GDPR – General data protection regulation Policy and Procedure

Policy & Procedure Implementation Checklist

Policy lead:	*Director of Business*
Document author:	*Director of Business*
Version Number:	*3*
Approved by:	*Senior Leadership Team*
Effective from:	*1st August 2024*
Date of next review:	*1st August 2027*
Diversity / Equality Impact Assessment required:	*n/a*
Data protection compliant:	*Yes*
Staff training / update required:	*All staff advised via Staff Newsletter August 2024*

GDPR General Data Protection Regulation Policy Summary

This document describes how BACKUP commits to respecting and protecting the privacy of young people, staff, volunteers and service users:

- *BACKUP will only keep necessary personal data.*
- *BACKUP processes data under legal bases including contractual necessity for employees, provision of health/social care for young people, and legitimate interests for other data.*
- *Individuals have rights to access, rectify, erase, restrict processing, object to processing, and data portability.*
- *The Director of Business serves as BACKUP's Data Protection Officer and is responsible for compliance, monitoring, and handling data protection issues.*
- *BACKUP uses secure servers and restricts access to personal data. They have policies for physical and digital security measures.*
- *Personal data is kept only as long as necessary, with regular reviews and a retention schedule.*
- *Information can be shared in limited circumstances like child safety risks or serious crimes. Otherwise, consent is required to share data.*
- *Extra protections are in place for sensitive data like race, information about health and sexual orientation.*
- *Specific procedures are in place for the handling of data about the young people supported by BACKUP.*
- *There is guidance and separate policy in place governing the use of CCTV within the charity.*
- *Procedures are in place for reporting and handling data breaches.*

The policy aims to ensure BACKUP complies with GDPR and data protection laws while delivering its services and managing employees. It emphasises protecting privacy while allowing necessary data use.

CONTENTS

POLICY

1. Policy Statement

1.1. BACKUP will respect and protect the privacy of young people[1], staff and volunteers and others who access any of the services we offer.

1.2. We will only keep personal data that is required to enable us to offer effective provision of accommodation and support services to young people and the efficient management of services, resources and performance management.

1.3. "Personal data", or "personally identifiable information" (PII) is defined as any data that can be used to identify an individual person, either on its own or in conjunction with other accessible data on that individual. This definition includes digital information (such as an IP address) and can also extend to pseudonymised data, where this can still be linked to an individual.

2. Privacy and dignity

2.1. BACKUP will have in place a separate document outlining its expectations in relation to how staff are to respect the privacy, dignity, independence and choice of all young people.

[1] BACKUP uses the term "*young people*" to refer to the people who need to use its services; as opposed to service users, customers or clients.

PROCEDURE

1. Legislation

1.1. The European Union's General Data Protection Regulation (GDPR) came into force on 25th May 2018 and the UK's Data Protection Act 2018 came into force on the same date. The terms of the GDPR and the Data Protection Act 2018 remain legally applicable to the UK, irrespective of the UK's exit from the European Union.

1.2. The GDPR provides the following rights for individuals in relation to Personal Data or PII:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

1.3. One of the biggest changes introduced by the GDPR is around accountability – a new data protection principle that says organisations are responsible for, and must be able to demonstrate, compliance with the other principles. Although these obligations were implicit in the Data Protection Act 1998 (1998 Act), the GDPR makes them explicit.

1.4. Organisations now need to be proactive about data protection, and evidence the steps they take to meet their obligations and protect the rights of the individual.

1.5. BACKUP is registered with the Information Commissioner's Office (ICO) under registration reference Z7361401. The Director of Business for BACKUP is the Data Protection Officer (DPO).

