our files are stored by Microsoft 365 and accessed through SharePoint and OneDrive. Keeping our cloud storage secure is a complex task and requires time, resource and specialist knowledge. To support us in this we have an agreement in place with an accredited supplier of IT services to help protect against loss of personal data as well as business downtime.

17.1.2 The cloud is protected by two factor authentication when outside of Lifeworks' domains which prevents credentials from being used without a second factor and mitigates the risk of compromised passwords.

17.1.3 Our SharePoint libraries have carefully designed layers of access to ensure only staff who should have access to data are able to see and use different folders. These layers of access are audited each year in the information asset register. Staff have been trained in adding layers of security (such as passwords and editing rights) into sharing links.

17.1.4 Access rights prevent staff accessing data held on the cloud by personal devices.

17.2 IT hardware

17.2.1 This applies to all electronic devices including those that can be connected to a computer via wi-fi or cable.

17.2.2 We issue the appropriate devices that enable staff to perform their role, staff are not permitted to use their own devices for work purposes.

17.2.3 All devices are security marked with asset ID stickers and are logged on the assets record.

17.2.4 Staff are required to sign for all devices allocated to them and a log is maintained.

17.2.5 The line manager is responsible for collecting in all devices including cables as per the individual record for all staff leaving our employment.

17.2.6 All laptops are encrypted as standard.

17.2.7 All Computers must have strong passwords, which include letters and symbols as well as numbers.

17.2.8 Password protected screen savers are installed on all computers, in addition staff must lock their screens when leaving computers unattended in the workplace.

17.2.9 All portable devices must be authorised for use by the data controller and will be protected by either a PIN or password, (dependent on the type of device).

17.2.10 Only encrypted data may be downloaded to portable storage devices.

17.2.11 Back up devices must be locked away securely when not in use.

17.2.12 Printing of confidential documents must not be sent to shared printers/photocopiers unless pass code security measures are in place.

17.2.13 Scans of confidential documents must only be sent to Lifeworks personal secure mailboxes and not shared.

17.2.14 Downloading of Lifeworks documents onto personal devices is strictly prohibited.

17.3 **iPhones**

17.3.1 Where fingerprint recognition is available this must be used.

17.3.2 Data held on iPhones will be automatically wiped following nine unsuccessful login attempts.

17.3.3 Staff are not permitted to redirect calls from their company phone to their personal mobile number.

17.3.4 Cameras on phones are not generally permitted and will be automatically disabled. Where this is permitted appropriate arrangements will be made.

17.3.5 Work emails may be synchronised with work iPhones.

17.3.6 Staff are not permitted to synchronize work emails with their personal iPhone.

17.3.7 Lost or stolen devices may be found by signing in to https://www.icloud.com/#find or by using the Find My iPhone app from another iPhone, iPad, or iPod touch. Open Find My iPhone to select a device and view its location on a map.

17.4 **Software security measurers**

17.4.1 Anti-virus and anti-malware - Anti-virus or anti-malware products regularly scan our network to prevent or detect threats. These products are kept up to date.

17.4.2 Intrusion defence - A well configured firewall is in place to stop any breaches happening before they penetrate deep into our network.

17.4.3 There is restricted access to our systems. Each user has their own username and there are a limited number of failed login attempts.

17.4.4 Permissions and access rights are reviewed periodically, at least annually.

17.4.5 The use of unapproved software is prohibited on all Lifeworks devices.

17.5 **Access controls**

17.5.1 Lifeworks enforces the need for strong passwords, staff should avoid using predictable passwords such as date of birth, family name or pet's names.

17.5.2 Passwords must not be shared, be aware that you are not observed when logging into PC's, Laptops and software.

17.5.3 Different passwords for personal use and work.

17.5.4 Reusing passwords is risky.

17.5.5 The use of memorable information when creating your password is the most secure but if you do need to write your password down, don't leave it on your computer or desk. Make sure any written passwords are stored somewhere that's secret or locked.

17.5.6 When logging in make sure that no one can observe your password (this includes the people who use our services).

17.5.7 Passwords or other access are cancelled immediately when a staff member leaves the organisation, it may also be necessary to do this when a staff member is absent/going to be absent for a prolonged period.

17.5.8 If you feel that your password has been compromised, then please change your password immediately and inform the Lifeworks Data Controller karendorow@lifeworks-uk.org.

17.6 **Email and internet**

17.6.1 Sending of emails between Lifeworks' email accounts is secure.

17.6.2 Sending emails containing sensitive personal information to external accounts should be sent using encrypted software such as Egress Switch.

17.6.3 Staff should not connect to unknown Wi-Fi Hotspots i.e. hotels, coffee shops or public transport.

17.7 **Phishing**

17.7.1 Cyber criminals may contact you via email, text, phone call or via social media. They will often pretend to be someone (or an organisation) you trust. It used to be easier to spot scams. They might contain bad spelling or grammar, come from an unusual email address, or feature imagery or design that feels 'off'. But scams are getting smarter and some even fool the experts.

