Policies and Procedures:

Data Protection Policy: Members

1. Introduction

Culture, Health and Wellbeing Alliance (CHWA) is committed to being transparent about how we collect and use the personal data of our members, and to meeting our data protection obligations in accordance with UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018.

This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data. This policy applies to the personal data of members.

2. Definitions

“Data” is information which is processed or is intended to form part of a filing system. This applies to electronic or hard copy formats.

“Data Subject” is any identifiable, natural, legal person.

“Members” refers to people who have signed up to the CHWA Mailing List, held by Mailchimp.

"Personal data" is any information that relates to an individual who can be directly or indirectly identified from that information.

“Processing” is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric and genetic data (where used for ID purposes).

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

3. Data protection principles

CHWA processes member-related personal data in accordance with the following data protection principles:

- Personal data is processed lawfully, fairly and in a transparent manner
- Personal data is collected only for specified, explicit and legitimate purposes

- Personal data is processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- Personal data is accurate, and all reasonable steps are taken to ensure that inaccurate personal data is rectified or deleted without delay
- Personal data is kept only for the period necessary for processing
- Appropriate measures are adopted to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

CHWA will update members' personal data promptly if a relevant individual advises that their information has changed or is inaccurate.

4. Types of data held

Personal data gathered from members is held by Mailchimp. The following types of data may be held by CHWA as appropriate, on relevant individuals:

- Name
- Geographic region in which a member works or is based
- Email
- Organisation for which the member works, if relevant

5. Individual rights

As a data subject, a member has a number of rights in relation to their personal data.

Members have the right to be informed about how CHWA processes personal data about them and the reasons for processing.

Subject access requests

Members have the right to access the personal data held on them by CHWA.

Further information on how to request access to personal data is available in Appendix 1.

Other rights

Members have a number of other rights in relation to their personal data.

They can require CHWA to:

- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and

- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

To ask for any of these steps to be taken, the member should send their request to the Executive Director, who should respond within 30 days. If the response to the request is that CHWA will take no action, this will be confirmed to the individual in writing.

6. Data disclosures

CHWA may be required to disclose certain data/information of our members. Such disclosures will only be made when strictly necessary for the purpose.

7. Data security

CHWA takes the security of members' data seriously. There are internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by workers in the proper performance of their duties.

Personal data (special category or not) should only be transferred where it is strictly necessary for the effective running of the organisation.

8. Data monitoring, breaches and decision making

The monitoring of members data will be carried out in accordance with UK GDPR and the Data Protection Act 2018, and only when deemed necessary and justifiable for business purposes.

Privacy Impact Assessments

Some of the processing that CHWA carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the Executive Director will carry out a Privacy Impact Assessment (PIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

If a member discovers that data has been lost or is missing, they should refer to our procedure for reporting data breaches, set out in Appendix 2.

International data transfers

CHWA will not transfer member-related personal data outside of the UK.

Automated decision making

Members have the right not to have decisions made about them solely on the basis of automated decision-making processes where there is no human intervention, where such decisions will have a significant effect on them.

CHWA does not make any decisions based on such processes.

9. Member responsibilities

Member are responsible for helping CHWA keep their personal data up to date. Individuals should let CHWA know if data changes.

10. Implementation, monitoring and review of this policy

CHWA shall review this policy, its implementation and effectiveness every 3 years. The views of all employees and volunteers may be sought and reflected in the review process.

Any new or updated legislation will be considered and reflected in future versions.

This policy was approved and agreed by the Board of Directors on the date shown below.

Signed:	
Name (please print):	Matt Walsh
Position:	Co-Chair of Board of Directors
Date:	3 Mar 2026
Review dates:	Every 3 years from the date above
Organisation name:	Culture, Health & Wellbeing Alliance CIC
Company Number:	12359172

Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Executive Director.

Appendix 1 – Subject Access Request Procedure

1. Introduction

Under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018, individuals have the right to receive confirmation that CHWA processes their personal data, and also a right to access that data so that they are aware of it and are able to verify the lawfulness of the processing. The process for doing so is called a Subject Access Request (SAR), and this document sets out the procedure to be undertaken when such a request is made by an individual regarding data processed about them by CHWA.