1.6. Practice covering the processing of personal information in social care is governed by the following legislation and guidance:

- The *Data Protection Acts 1998* and *2018*
- The *General Data Protection Regulation* (GDPR) (Regulation (EU) 2016/679)
- *Data Protection (Processing of Sensitive Personal Data) Order 2000*
- *Freedom of Information Act 2000*
- *Computer Misuse Act 1990*
- *Privacy and Electronic Communications Regulations 2003*
- *Caldicott Recommendations*

- NHS Codes of Practice, including; *Confidentiality: NHS Code of Practice (DOH 2003)*
- *Human Rights Act 1998*
- *Public Records Act 1958*
- *Records Management Code of Practice for Health and Social Care* (DOH, 2016)
- *A Guide to Confidentiality in Health and Social Care* (HSCIC, 2013)
- The HSCIC *Checklist Guidance for Reporting, Managing and Investigation Information Governance and Cyber Security Serious Incidents Requiring Investigation (SIRI)*.

1.7. BACKUP is not required to appoint a DPO under the GDPR but we have decided to do so voluntarily. We understand that the same duties and responsibilities apply had we been required to appoint a DPO. We support our DPO to the same standards.

2. Corporate responsibility for data protection and governance

2.1. Whilst the responsibility for having overall accountability for Information Governance lies with the Trustees of Backup, the DPO has day-to-day responsibility for implementing and monitoring procedures to ensure compliance with relevant legislation and these policies and procedures.

2.2. BACKUP's DPO is the Director of Business.

2.3. When performing their tasks, the DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

2.4. The DPO will be given the required independence and resources to perform their tasks and will not be penalised for performing DPO duties.

2.5. We ensure that any other tasks or duties we assign our DPO do not result in a conflict of interests with their role as a DPO.

2.6. The DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.

2.7. The DPO will produce a regular monitoring report to Trustees on compliance and any data breaches, at least annually.

2.8. The DPO is easily accessible as a point of contact for our employees and all stakeholders on all Data control issues. S/he also acts as a contact point for the ICO where necessary.

2.9. The DPO also advises on the need for a Data Protection Impact Assessment (DPIA) where BACKUP handles personal or sensitive data, or where a new project or development is begun or new technologies are introduced. (See Data Protection: Impact Assessment Policy.)

2.10. BACKUP (In its capacity as, what GDPR refers to as, a 'Controller') will only appoint 'Processors' (e.g. Sub-contractors for functions such as pay roll or HR) who can provide 'sufficient

guarantees' that the requirements of the GDPR will be met and the rights of data subject. An approved code of conduct or certification scheme may be available in the future, but no such schemes have been approved so far. There is a page entitled 'Contracts and liabilities between controllers and processors' on the ICO website for more comprehensive information. (Click here for a Link)

2.11. Where personal data is breached, threatened with a breach or narrowly avoided being breached, the DPO will consider the risk posed to individual(s), considering the likelihood and severity of harm to an individual's rights and freedoms. If this is likely, the DPO will notify the ICO in line with BACKUP's Data Breach Reporting Procedure.

3. The legal bases for processing data

3.1. The GDPR requires data controllers to specify their lawful basis for the processing of personal data. It is no longer permissible to use consent as a legal basis when this is given as a condition for the provision of a service or employment. This is because the consent cannot be regarded as freely given, "where there is a clear imbalance between the data subject and the controller" as exists between BACKUP, its employees and young people.

3.2. BACKUP will, therefore, use the following legal bases for the processing of personal data: -

3.2.1. Pursuant to GDPR Article 6(1)(b) for employees that the processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contact.

3.2.2. Pursuant to GDPR Article 9(2)(h) for young people that the processing is necessary for the provision of health or social care.

3.2.3. For all other information held, e.g. Ex-employee information, we will rely upon legitimate interests of the organisation pursuant to GDPR Article 6(1)(f)

3.3. Article 9 of the GDPR places restrictions on the processing of personal data revealing any of the following:

3.3.1. Racial or ethnic origin

3.3.2. Political opinions

3.3.3. Religious or philosophical beliefs

3.3.4. Trade union membership

3.3.5. Genetic data

3.3.6. Biometric data for the purpose of uniquely identifying a natural person

3.3.7. Data concerning health

3.3.8. Data concerning a natural person's[2] sex life or sexual orientation

3.4. These categories are classed as "special categories of data" that can be processed only if one or more of the following applies:

3.4.1. The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

3.4.2. Processing is necessary for the purposes of carrying out the obligations of and exercising specific rights of the controller or of the data subject in the field of employment