17.7.2 Criminals are increasingly using QR codes within phishing emails to trick users into visiting scam websites. As we explain, QR codes are usually safe to use in pubs and restaurants, but you should be wary of scanning QR codes within emails.

17.7.3 Scammers try to quickly gain your trust. They aim to pressure you into acting without thinking. If a message or call makes you suspicious, stop, break the contact, and consider the language it uses. Scams often feature one or more of these tell-tale signs:

- Authority - Is the message claiming to be from someone official? For example, the CEO, your bank, doctor, a solicitor, or a government department. Criminals often pretend to be important people or organisations to trick you into doing what they want.
- Urgency - Are you told you have a limited time to respond (such as 'within 24 hours' or 'immediately')? Criminals often threaten you with fines or other negative consequences.
- Scarcity - Is the message offering something in short supply, like concert tickets, money or a cure for medical conditions? Fear of missing out on a good deal or opportunity can make you respond quickly.
- Current events - Are you expecting to see a message like this? Criminals often exploit current news stories, big events or specific times of year (like tax reporting) to make their scam seem more relevant to you.

17.7.4 How to check if a message is genuine - If you have any doubts about a message, contact the organisation directly. Don't use the numbers or address in the message – use the details from their official website.

17.7.5 Remember, your bank (or any other official source) will never ask you to supply personal information via email or call and ask you to confirm your bank account details. If you suspect someone is not who they claim to be, hang up and contact the organisation directly. If you have paper statements or a credit card from the organisation, official contact details are often written on them.

17.7.6 All Phishing emails must be reported to the Head of Data Protection.

18.0 Retention schedule and disposal procedures

18.1 Records should be kept for as long as they are needed to meet the operational needs of the Authority, together with legal and regulatory requirements.

18.2 We will assess our records to:

- Determine their value as a source of information, its operations, relationships and environment.
- Assess their importance as evidence of business activities and decisions.
- Establish whether there are any legal or regulatory retention requirements in respect of the General Data Protection Regulation Act 2018.

18.3 A disposal schedule is a key document in the management of records and information. It is a list of series or collections of records for which predetermined periods of retention have been agreed. (See appendix E).

18.4 Records on disposal schedules will fall into two categories:

- Destroy after an agreed period – where the useful life of a series or collection of records can be easily predetermined (for example, destroy after 6 years; destroy 3 years after the end of the financial year).
- Review - is the examination of closed records to determine whether they should be destroyed, retained for a further period or transferred to an archive for permanent preservation.

18.5 Duplicate records should be destroyed and where information has been regularly shared between business areas, only the original records should be retained if required.

19.0 Destruction of records

19.1 **Hard copy records:**

- Hard copy records of a none-sensitive nature can be placed in a normal rubbish bin.
- If they contain sensitive or highly sensitive information, they should be shredded on-site or transferred for destruction using the Lifeworks appointed contractor for disposal of sensitive material.

19.2 **Electronic records**

- Electronic records of a non-sensitive nature can simply be deleted.
- Lifeworks encourages regular IT cleansing to ensure records/duplicate records are not retained for longer than necessary.
- Emails will be retained for a maximum of 12-month; after such time they will automatically be deleted from our systems.
- Disposal of IT hard drives is undertaken by a British Standard or ISO accredited destruction service via our IT support services contractor.

20.0 Audit monitoring procedures.

20.1 The management of digital access rights is subject to regular compliance checks to ensure that these procedures are being followed and that staff are complying with their duty to use their access rights in an appropriate manner.

20.1.1 Areas considered in the compliance check include whether:

- The allocation of administrator rights is restricted.
- Access rights are regularly reviewed.

- Whether there is any evidence of staff sharing their access rights; staff should know that this can result in disciplinary procedures.
- Staff are appropriately logging out of the system.
- The password policy is being followed.
- Staff understand how to report any security breaches.

21.0 Data security audit procedures

21.1 Record systems: the purpose being to discover whether confidentiality has been breached, or put at risk through deliberate misuse of systems, or as a result of insufficient controls. How frequently information is audited can vary, but as a minimum there should be a full annual audit.

21.2 Confidentiality audits will focus on controls within electronic records management systems and paper.

21.3 Sample audit checks to ensure the GDPR policy is being adhered to by conducting unannounced spot checks.

22.0 Audit trail

22.1 You do not need to document the disposal of records which have been listed on the records retention schedule.

22.2 Documents disposed outside of the schedule either by being disposed of earlier or kept for longer than listed will need to be recorded for audit purposes.

22.3 This will provide an audit trail for any inspections conducted by the Information Commissioner.

23.0 Breach

23.1 Assessing the risk - in the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Lifeworks will promptly assess any risks associated with the breach. In particular, we will assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.