What is personal data?

"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 the individual's name. "Special categories of personal data" includes information relating to:

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

2. Procedure

To make a SAR, the relevant individual should complete a Subject Access Request form and send to the Data Controller (Executive Director - currently victoria@culturehealthandwellbeing.org.uk but please check the Who We Are pages on the site for staff) with Subject Access Request in the email heading. Including specific details of the data being requested will enable a more efficient response from us.

On receipt of a Subject Access Request Form, in some cases, we may ask for proof of identification before the request can be processed. The Data Controller will inform the relevant individual if their identity needs verifying and the documents required.

The Data Controller will then confirm:

- whether or not the relevant individual's data is processed and if so why; the categories of personal data concerned and the source of the data if it is not collected from the relevant individual;
- to whom the relevant individual's data is or may be disclosed, including to recipients located in countries outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long the relevant individual's personal data is stored (or how that period is decided);

- the relevant individual's rights to rectification or erasure of data, or to restrict or object to processing;
- the relevant individual's right to complain to the Information Commissioner if they think CHWA has failed to comply with their data protection rights; and
- whether or not CHWA carries out automated decision-making and the logic involved in any such decision-making.

The individual will be provided with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless agreed otherwise. Only personal data relating to the relevant individual who made the request will be released.

CHWA will normally respond to a SAR within a period of one month from the date it is received. In some cases, such as where we process large amounts of the individual's data, we may respond within three months of the date the request is received. The Executive Director will write to the individual within one month of receiving the original request to tell them if this is the case.

We will be unable to supply certain pieces of information, for instance where it is subject to legal privilege or relates to management planning. Where this is the case the Executive Director will write to the individual to inform them that the request cannot be compiled with and give an explanation for the reason.

Relevant individuals must inform the Executive Director immediately if they believe that the data is inaccurate, either as a result of a SAR or otherwise. We will write to the individual within one month of receiving the notification, unless the required correction is complex in which we may respond within three months. If the response is that no action will be taken, we will inform the individual of the reasons for this, and of their right to complain to the Information Commissioner.

In the event that inaccurate data was disclosed to third parties, we will inform the third party of the correction where possible, and also inform the individual of the third parties to whom the data was disclosed.

Refusing a SAR

If a SAR is manifestly unfounded or excessive, or repetitive, we are not obliged to comply with it. If an individual submits a request that is unfounded or excessive, or to which we have already responded, the Data Controller will notify the individual that this is the case and whether or not we will respond to it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. We will inform the individual of their right to complain to the Information Commissioner.

Enforced SARs

Forcing individuals to obtain information about themselves via a SAR, usually in relation to their criminal record, is a criminal offence. No individual will be required to make a SAR to another organisation, e.g. ACRO Criminal Records Office, HM Prison Service, HM Courts and

Tribunal Service or the Crown Prosecution Service, in relation to any aspect of their recruitment, selection or ongoing employment with CHWA.

In the event we require information about an individual's criminal record, we will request this information in accordance with our Safeguarding vulnerable adults and children policy.

Subject Access Request Form

You should complete this form to make a subject access request, which means you are asking CHWA to confirm to you that it processes your personal data, and to obtain access to that data.

Personal details	
Your name:	
Your job title	
Home address:	
Telephone number:	
Email 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.	

Employee declaration	
I confirm that I am the employee 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:	

Appendix 2 – Procedure for reporting data breaches

1. Introduction

CHWA is fully aware of its obligations under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 to process data lawfully and to ensure it is kept securely.

We take these obligations extremely seriously and have protocols in place to ensure that, to the best of our efforts, data is not susceptible to loss or other misuse.

The UK GDPR incorporates a requirement for a personal data breach to be notified to the supervisory authority and in some cases to the affected individuals. This procedure sets out CHWA's stance on taking action in line with UK GDPR if a breach occurs.