3.4.3. Processing is necessary to protect the vital interests of the data subject (i.e. it is necessary to protect their life) or of another natural person where the data subject is physically or legally incapable of giving consent

3.4.4. Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects

3.4.5. Processing relates to personal data which are manifestly made public by the data subject.

3.4.6. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

3.4.7. Processing is necessary for reasons of substantial public interest

3.4.8. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

3.4.9. Processing is necessary for reasons of public interest in the area of public health.

3.4.10. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

3.5. The special categories of personal data processed by BACKUP on its employees are:

3.5.1. Racial and ethnic origin

3.5.2. Trade union membership

3.5.3. Sex

3.5.4. Sexual orientation

3.6. Wherever employees or young people are asked to disclose data about these special categories of their data, the right to withhold this from BACKUP will be made explicit to them at the point

[2] A human being as distinguished from a person (as a corporation) created by operation of law
Natural person Definition & Meaning | Merriam-Webster Legal

of collection, and the consent to process it will likewise be requested when it has voluntarily been disclosed.

3.7. As an employer committed to the promotion of equal opportunities, BACKUP will request the consent of employees to process information on their sexual orientation, gender identity or expression, should they choose to disclose it. The processing of this information will be for the purposes of promoting equal opportunities. Employees are under no legal or professional obligation, however, to disclose their sexual orientation, gender identity or expression to BACKUP, and their right to privacy in these matters will be respected and upheld[3].

3.8. As a support provider, BACKUP processes a substantial amount of personal information on the young people it supports, recognising that children and vulnerable adults divulge such information to professionals that is often sensitive and painful. Accordingly, BACKUP will ensure that such information is always treated with respect, upholding the individual's right to privacy, their personal dignity and protecting their best interests at all times.

3.9. BACKUP is lawfully permitted to process data on young people pursuant to GDPR Article 9(2)(h) in that it is necessary to do so for the purposes of providing the services for which we are contracted, in order to fulfil our duty of care and to act in the best interests of individuals who may not always have the mental capacity to consent.

3.10. As a necessary component of providing holistic, personalised care services, BACKUP may collect sensitive data on young people; in particular, racial or ethnic origin, political opinions, religious beliefs, data concerning health, and data concerning sex life and/or sexual orientation. What information is processed will vary relative to the identified care needs of each individual. Information that is not relevant to a young person's identified needs will not be recorded.

3.11. There may be exceptional circumstances in which information will need to be shared with other professionals, where the conditions of GDPR Article 9(2)(h) do not apply. For example, when:

- A person's life is considered to be at risk.
- Other people's lives are considered to be at risk.
- It is a requirement of a court order.
- It is a requirement of law.
- It is in the public interest.

These circumstances are covered by Article 6, paragraph 1d and 1e of the GDPR, viz. "vital interests" and "public interest" respectively.

3.12. Any requests for information from an external agency on the grounds of public interest should be treated with care, discussed with the DPO and fully documented. Depending on the nature of the request and the information requested, it may be necessary to arrange a review meeting with the relevant agencies involved.

---

[3] The charity carries out an anonymous survey of all employees once a year, for the purposes of comparing applications for employment to the actual makeup of its staff team. It is not possible to match responses to individuals.

3.13. Where a request for disclosure is made in relation to a serious crime (see paragraph3.14 for how "serious crime" is treated), the following conditions must be satisfied:

- The crime must be sufficiently serious for the public interest in disclosure to prevail over the individual's right to confidentiality.
- It must be established that without the disclosure the task of preventing or detecting the crime would be seriously prejudiced or delayed.

3.14. There is no absolute definition of "serious crime". This policy therefore uses the definition of "serious arrestable offences" given in the Police and Criminal Evidence Act (1984) (section 116). These are offences which have caused or may cause:

- Serious interference with the administration of justice with the regard to the investigation of an offence
- Death
- Serious injury
- Substantial financial loss or gain.