23.2 Notification - we will be clear about who needs to be notified and why.

23.2.1 Lifeworks will as a matter of course immediately notify purchasers if there are any security incidents.

23.2.2 The GDPR introduces a duty on all organisations to report certain types of personal data breach to the ICO. You must do this within 72 hours of becoming aware of the breach, even if all of the information is not yet available. To report a breach please follow the following link. https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/.

23.2.3 If a breach is likely to result in a substantial risk to the rights and freedoms of individuals, Lifeworks staff must inform those concerned directly and without undue delay. In other words, this will take place as soon as possible (prior to informing the ICO) to help mitigate immediate risk of damage and to help individuals take steps to protect themselves from the effects of the breach.

23.2.4 Other regulatory bodies such as OFSTED, CQC, and the police.

23.3 Containment and recovery – the response to the incident should include a recovery plan and,

where necessary, procedures for damage limitation.

23.4 Evaluation and response – any breach will be investigated to establish the cause and also to evaluate the effectiveness of our response.

23.5 All breaches must be reported internally using the procedures set out in the Incident Reporting Procedures Flowchart (Appendix F).

NOTIFICATION CONTACTS
Notification for Devon County Council is via KeepDevonSafe@devon.gov.uk
ICO – Data breach reporting form https://ico.org.uk/for-organisations/report-a-breach/personal- data-breach/
ICO Call for advice Monday to Friday between 9am and 5pm - 0303 123 1113

24.0 Employee awareness and training

24.1 All staff, during induction, are made aware of the organisation's policies and procedures, all of which are used for training updates. All policies and procedures are reviewed and amended where necessary and staff are made aware of any changes. Observations are undertaken to check skills and competencies. Various methods of training are used including one to one, online, workbook, group meetings, individual supervisions and external courses are sourced as required.

24.2 Care staff must read this policy in conjunction with the Confidentiality Policy which provides specific detail in respect of;

- The Caldicott Principles
- Information and Care Needs Assessment
- Handling of Information by Care Workers
- Exceptional Breaches of Confidentiality

24.3 A training needs analysis has been undertaken specifically in relation to Data Protection to identify what training needs to be undertaken by who and how often.

Appendix A

Subject access request procedure (GDPR compliant)

1.0 Introduction

1.1 Under the General Data Protection Regulation (GDPR), you have a right to receive confirmation that an organisation processes your personal data, and also a right to access that data so that you may be aware of it and are able to verify the lawfulness of the processing. The process for doing so is called a subject access request and this sets out the procedure to be undertaken when such a request is made by you regarding data processed about you by Lifeworks.

2.0 What is personal data?

2.1 "Personal data" is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, including your name.

"Special categories of personal data" includes information relating to:

- race
- ethnic origin
- politics
- religion
- genetics
- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation.

3.0 Information you are entitled to

3.1 When you make a subject access request, you will be informed of:

- whether or not your data is processed and the reasons for the processing of your data
- the categories of personal data concerning you
- where your data has been collected from if it was not collected from you
- anyone who your personal data has been disclosed to or will be disclosed to, including anyone outside of the EEA and the safeguards used to ensure data security.
- how long your data is kept for (or how that period is decided)
- your rights in relation to data rectification, erasure, restriction of and objection to processing
- your right to complain to the Information Commissioner if you are of the opinion that your rights have been infringed.
- the reasoning behind any automated decisions taken about you.

4.0 Making a subject access request

4.1 Lifeworks preference is that subject access requests are made using our form. They can also be made in writing, by email or verbally.

4.2 Requests may be made by you personally or by a third party e.g. a solicitor acting on your behalf. We will request evidence that the third party is entitled to act on your behalf if this is not provided at the same time as the request is made.

5.0 Upon receiving a subject access request

5.1 Lifeworks will comply with your request without delay and at the latest within one month unless one of the following applies:

- In some cases, we will be unable to supply certain pieces of information that you have requested. This may be because it is subject to legal privilege or relates to management planning. Where this is the case, Lifeworks will inform you that your request cannot be complied with, and an explanation of the reason will be provided.
- We require extra time because the requests are complex or numerous. In these circumstances, Lifeworks will write to you within one month of receipt of your request to explain why an extension is required. Where an extension is required, information will be provided within three months of the request.

5.2 Before supplying the data (where appropriate) we may contact you asking for proof of identity. You must produce this evidence for your request to be complied with.

5.3 Your request will normally be complied with free of charge. However, we may charge a reasonable fee if the request is manifestly unfounded or excessive, or if it is repetitive. In addition, we may charge a reasonable fee if you request further copies of the same information. The fee charged will be based on the administrative cost of providing the information requested.

6.0 Refusing a request

6.1 Lifeworks may refuse to comply with a subject access request if it is manifestly unfounded or excessive, or if it is repetitive. In these circumstances, we will write to you without undue delay and at the latest within one month of receipt to explain why we are unable to comply. You will be informed of the right to complain to the Information Commissioner and to a judicial remedy.

Appendix B

Subject Access Request Form

Personal details	
Name	
Telephone number	
Email address	
Home address	

Information sought
Please use the space below to describe, in as much detail as possible, the information you wish to have access to. If appropriate, please include any dates relevant to the information sought.