2. Personal data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed. A 'breach', for these purposes, is identifiable as a security incident which has affected the confidentiality, integrity or availability of personal data.

As indicated above, a data breach for these purposes is wider in scope than the loss of data. The following are examples of data breaches:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a data controller or data processer
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

Breach detection measures

We have implemented the following measures to assist us in detecting a personal data breach: regular training provision for employees, security monitoring system alerts for unauthorised users or access, robust reporting procedure, data protection agreement with third parties.

We may also become aware of a personal data breach from a member of staff, a CHWA member, a member of the public etc.

Notifiable breaches

For the purposes of this procedure, a data breach will be notifiable when it is deemed by CHWA as likely to pose a risk to people's rights and freedoms. If it does not carry that risk, the breach is not subject to notification although it will be entered on our breach record.

A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

When assessing the likelihood of the risk to people's rights and freedoms, we will consider:

- the type of breach
- the type of data involved including what it reveals about individuals
- how much data is involved
- the individuals involved e.g. how many are involved, how easy it is to identify them etc

- how bad the consequences for the individuals would be and
- the nature of our work and the resultant severity of a breach.

Reporting a breach

If an employee identifies a breach of HR related data, they must inform their line manager immediately, who will refer the matter to the Executive Director. An investigation will be initiated to establish the events leading to the breach and determine what actions should be taken to restrict any consequences. A decision will be taken at that point about whether the breach is deemed notifiable, and whether it is deemed as resulting in a high risk to the rights and freedoms of individuals.

If there has been a breach of HR related personal data that poses a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of discovery. If notification is made beyond this timescale, we will provide reasons for this. If it has not been possible to conduct a full investigation into the breach within 72 hours, an initial notification of the breach will be made within 72 hours, giving as much detail as possible, together with reasons for incomplete notification and an estimated timescale for full notification. The initial notification will be followed up by further communication to the Information Commissioner to submit the remaining information.

The following information will be provided when a breach is notified:

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned and
    - the categories and approximate number of personal data records concerned
- the name and contact details of the Executive Director where more information can be obtained
- a description of the likely consequences of the personal data breach and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

The Police may also be informed if it is found that unauthorised individuals have unlawfully accessed special category data that has been kept securely within the organisation.

If a notifiable breach has occurred which is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals as soon as possible that there has been a breach and provide them with the following information:

- a description of the nature of the breach
- the name and contact details of the Executive Director where more information can be obtained
- a description of the likely consequences of the personal data breach and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

Record of breaches

CHWA will record all personal data breaches regardless of whether they are notifiable or not, as part of our general accountability requirement under UK GDPR and the Data Protection 2018. We will record the facts relating to the breach, its effects and the actions taken.

Appendix 3 - Personal Data Document Retention Periods

Personal data processed must be kept for no longer than is necessary for that purpose or those purposes.

In some cases, the period of time is set out in law as a statutory minimum period, is covered by time limitations for legal claims or informed by practices advised by professional organisations. In other cases it will be a matter of judgement and risk assessment.

CHWA will:

- Document and keep under review the length of time we retain personal or special category data;
- Consider the purpose or purposes for which we hold the data in deciding whether (and for how long) to retain it;
- Retain personal data only if one of the legal bases for processing, as set out in the GDPR, applies;
- Include information about retention periods in our privacy notices that we provide to employees and job applicants when we obtain their personal data, including the period for which the data will be stored, or if it is not possible to specify that, the criteria used to determine the retention period;
- Maintain a record of our data processing activities, including where possible, the envisaged time limits for erasure of the different categories of data;
- Securely delete data that is no longer needed for our identified purposes or for which there is no legal basis for retention; and
- Update, archive or securely delete data if it goes out of date.

Our current document retention schedule is set out below, indicating in each case the basis for our retention period decision.

Key:
CIPD – Chartered Institute of Personnel and Development

CQC – Care Quality Commission

FCA – Financial Conduct Authority

GMC – General Medical Council

HSE – Health and Safety Executive

ICO – Information Commissioner's Office

Limitation incl. EC – The time limits within which a relevant claim may be brought in an employment tribunal, plus the full length of time this may be extended by due to an ACAS early conciliation.