3.15. The disclosure of information to the police in order to comply with BACKUP's 'Alcohol, Legal Highs and Illegal Substances Policy and Procedures', available on the S drive is permissible with or without the expressed permission of the young person. If such information is to be shared this should only be done in consultation with the Director or CEO.

3.16. In the event of a member of staff being made aware of information relating to possible or actual physical, sexual, financial or emotional abuse of children or vulnerable adults, they must report their concerns immediately to their line manager and follow BACKUP's 'Safeguarding Policy and Procedures Children' or BACKUP's 'Safeguarding Policy and Procedures Adults', to which reference should be made in the report. The safety of children and vulnerable adults should always be given the highest priority and should override considerations of confidentiality.

4. Personal data and children

4.1. Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

4.2. An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.

4.3. We design our processing with children in mind from the outset.

4.4. If our processing is likely to result in a high risk to the rights and freedom of children, then a DPIA must be completed by the Project Manager (See Data Protection: Impact Assessment Policy.)

4.5. As a matter of good practice, we take children's views into account when designing our processing.

4.6. We rely upon 'legitimate interests', for processing personal information for children and take responsibility for identifying the risks and consequences of the processing and put age appropriate safeguards in place.

NB: BACKUP only work with clients aged 16 and over.

5. Data processing procedures – young people

5.1. Any employee processing personally identifiable information for BACKUP must ensure that:

5.1.1. Only the minimum necessary personal data is processed

5.1.2. Pseudonymisation is used wherever possible. - "Pseudonymisation" refers to the use of other identifying data in place of individuals' names (such as an employee number) where it is not necessary for that processing activity to disclose names, e.g. for the purposes of compiling reports or statistical information.

5.1.3. Processing is transparent (where feasible, allowing individuals to monitor what is being done with their data)

5.2. Employees must "granularise" sets of personal data pertaining to more than ten individuals when these are being shared in any format (digital or hard copy). Large spreadsheet lists and any other such sets of data should be broken down into smaller units such that any one transfer does not include information on more than ten individuals. This applies even if the data has also been pseudonymised.

5.3. BACKUP will establish individual files for each young person, which the staff supporting the young person are responsible for maintaining.

5.4. Records must be kept up to date and relevant, ensuring that each entry is signed and dated.

5.5. Staff should avoid taking hard copies of any young person's files out of the office; although there may be exceptional circumstances where a young person's files need to be removed. In such cases, the agreement of the Project Manager must be sought before removing files from their usual location. Such instances should be documented by giving the name of the person taking the file, the young person's name and expected date of return.

5.6. If removing a file, copies of the front sheets or 'grab sheets' detailing essential information should be retained, so that staff working with the young person will have access to such information in the event of an emergency. When files are returned to their original location this also must be documented

5.7. The confidentiality of each young person's files must be respected and maintained at all times. Paper files must not be left open on desks or around the office and must be stored in a lockable cabinet when not being used. Digital files must be stored securely in accordance with the BACKUP's 'Information Security Policy' – Section 11 of this document.

5.8. Letters and other information from external agencies (known as “third party information”) should be immediately date stamped and filed after reading. Third party information must be readily accessible to the relevant members of staff and should not be stored in places other than the main case file.

5.9. *Access to a young person’s file is limited to the support worker(s), their line manager or those members of staff who are directly involved in the support of the young person, or to staff involved in the auditing of the service provided*.

5.10. If a young person approaches a reception area or office expressing information of a personal nature, it should be made clear to them that there is a private interview space, if needed, and that personal information does not need to be given in a public area if they are not comfortable doing this.

5.11. Where possible, telephone calls should be passed directly to the member of staff who would most appropriately deal with the enquiry. If this is not possible, then a message should be taken, and passed to the member of staff in question. Where the information is personal this should be placed in an envelope marked ‘Private & Confidential’, dated and signed by the person taking the message. If a call is urgent and the relevant member of staff is not available, brief details should be taken, and then referred to the relevant line manager, or other senior member of staff.

5.12. Young people who phone an office should be made aware that they do not have to give personal information over the phone, especially if they cannot speak to the person dealing with their case.

5.13. If an emergency call comes in for a young person, the person taking the call should take the message and contact the person concerned directly.