Declaration (if submitting this form for yourself)	
I confirm that I am the person named above and the information requested above is in relation to me. I understand that I may be required to provide evidence to verify my identity.	
Your signature	
Date	

Declaration (if submitting this form on behalf of someone else)	
I confirm that I am acting on behalf of the person named above. I understand that I may be required to provide evidence to verify my identity, and that I have been requested to act on behalf of the person named above.	
Your signature	
Date	

Appendix C

Lifeworks Privacy Notice
For People Who Use Our Services

This notice summarises what personal data Lifeworks Charity Ltd ("Lifeworks", "us" or "we") gathers and hold about people who use our services, prior to, during and afterwards. We are committed to protecting your privacy and being transparent about why we need your personal data and how we process it and what your legal rights are in relation to it. "Processing" can mean collecting, recording, organising, storing, sharing and destroying data.

Lifeworks Charity Ltd is a Charity (Registered Charity No. 1054167) and a Company (Company Registration No. 3177139). We are registered with the Information Commissioners Office (Z7265181)

What is your personal data and how does the law regulate our use of it?

"Personal data" is information relating to you as a living, identifiable individual. We refer to this as "your data". The UK-GDPR (United Kingdom Data Protection Regulation) requires Lifeworks as data controller for your data to:

- Process your data in a lawful, fair and transparent way.
- Only collect your data for explicit and legitimate purposes.
- Only collect data that is relevant and limited to the purpose(s) we have told you about.
- Ensure that your data is accurate and up to date.
- Ensure that your data is only kept as long as necessary for the purpose(s) we have told you about.
- Ensure that appropriate security measures are used to protect your data.

Information about you

So that we can provide safe and professional services we will collect and store personal information about you. Much of this information we hold will have been provided by you, but some may come from external sources, such as previous providers, your local authority and health professionals This personal information may include but is not limited to the following:

- Your name.
- Your address.
- Your date of birth.
- Your next of kin.
- Details of how you pay us or funding arrangements.
- Your likes and dislikes.

Other details about you that you or others provide to us, this personal information may also include special categories of personal information such as:

- Health and care plans.
- Religion.
- Information about your race or ethnicity.

How we use this information

We will collect, share and store your personal information because:

- We have an agreement with you or your local council to provide services.

- It is the law.
- We have to provide information to other organisations that we work with e.g. Ofsted and the Care Quality Commission (the CQC).
- We want to make our support better for you and other people who use our services.

Lifeworks may use your information to:

- Choose the support you may need.
- Keep you safe and healthy.
- Find out what works and what doesn't when it comes to the support you receive.

How we keep your information safe

We will always keep your information private and safe. The only people that will see your information are:

- People with permission.
- People who have the right to see it by law.

People or organisations who may have a legal reason to see your information include:

- Health and Care Professionals such as your GP, social workers, pharmacy.
- Your local authority.
- OFSTED and CQC.
- The police and security services.

We will not share your confidential information for research or planning purposes, with the exception of where there is a legal mandate or overriding public interest.

Your rights under data protection law

You have the following rights under Data Protection Law:

- You can ask to see a copy of the information we have about you.
- If you think the information, we have about you is wrong, or has parts missing, you can ask us to correct it.
- If you think we have information about you that is no longer needed, you can ask us to delete it (but we won't be able to delete it if the law says it is still needed).
- You can ask that we stop some of the ways that we use your information, even if you don't want it to be deleted.
- You can ask us to delete your information by withdrawing consent. Please contact us if you want to do this.
- You can ask not to use information for legitimate interests. (Legitimate interests are when we have a clear reason or goal for doing something.
- If we cannot do what you have asked the Data Protection Officer will explain why.

The lawful basis on which we process your data

The UK-GDPR require that we provide you with information about the lawful basis on which we process your personal data, and for what purpose(s).

The lawful basis for processing your personal data is contained within Article 6 of the UK- GDPR which states:

- The data subject has given consent to the processing of his or her personal data for specific purposes.

- Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Data retention

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

Security

Lifeworks has the following measures in place to protect your data:

- We adopt data collection, storage and processing practices and security measures to protect against unauthorised access, alteration, disclosure or destruction of your personal information.
- Data that we have collected is held on protected devices, including where it is held as part of a back-up version.
- We use layered security software to prevent unauthorised access, alteration, disclosure or destruction of the data. Our security system is subject to regular audit and testing.

How can you contact us about this privacy notice?

You can write to our Data Protection Officer (DPO), Karen Dorow if you have any questions or comments about this Privacy Notice or if you are unhappy about the way we have handled your data.

You may do this yourself or ask someone who supports you to do this for you. Contact details are:

- By email at karendorow@lifeworks-uk.org.
- By phone at 01803 865075.
- By post to: Lifeworks Charity Ltd, Room 33, Lescaze Offices, Shinners Bridge, Dartington, Totnes, Devon TQ9 6JD.