NMC – Nursing and Midwifery Council

Document	Minimum Retention Period	Authority/Justification
Employee Relations		
Application forms and interview notes (for unsuccessful candidates)	6 months to a year	Recommended practice (CIPD) Defamation Act 1996 1-year limitation (in respect of any shared comments)
Applications (successful)	6 months following end of probation period – may retain useful data e.g. skills	Assess and verify suitability for role Limitation incl. EC for unfair dismissal and discrimination claims etc.
Authorised absence records (annual leave, time of for dependents, jury service etc.)	2 years from when the entry was made	Working Time Regulations 1998 Part II
Collective agreements	6 years after ending	Limitation Act 1980 – limitation for breach of contract and negligence
Contracts, offer letters and variations (including any flexible working outcome)	6 years following end of employment	Limitation Act 1980 – limitation for breach of contract
Criminal record checks and disclosures (e.g. a DBS certificate)	6 months from date of receipt of information, or until next CQC/Ofsted inspection date (or longer, in extenuating circumstances, and after discussion with the DBS)	Recommended practice (DBS) The Health and Social Care Act 20018 (Regulated Activities) Regulations 2014
Record of criminal record checks undertaken including; employee name, job title, certificate type, certificate number, date of issue and details of any recruitment decision made	6 years following end of employment	Limitation Act 1980 – limitation for negligence (made by public etc.) Recommended practice (DBS) The Health and Social Care Act 20018 (Regulated Activities) Regulations 2014
Capability and disciplinary documents (substantiated)	2 years following the issue of the warning	TUPE 2006

		Case law permitting expired warnings to be referred to (but not built upon). Unreasonable to refer back after 2 years
Driving licence (if required)	Duration employee drives on business plus 3 years	Limitation Act 1980 – 3-year limitation for negligence for a known act/incident
Driving offences	Remove once the conviction is 'spent' unless subject to exemptions.	Rehabilitation of Offenders Act 1974
Flexible working request documents	18 months following outcome (including any appeal outcome)	12-month statutory embargo on a further request plus 6-month tribunal limitation incl. EC for auto-unfair dismissal and discrimination claims etc.
Grievance documents	6 months following end of employment	Limitation incl. EC for 'last straw' constructive dismissal and discrimination claims etc
Investigations – no case to answer	6 months following conclusion	Limitation incl. EC discrimination claims etc
Maternity medical records	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 as amended
Medical capability documents and records incl. OH reports	6 months following end of employment	Equality Act 2010 Limitation incl. EC for unfair dismissal and discrimination claims etc.
Qualifications	6 years following end of employment	Limitation Act 1980 – limitation for negligence (made by public etc.)
Right to work checks	Two years after employment	Recommended practice (Home Office)
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy	Recommended practice (CIPD) Limitation Act 1980
Redundancy – documentation	6 years following end of redundancy	Limitation Act 1980
References received for employment	6 months following end of probation period	Assess and verify suitability for role Limitation incl. EC for unfair dismissal and discrimination claims etc.
References issued for employment	1 year	Defamation Act 1996 1-year limitation (in respect of any shared comments)