5.14. Staff are instructed never to give out a young person’s telephone number(s) or addresses, unless specific consent has been given.

6. Data processing procedures - staff

6.1. Supervision files must be kept in a locked filing cabinet, with access restricted to the line manager, senior managers and relevant administrative staff where appropriate.[4]

6.2. Staff telephone numbers and addresses must not be kept in any accessible phone books or card indexes on view in the scheme or office.

6.3. If an emergency call comes in for a member of staff, the person taking the call should take the message and contact the person concerned directly.

[4] Supervision notes should then be scanned and saved to the individual’s personnel file on the R:drive; in order for the frequency of meetings to be monitored.

6.4. If enquiries are made about a member of staff the enquirer's name should be taken and the member of staff informed.

6.5. Staff are instructed never to give out staff telephone numbers or addresses where there is doubt as to the enquirer's identity, or to whether the individual has consented to their personal information being shared.

6.6. If staff have any doubts as to what action they should take, they should pass the query to their line manager or a member of Business Support during normal office hours, or to the relevant on call or the Out of Hours service at any other time.

6.7. Sick notes are confidential documents and should be handed to a line manager, Business Support, Payroll, or a member of the Human Resources, in a sealed envelope marked "Private & Confidential".

6.8. Enquiries from statutory authorities for information about staff (e.g. Police), should always be referred to a Director or the CEO.

6.9. BACKUP outsources HR to Solutions for HR and Payroll to Ryans Accountants. In line with section 3.10. of this policy we have a written agreement with these suppliers to ensure these functions are legally compliant with data protection legislation and to demonstrate our commitment to information security, transparency and quality assurance, in addition to protecting the rights of individuals with respect to their personal data.

7. Requests for personal data by staff

7.1. As part of BACKUP's induction, all staff members will be given BACKUP's 'Privacy Statement for BACKUP Employees' - appendix (iii) and on the s drive.

7.2. BACKUP is committed to working in an open and honest manner with the young people it supports and its employees. GDPR states data subjects have, "the right of access to [their] personal data...and to exercise that right easily and at reasonable intervals, in order to be made aware of, and verify, the lawfulness of the processing". This right will be protected and upheld for all employees and young people as described below.

7.3. Employees may request to see their personal data that is processed by BACKUP, and to know our reasons for doing so. This is called a "Data subject access request", which an employee can make by submitting a 'Request for a copy of information held on a staff member' (Appendix (iv) or found on the s drive) to the organisation's Data Protection Officer. (Director of Business)

7.4. Information requested by the employee will be provided as soon as possible and no later than one month after the receipt of the form named above. We aim to provide a copy of the data requested within 40 days of the written request. If you have any particular needs, we will endeavour to provide the information you have requested in an accessible format (e.g. providing large print copies for those with sight loss).

7.5. Employees making subject access requests must specify when making their request specifically which items of personal data that they wish to see.

7.6. There will be no charge to the employee for making a subject access request, unless the request is manifestly unfounded, excessive or repetitive, in which case a fee may be charged.

7.7. Employee data contained in Disclosure and Barring Service (DBS) Checks is never kept on an applicant's personnel file and is stored separately and securely in a lockable, not portable, storage cabinet. Access to the cabinet and information stored within is strictly controlled and limited to those who are entitled to access as part of their duties. For further information, please refer to the BACKUP's 'DBS and Management of Ex-offenders Policy' on the S drive.

7.8. Confidential references received by BACKUP are not exempt from data subject access requests. However, in deciding whether to disclose information, it is necessary also to consider the data privacy rights of the referee. Information contained in or about a confidential reference need not be provided if the release of the information would identify an individual referee unless:

- The referee has given his or her consent
- The identity of the referee can be protected by anonymising the information
- It is reasonable in all the circumstances to release the information without consent.