If you wish to make a Subject Access Request in relation to your rights under GDPR, please request our guidance and form using the contact details above.

Appendix D

Lifeworks Privacy Notice For Job Applicants

This notice summarises what personal data Lifeworks Charity Ltd ("Lifeworks", "us" or "we") gathers and hold about job applicants. We are committed to protecting your privacy and being transparent about why we need your personal data and how we process it and what your legal rights are in relation to it. "Processing" can mean collecting, recording, organising, storing, sharing and destroying data.

Lifeworks Charity Ltd is a Charity (Registered Charity No. 1054167) and a Company (Company Registration No. 3177139). We are registered with the Information Commissioners Office (Z7265181)

What is your personal data and how does the law regulate our use of it?

"Personal data" is information relating to you as a living, identifiable individual. We refer to this as "your data". The UK-GDPR (United Kingdom Data Protection Regulation) requires Lifeworks as data controller for your data to:

- Process your data in a lawful, fair and transparent way.
- Only collect your data for explicit and legitimate purposes.
- Only collect data that is relevant and limited to the purpose(s) we have told you about.
- Ensure that your data is accurate and up to date.
- Ensure that your data is only kept as long as necessary for the purpose(s) we have told you about.
- Ensure that appropriate security measures are used to protect your data.

Information about you

As part of our Safer Recruitment processes, we will collect and store personal information about you. Much of this information we hold will have been provided by you, but some may come from third parties, such as previous employers and the Disclosure and Barring Service.

This personal information may include but is not limited to the following:

- Your personal details including your name, address, date of birth, email address, phone numbers.
- Information included on your CV or application including references, education history and employment history.
- Documentation relating to your right to work in the UK.

Other details about you that you or others provide to us, this personal information may also include special categories of personal information such as:

- Health data.
- Criminal conviction data.

Criminal conviction data

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment should you be successful in obtaining employment. We use criminal conviction data in the following ways to assess your suitability to for the role you have applied for.

We rely on the lawful basis of carrying out legally required duties and our legitimate interests.

to process this data.

How we use this information

We need to collect your data to ensure we are complying with legal requirements such as:

- Carrying out checks in relation to your right to work in the UK.
- Conducting DBS checks.
- Making reasonable adjustments for disabled employees.

We also collect data so that we can carry out activities which are in the legitimate interests of the Company. We have set these out below:

- Making decisions about who to offer employment to.
- Assessing training needs.

How we keep your information safe

We will always keep your information private and safe. Your data will only be shared with colleagues within the Company where it is necessary for them to undertake their duties with regard to recruitment.

Your data will be shared with third parties such as the DBS if you are successful in your job application.

Your rights under Data Protection law

You have the following rights under Data Protection Law:

- The right to be informed. This means that we must tell you how we use your data, and this is the purpose of this privacy notice.
- The right of access. You have the right to access the data that we hold on you. To do so, you should make a subject access request.
- The right for any inaccuracies to be corrected. If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it.
- The right to have information deleted. If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it.
- The right to restrict the processing of the data. For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct.
- The right to portability. You may transfer the data that we hold on you for your own purposes
- the right to object to the inclusion of any information. You have the right to object to the way we use your data where we are using it for our legitimate interests.
- The right to regulate any automated decision-making and profiling of personal data. You have a right not to be subject to automated decision making in way that adversely affects your legal rights.

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that may not be able to process your application properly or at all. In some cases, we may continue to use the data where so permitted by having a legitimate or legal reason for doing so.

The lawful basis on which we process your data

The UK-GDPR require that we provide you with information about the lawful basis on which we

process your personal data, and for what purpose(s).

The lawful basis for processing your personal data is contained within Article 6 of the UK- GDPR which states:

- The data subject has given consent to the processing of his or her personal data for specific purposes.
- Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Data retention

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

If your application is successful, your data will be kept and transferred to the systems we administer for employees. We have a separate privacy notice for employees, which will be provided to you.

Security

Lifeworks has the following measures in place to protect your data:

- We adopt data collection, storage and processing practices and security measures to protect against unauthorised access, alteration, disclosure or destruction of your personal information.
- Data that we have collected is held on protected devices, including where it is held as part of a back-up version.
- We use layered security software to prevent unauthorised access, alteration, disclosure or destruction of the data. Our security system is subject to regular audit and testing.

How can you contact us about this privacy notice?

You can write to our Data Protection Officer (DPO), Karen Dorow, if you have any questions or comments about this Privacy Notice or if you are unhappy about the way we have handled your data.

You may do this yourself or ask someone who supports you to do this for you. Contact details are:

- By email at karendorow@lifeworks-uk.org.
- By phone at 01803 861062.
- By post to: Lifeworks Charity Ltd, Room 33, Lescaze Offices, Shinners Bridge, Dartington, Totnes, Devon TQ9 6JD.