References and correspondence that may produce legal affects (mortgage, loan, etc)	3 years following issue	Limitation Act 1980 – limitation for negligence when immediately aware
Sickness records (see also Statutory Sick Pay below)	6 years Pseudonymise where feasible	Limitation incl. EC for unfair dismissal and discrimination claims etc. Recommended practice (data laws)
Sickness and injury records (work related) (other than those listed under 'Health and Safety')	15 years	3 years for personal injury claim 15 years for negligence (in respect of latent damage) Limitation Act 1980
Subject access request letters	1 year following completion of a request	May charge a fee for repeat copies. May be unreasonable to charge a fee after 12 months.
Trade Union agreements	10 years after ceasing to be effective	Recommended practice (CIPD)
Trust deeds, rules and minute books	Permanently	Recommended practice (CIPD)
Unauthorised absence records	6 months following end of employment	Recommended practice (CIPD)
Whistle-blowing – reports and documents linked to an investigation which is partially or wholly substantiated.	6 months following the outcome of the report or any remedial action taken because of the report	Public Interest Disclosure Act 1998 ('PIDA 1998') Employment Rights Act 1996
Whistle-blowing – documents linked to an entirely unsubstantiated claim	Remove immediately any personal data	Recommended practice (IAPP)
Health and Safety		
Accident books, records and reports	15 years	3 years from last entry (or until person is 21 years old) The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and max. 15 years for negligence (in respect of latent damage) Limitation Act 1980
Assessments under health and safety regulations and records of consultations with safety representatives and	Permanently. COVID-19 risk assessments should be kept as long as they remain relevant	Recommended practice (CIPD)

committees, including COVID-19 risk assessments		
First aid training	6 years after employment	Health and Safety (First-Aid) Regulations 1981
H&S representatives training	5 years after employment	Health & Safety (Consultation with employees) Regulations 1996
H&S training - employees	5 years after employment	H&S Information for Employees Regulations 1989
Health records made in connection with health surveillance (according to HSE)	40 years	Recommended practice (HSE) The Control of Substances Hazardous to Health Regulations 1999 and 2002
Risk assessments including COVID-19 risk assessments	Permanently. COVID-19 risk assessments should be kept as long as they remain relevant	Recommended practice (CIPD)
Statutory and regulatory training	6 years after employment	Limitation Act 1980
Payroll and Finance		
Accounting records	3 years (private company) 6 years (public)	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
Expense accounts	6 years following year end (public companies)	Companies Act 1985, section 222 as modified by the Companies Act 1989 and Companies Act 2006
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended
Inland Revenue/HMRC approvals	Permanently	Recommended practice (CIPD)
National Minimum Wage records	3 years after the end of the pay reference period following the one that the records cover	National Minimum Wage Act 1998
Statutory Maternity Pay records, calculations, certificates (Mat B1s) and leave	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 as amended and Maternity & Parental Leave Regulations 1999
Statutory Adoption Pay records, calculations, matching certificates and leave	3 years after the end of the tax year in which the maternity period ends	Maternity & Parental Leave Regulations 1999

Statutory Paternity Pay records, calculations and leave	3 years after the end of the tax year in which the maternity period ends	Maternity & Parental Leave Regulations 1999
Statutory Shared Parental Pay records, calculations, certificates (Mat B1s), notices and leave	3 years after the end of the tax year in which the maternity period ends	Maternity & Parental Leave Regulations 1999
Statutory Sick Pay (SSP) records, calculations, medical certificates, self-certificates plus COVID-19 related SSP claims including the dates the employee was off sick, which of those dates were qualifying days, the reason reported for absence, the employee's National Insurance number	6 years	Recommended practice (CIPD) to cover range of legislation that may be relevant. There is no longer a statutory retention period but employers must keep sickness records to meet their business needs. For SSP paid because of COVID-19, this can be claimed back from HMRC for 3 years after the end of the tax year; HMRC may request records.
VAT deferral (COVID-19) The government allowed VAT payments due between 20/3/2020 and 30/6/2020 to be deferred until 31/3/2021 (not currently relevant for CHWA)	6 years	HMRC VAT deferral guidance
Wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970
Benefits		
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy however no information should ever be retained unless it is a necessary consequence of the funding	Recommended practice (ICO)
Pension records	12 years after benefit ceases. Avoid access unless required	Recommended practice (CIPD)
Retirement Benefits Schemes – records of notifiable events	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995
Governance		

Entries in documents from incorporation, shareholdings, resolutions, memorandum and articles, annual returns, register of directors' interests, share documents, accounts, liability policies, pension scheme documents etc	Permanently or as per retention period for each document	Recommended practice (CIPD)
Working time		
Timesheets, overtime records and other documents relating to working time (not currently relevant for CHWA)	2 years from date on which they were made	Working Time Regulations 1998 Part II