7.9. Even if a referee states that they do not want their comments to be shared, we are obliged to provide the reference to the subject if it is reasonable in all the circumstances to comply with the request without the referee's consent. In considering whether it is reasonable, we should take account of factors such as:

- Whether the referee was given express assurances of confidentiality
- Any relevant reasons the referee gives for withholding consent
- The potential or actual effect of the reference on the individual
- The fact that a reference must be truthful and accurate and that without access to it the individual is not in a position to challenge its accuracy
- That good employment practice suggests that an employee should have already been advised of any weaknesses
- Any risk to the referee.

7.10. BACKUP cannot refuse to disclose information from a confidential reference without giving a reason.

7.11. If disclosure of a reference would identify only the organisation that has given the reference rather than a specific individual, disclosure would not be an issue.

7.12. If a subject access request is received for information contained in a confidential reference that has been sent or received internally, it will be treated in the same way as a reference from an external referee. Internal references are not exempt from data subject access.

8. Requests for personal data by young people

8.1. All young people will be given a copy of BACKUP's 'Approach to confidentiality for young people' - Appendix (i) and on the s drive. They may request to see their personal data and to know the reasons for processing it. This is called a "Data subject access request", which a young person can make by submitting a 'Request for a copy of information held on a young person' available from their Key Worker. (Appendix (ii) or found on the s drive to the organisation's DPO.

8.2. The relevant Manager must be notified whenever a young person requests access to their file. Written copies will normally be arranged within 40 days of the request. A request to read data about them but not take copies can be managed within 5 days of the request. See 8.3 and Appendix (i) In practice we may be able to respond to requests much more quickly. Reasons for delay may include:

- Waiting for a key worker to be on duty.
- Ensuring the young person is suitably prepared.
- Ensuring that someone is available to discuss the contents with the person if necessary.

8.3. A member of staff will remain with the young person while they are reading their file. If any recorded information is challenged by the young person, the information should not be removed but the objection will be recorded and the matter referred to a Director who will take the appropriate action.

8.4. It may not always be possible to disclose to a young person all information kept on file. This particularly applies to third party information (in the event that the agency or individual has not given us permission) or because an individual could be put at risk by sharing information. There may also be some circumstances under which it is not appropriate to disclose some information in a young person's file to the individual concerned, for example when it is possible that this may have a negative impact on that person's mental health or wellbeing.

8.5. If a young person wishes to retain copies of any information this should be agreed, although permission must be granted by the third parties for third party information.

9. Requests for personal data regarding young people

9.1. All information concerning young people is confidential within BACKUP. Information about the young person (however disclosed) may be disclosed to other staff, to the extent needed to enable them to carry out an efficient/effective service to the young person.

9.2. Information about the young person may also be used as part of the Scheme's monitoring process. When this happens, we are normally collating data e.g. length of time the young person has been living in the scheme, so individuals are not named or identified.

9.3. Information about a young person will not be disclosed to anyone else unless the young person gives their informed consent e.g. if a young person wants the Support Worker to help them with a claim for Job Seeker's Allowance or if Commissioners (who pay directly for support services) request any information.

9.4. There may are a number of exceptional circumstances when information about a young person may be disclosed, for example:

- If we believe the need to protect the health and welfare of the young person or other person (e.g. a child) overrides the need to maintain confidentiality.
- Where disclosure is required by a senior ranking police officer in connection with the investigation of an alleged or anticipated serious crime and where failure to disclose would prejudice or delay the detection or prosecution of an alleged or anticipated serious crime. (see 4.12 to 4.17 above)

9.5. Information on young people will also be kept confidential from family members or friends, unless they have given their consent.

9.6. If a member of staff has any doubt as to whether the information should be disclosed, they must consult with the DPO or the CEO.

9.7. Day to day practice in responding to requests for data about young people:

9.7.1. We try never to acknowledge whether or not an individual is living in a Scheme. We say that we will check our records and get back to them. This enables us to think about the request and then also check if the caller has given the correct identity. If the checks are OK, we would offer to pass on a message or a letter. We would never give the address or other contact details.

9.7.2. If a police officer asks for information about one a young person, we only give information if the police officer is investigating a serious crime. We would never give this information on the basis of a call to us. We would phone back to check the identity of the caller. (See 4.14 & 4.16)

9.7.3. If an outside agency wants specific information about a young person, we must be sure that the individual has given their consent before any information is passed on.