If you wish to make a Subject Access Request in relation to your rights under GDPR, please request our guidance and form using the contact details above.

Appendix E

Lifeworks Privacy Notice
For Employees, Agency Staff & Volunteers

Lifeworks Charity Ltd is committed to protecting your privacy online, and to letting you know how we use any personal information that you provide to us. This notice is to explain to you how we may use personal information we collect before, during and after your employment with us.

Lifeworks Charity Ltd is a Charity (Registered Charity No. 1054167) and a Company (Company Registration No. 3177139). We are registered with the Information Commissioners Office (Z7265181)

This notice summarises what personal data Lifeworks Charity Ltd ("Lifeworks", "us" or "we") gathers and hold about its employees, how we use it, how we share it, how long we keep it and what your legal rights are in relation to it.

What is your personal data and how does the law regulate our use of it?

"Personal data" is information relating to you as a living, identifiable individual. We refer to this as "your data". The UK-GDPR (United Kingdom Data Protection Regulation) requires Lifeworks as data controller for your data to:

- Process your data in a lawful, fair and transparent way.
- Only collect your data for explicit and legitimate purposes.
- Only collect data that is relevant and limited to the purpose(s) we have told you about.
- Ensure that your data is accurate and up to date.
- Ensure that your data is only kept as long as necessary for the purpose(s) we have told you about.
- Ensure that appropriate security measures are used to protect your data.

Information about you

We will collect and store personal information from you when you apply to work or volunteer for us. Much of this information we hold will have been provided by you, but some may come from external sources, such as referees. This personal information may include but is not limited to the following:

- Your name.
- Your email address.
- Your address.
- Your phone number.
- Your bank details.
- Your date of birth.
- Your educational and workplace history.
- Your next of kin.
- Your working time records including holidays, sickness and other absence.
- Your training records.
- Your supervision, appraisal, other performance measures.
- Your grievance records.

Other details about you that you or others provide to us, this personal information may also include special categories of personal information such as:

- Medical information.
- Information about disabilities.
- Information about your race or ethnicity.

As an organisation supporting Children and vulnerable adults you may be required to undertake checks through the Data and Barring Service. The outcome of these checks is held on file and must be renewed annually.

How we use this information

Your personal information will only be used by us to:

- Comply with employment law regulations.
- Comply with our Health & Safety and Occupational Health obligations.
- To prevent, detect and prosecute fraud or other crime.
- Where there is a legal requirement such as duty to refer under our safeguarding obligations.
- Regulatory monitoring visits i.e. Ofsted or CQC.

Your rights under data protection law

You have the following rights under Data Protection Law:

- The right to access – You have the right to request us to give you copies of the personal information we have about you.
- The right to rectification – If the information we hold for you is incomplete or wrong, you have the right to request a correction.
- The right to erasure – Where we have no overruling legal basis or legitimate reason to carry on processing your personal information, you may ask that we delete your personal information.
- The right to restrict processing – You have the right to ask that we restrict the processing of your personal information, under certain conditions.
- The right to object to processing – You have the right to object to processing if we can process your information because the processing is part of our public tasks or is in our legitimate interests.
- The right to data portability – This only applies to information you have given us.

Further guidance on your rights is available from the Information Commissioner's Office.

The lawful basis on which we process your data

The UK-GDPR require that we provide you with information about the lawful basis on which we process your personal data, and for what purpose(s).

The lawful basis for processing your personal data is contained within Article 6 of the UK- GDPR which states:

- The data subject has given consent to the processing of his or her personal data for
- one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Sharing your data

We take employee privacy very seriously and adhere to all applicable privacy laws and regulations. We understand that your personal data is important, and we are committed to protecting it. Under this policy, all employee data will be:

- Handled and managed by our designated HR department. Our HR department is trained and knowledgeable in handling sensitive information and will ensure that your data is kept confidential and secure at all times.
- Updated by your line manager who plays a crucial role in ensuring that employee files are kept current and accurate. This includes regularly reviewing and updating relevant information such as supervisions and appraisals. In addition, line managers are responsible for obtaining and documenting any necessary consent from employees before making changes to their files. This includes obtaining consent for any sensitive information and ensuring that all updates are made in accordance with applicable laws and regulations. Furthermore, line managers are expected to maintain the confidentiality of employee files and only share information on a need-to-know basis. Any personal or sensitive information should not be disclosed without prior authorisation from the employee or as required by law.
- In certain circumstances, such as for payroll and benefits administration, your data may also be shared with our designated finance department. However, this will only be done for the purpose of providing you with the necessary compensation and benefits as outlined in your employment contract.
- We may also share your data with external third-party service providers, but only when necessary and with strict confidentiality agreements in place.

Rest assured, your data will not be shared with any other individuals or organisations without your explicit consent, unless required by law or to protect your health in an emergency.

Data retention

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

- If your application for employment or volunteer is unsuccessful, we will retain your application for up to six-months.
- As an employee or volunteer we will retain your records for up to six years after employment.