9.7.4. It is particularly important that young people understand that we will be asked for a reference when they apply for a move on property. We will not be giving out personal information, but we will be passing on information about how the tenancy was managed including noise or nuisance complaints and any large rent arrears.

9.7.5. We never give out the mobile telephone number of any member of staff. We offer to phone the member of staff concerned and ask them to contact the caller.

10. Consent to photography, video and voice recording

10.1. Young people, donors, members of the public and others will be asked to give permission for BACKUP to use their photographs, likeness, recorded interviews and non-anonymised quotes in any publicity material, emails, newsletters, websites and so on.

10.2. *This permission can be withdrawn at any time*.

11. Information security policy

11.1. The maintenance of BACKUP's IT systems is undertaken by Safer Technologies Ltd and a written agreement is in place advising that that our systems are compatible with the Cyber Essentials Certificate - https://www.cyberessentials.ncsc.gov.uk/

11.2. Staff must ensure at all times that high standards of data quality, data protection, integrity, confidentiality and records management are met. It is the responsibility of all staff to familiarise themselves with this policy and adhere to its principles.

11.3. BACKUP will not only reflect the principles of Information Security in its governance of information but also the principles of Openness, Legal Compliance and Quality Assurance

11.4. Non-confidential information on BACKUP and its services will be made available to the public through a variety of media. BACKUP have clear procedures and arrangements for handling queries from young people, the public, and other parties. Procedures and arrangements for liaison with the press and broadcasting media can be found in BACKUP's 'Media Policy', which can be found on the S drive.

11.5. BACKUP will promote effective confidentiality and security practice to its staff through policies and training.

11.6. In line with the Business Continuity Plan, BACKUP will undertake rehearsals of their business continuity arrangements, against one or more scenarios and will report back to Board about the outcomes of these rehearsals.

11.7. BACKUP will record, monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

11.8. Managers are expected to take ownership of, and seek to improve, the accuracy and quality of information within their services. It is expected that managers will routinely audit information about young people and staff stored locally for accuracy, consistency and relevance.

11.9. Physical security is also important for data security and the following will be taken into consideration where data is stored:

11.9.1. The quality of doors and locks, and the protection of premises by such means as alarms, security lighting or CCTV.

11.9.2. The control of access to premises, and how visitors are supervised

11.9.3. Disposal of any paper and electronic waste

11.9.4. Keeping IT equipment, particularly mobile devices, secure.

12. Fundraising

12.1. This policy takes into account the Institute of Fundraising's Code of Fundraising Practice which includes both relevant law and standards set by the Fundraising Regulator and incorporates the relevant requirements of the GDPR.

12.2. BACKUP applies this Data Protection policy to all collected personal data, including any information held only a database and applies it when writing to individuals, sending them an email, or calling them on the phone.

12.3. BACKUP will seek consent for any marketing communications that are made via:

- Email
- SMS
- Automated telephone calls
- Telephone calls to individuals who are on the Telephone Preference Service (TPS)

12.4. If BACKUP send direct marketing to an individual by post or email without consent, then it will be relying on the organisation's 'legitimate interest' (see 12.8) and will always give individuals the chance to opt out.

12.5. If BACKUP contacts an individual by a live (person to person) telephone call for marketing purposes, then we will be relying on organisation's 'legitimate interest' (see 12.8) and will always give individuals the chance to opt out.

12.6. To obtain consent from an individual for direct marketing BACKUP will always have some form of unambiguous positive action that shows that the person is happy to receive those future communications that will to be separate or additional to the act of donating. This will usually be via a tick box (not pre-ticked) or by supplying contact details on a form or online, provided where it is clear that they are doing so in order to receive direct marketing. This may include oral consent or by a clear action– for example, putting a business card in a bowl at an event where it is clear that is how they can give their contact details to hear more about the charity.

12.7. To determine 'legitimate interest', BACKUP will consider what the individual would reasonably have expected their personal information to be used for at the time that they provided it. If the individual would not have reasonably expected the information to be used for direct marketing, then it will not be used for such by BACKUP.