Security

Lifeworks has the following measures in place to protect your data:

- We adopt data collection, storage and processing practices and security measures to protect against unauthorised access, alteration, disclosure or destruction of your personal information.
- Data that we have collected is held on protected devices, including where it is held as part of a back-up version.
- We use layered security systems to prevent unauthorised access, alteration, disclosure or destruction of the data. Our security system is subject to regular audit and testing.

How can you contact us about this privacy notice?

If you have any questions or comments about this Privacy Notice you may contact our Data Protection Officer (DPO), the Operations Manager – Finance and Support Services. In their absence, Karen Dorow, Charity CEO and College Principal should be contacted:

- By email at karendorow@lifeworks-uk.org.
- By phone at 01803 865075.
- By post to: Lifeworks Charity Ltd, Room 33, Lescaze Offices, Shinners Bridge, Dartington, Totnes, Devon TQ9 6JD.

If you wish to make a Subject Access Request in relation to your rights under GDPR, please request our form using the contact details above.

Appendix F

Retention and Disposals Schedule

CATEGORY	HEADING	DESCRIPTION	RETENTION PERIOD	LEAD	COMMENTS
Governance	BoT	Board meeting papers	6 years	Clerk to the BoT	
Governance	BoT	Board meeting minutes	permanently	Clerk to the BoT	
Governance	BoT	Annual reports	permanently	Clerk to the BoT	
Governance	BoT	Annual reports - background papers	2 years	Clerk to the BoT	
Governance	Policies	Previous version archive		CEO	
Governance	BoT	Risk register	6 years	CEO	
Governance	BoT	Memorandum & Articles	permanently	Clerk to the BoT	
Governance	BoT	Declaration of interests	permanently	Clerk to the BoT	
HR	Recruitment	Application form and interview notes for unsuccessful applicants	6-months	HR Manager	
HR	Recruitment	Application form and interview notes for successful applicants	6-years after employment ends	HR Manager	
HR	Personnel records	Employees & volunteers	6-years after employment ends	HR Manager	
HR	Training records	Employees & volunteers	6-years after employment ends	HR Manager	
HR	Absence	Parental leave	6-years after employment ends	HR Manager	
HR	Redundancy	Calculations of payments, refunds, notification to the Secretary of State	6 years	HR Manager	From date of redundancy

HR	Supervisions & appraisals	Employees	6-years after employment ends	HR Manager	Held on Breathe HR
HR	Concerns about adults	Concerns about behaviour around children	until pension age or for 10 years whichever is longer	HR Manager	NSPCC guidance
HR	Outsourced Payroll – Post August 2025	SSP, SMP, SPP	6 years	HR Manager	Bright Pay / Frost Chartered Accountants
HR	Outsourced Payroll – Post August 2025	HMRC tax & NIC	6 years	HR Manager	Bright Pay / Frost Chartered Accountants
HR	Payroll – Post August 2025	Individual earnings	6 years	HR Manager	Bright Pay / Frost Chartered Accountants
H&S	Accident records/books	Employees & volunteers	3 years from last entry in book	Charity CEO and College Principal	The reporting of injuries, diseases and dangerous occurrences, Regulation 1995 (RIDDOR)
Finance	Payroll – Pre-August 2025	SSP, SMP, SPP	6 years	Operations Manager – Finance and Support Services	Breach of employment claim
Finance	Payroll	Working time records - clockings, absence	2 years	Operations Manager – Finance and Support Services	Astrow
Finance	Payroll – Pre-August 2025	HMRC tax & NIC	6 years	Operations Manager – Finance and Support Services	Sage payroll
Finance	Payroll – Pre-August 2025	Individual earnings	6 years	Operations Manager – Finance and Support Services	Sage payroll

Finance	Accounts	Expense payments	6 years	Operations Manager – Finance and Support Services	
Governance	BoT	Finance reports, budget planning & monitoring	6 years	Operations Manager – Finance and Support Services	
Finance	Accounts	Supplier payments	6 years	Operations Manager – Finance and Support Services	Xero
Finance	Accounts	Customer receipts	6 years	Operations Manager – Finance and Support Services	Xero
Finance	Accounts	Management accounts	6 years	Operations Manager – Finance and Support Services	Excel Reports
Finance	Accounts	Asset and depreciation register	6 years	Operations Manager – Finance and Support Services	after disposal
Finance	Accounts	Capital works projects	6 years	Operations Manager – Finance and Support Services	
Finance	Accounts	ESFA funding	6 years	Operations Manager – Finance and Support Services	
Finance	Accounts	Department for education Capital funding programme	6 years	Operations Manager – Finance and Support Services	

Finance	Fundraising	Grants & trust income	6 years	Operations Manager – Finance and Support Services	
Operations	Marketing & publicity	Photos	as per permissions forms	Operations Manager – Finance and Support Services	
Operations	Education	Education - student records EHCP & safeguarding	25 years	Charity CEO and College Principal	
Operations	Eduaction	Education - student achievement grades	7 years after leaving	Charity CEO and College Principal	
Operations	Social Care	Childrens home - case records	75 years or 15 years from date of death https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/463220/Guide_to_Children_s_Home_Standards_inc_quality_standards_Version1.17_FINAL.pdf	Operations Manager – Finance and Support Services	Regulations 35-39 detail the records that must be kept in children's homes. All children's case records (regulation 36) must be kept up to date and stored securely whilst they remain in the home. Case records must be kept up-to-date and signed and dated by the author of each entry. Children's case records must be kept for 75 years from the date of birth of the child, or if the child dies before the age of 18, for 15 years from the date of his or her death
Operations	Social Care	Adult residential home - individual client file	8 years after leaving the service	Registered Manager	
Operations	Social Care	Staff meeting minutes	3 years	Head of Department	All areas

Operations	Safeguarding	Childrens home	75 years or 15 years from date of death	Operations Manager – Finance and Support Services	Safeguarding incident reports (including missing persaons), referral documents, statutory notifications, investigation documents.
Operations	Medication	MAR charts	75 years or 15 years from date of death	Operations Manager – Finance and Support Services	
Operations	Regulation 44 report		75 years	Operations Manager – Finance and Support Services	Independent visitor report
Operations	Regulation 45 report		75 years	Operations Manager – Finance and Support Services	Internal review RM

Appendix G

Incident Reporting Procedure For Breaches Health & Safety and Data Protection only

Incident Occurrence:

Respond swiftly according to severity of incident ie, first aid, emergency services, securing area, evacuation etc.

Initial Recording:

As soon as it is safe to do so, note down:

- Date & Time
- Person/s involved
- Witnesses
- Photographs where appropriate - preserve evidence

Reporting:

Immediately report headlines (verbally or via email) to Manager and:

- Data Breach - Operations Manager – Finance and Support Services (Charity CEO and College Principal)
- Health & Safety - Operations Manager – Finance and Support Services (Charity CEO and College Principal) NB.This must be done on the same day.
- SLT members to decide if reportable, ie. RIDDOR, ICO
- Operations Manager – Finance and Support Services - Insurance Claims co-ordination

Recording:

- **Health & Safety** - Record any injuries and first aid given in the accident book. Manager to send completed Incident Report Form to LFC within a week and complete the H&S top level report chart.
- **Data Protection** -Manager to send completed Incident Report Form to JP within a week and complete the H&S top level report chart.

  NB. A copy of the incident report should be saved in the Incident Reporting folder in the Health and Safety library.

Investigation:

- Relevant SLT members to lead incident investigations when required.
- HR department to be informed of outcomes where appropriate i.e. injury, absence, disciplinary, insurance claim, litigation.
- Operations Manager – Finance and Support Service to lead with Insurance Claims where appropriate

Review:

Investigation outcomes could inform:

- Risk Assessments
- Policy reviews
- Training
- Future practice

Governance:

- CEO to share H&S & DP Top Level report chart with the Board quarterly.
- Incident forms scrutinised at annual audit

Appendix H

Policy Information Chart

Title	General Data Protection Policy V7.1
Document purpose/summary	To assist employees by providing clear guidance about Data Protection.
Owner	Operations Manager – Finance and Support Services
Policy Department	Data Protection/Security
Ratification date	Sept 2025
Review date and frequency	Annually after publication, or earlier if there is a change in evidence
Consultation process	SLT, Managers
Ratified by	BOT
Target audience	All Lifeworks staff
Circulation	Electronic: Breathe HR Written: Upon request to the Policies Administrator Please contact the Policy Administrator if you require this document in an alternative format.
Equality analysis checklist completed	Yes
References/sources of information	Information Commissioners Office **www.ico.gov.uk** Social Care Assessment Data Protection Toolkit Digital Social Care
Associated documentation/cross referenced policies	Data Retention and Disposals Schedule Privacy Notices Staff Handbook Information Sharing Policy Media Communications and the Use of Images
Supersedes document	V6.0

Executive approval is subject to the understanding that the policy Owner has followed the organisation process for policy ratification.

Document Review History

Version no.	Type of Change: Major, minor, none or taken out of use	Date	Author of change	Description of change
V2.0	Update	May 2018	Head of Finance and Governance	Minor update.
V3.0	Regulatory update	Sept 2020	Head of Finance and Governance	To comply with GDPR.
V4.0	Regulatory update	July 2021	Head of Finance and Governance	Regulatory change following Brexit. To meet requirements of the Social Care Data Protection Toolkit for Impact Assessments and Spot Checks.
V5.0	Complete review	June 2022	Head of Finance and Governance	Section rewrites.
V6.0	Annual review	June 2023	Head of Finance and Governance	Amalgamation of policies and rewrite of sections.
V7.0	Annual review	June 2024	Head of Finance and Governance	Updates.
V7.1	Annual review	June 2024	HR Manager	Minor updates to reflect change in organisational structure