12.8. Further information can be found in the document 'GDPR: The essentials for fundraising organisations' from The Institute of Fundraising.

13. Keeping personal data

13.1. BACKUP will not keep personal data for longer than it is needed and all personal data is managed, stored and erased in line with its '***Records Management and Retention Policy***'.

13.2. Data is not to be kept indefinitely '*just in case*', or if there is only a small possibility that BACKUP will use it.

13.3. Retention schedules; BACKUP will use the following retention schedules to review data to determine when to keep, delate, part delate or pseudonymisation data once it is no longer needed.

13.4. BACKUP will review data on an annual basis to the check that the retention schedule is capturing all data to be deleted or anonymised.

13.5. BACKUP will review the personal data it holds about an employee when they leave the organisation's employment. It will retain enough data to enable the organisation to provide references or for pension arrangements. BACKUP will delete personal data that it is unlikely to need again from its records – such as the employee's emergency contact details, previous addresses, or death-in-service beneficiary details.

13.6. Any data that BACKUP justifies keeping for statistical purposes will have safeguards in place to protect individuals. For example, pseudonymisation.

14. Closed circuit television (CCTV)

14.1. When deciding to use closed-circuit television (CCTV) surveillance camera systems BACKUP will carefully consider whether a surveillance system would be an effective solution and a justified impact on people's privacy.

14.2. BACKUP will consult all stakeholders that the scheme may affect in relation to the impact of their privacy.

14.3. BACKUP will take into consideration the reason for the surveillance in deciding if a system would be effective. (For example, for the police to use as part of an investigation it is important that the information can be used by the police. How practicable is it to take copies of a recording off a system when requested? Can this be done without interrupting the operation of the system? Can it be provided in a suitable format without losing image quality or time and date information. If any of these are not the case, then this may undermine the purpose for undertaking surveillance)

14.4. BACKUP will regularly evaluate whether it is necessary and proportionate to continue using any current systems.

14.5. The handling and recording of information relating to individuals collected from surveillance systems will be treated as any other personal data as specified in these policies and procedures. This also applies to the Governance of the data (see section 3).

14.6. Surveillance recordings will be deleted in line with BACKUP's retention schedule – see 13.4.

14.7. The Viewing of live images on monitors, (For example, to monitor congestion for health and safety purposes), will be restricted to an authorised and trained person.

14.8. Recorded images will also be viewed in a restricted area, such as a designated secure office.

14.9. Backup operates the same principles for requests of personal data from surveillance as those requests for any other data (see sections 8. 9 and 10)

BACKUP Policy, Procedure, Strategy this document relates to:	• CCTV • Complaints, comments and compliments • Disciplinary and Grievance • Equality, Diversity and Inclusion • GDPR: Data Protection Access Policy • GDPR: Data Protection Flow Chart • GDPR: Data Protection Impact Assessment • GDPR: Introduction to GDPR • GDPR: Privacy Policy • GDPR: Subject Access Request – a member of staff • GDPR: Subject Access Request – a young person • Professional Code of Conduct (within Staff Handbook) • Record Retention Schedule
Ofsted Regulation Standards this document relates to:	• Regulation 4(g) leadership and management standard • Regulation 5(d) and 5(f)(iv) – protection standard • Regulation 7(e)(i) – the support standard

……

This policy is due for renewal on the
1st August 2027

BACKUP NORTH WEST
Bridgeman House, 77 Bridgeman Street, Bolton BL3 6BY
www.backup-charity.org.uk
Registered Charity Number 1064698. Company Number 3399617.

APPENDIX A

Privacy Policy

Our Contact Details:

BACKUP NORTH WEST

Bridgeman House

77 Bridgeman Street

Bolton BL3 6BY

T: 01204 520183

E: businesssupport@backup-charity.org.uk

www.backup-charity.org.uk

Registered Charity Number 1064698

Company Number 3399617.

What type of personal information do we collect ?

- Personal details, i.e. Names, addresses, contact numbers, date of birth
- Identification number (such a National Insurance Number)
- Family details, i.e. Marital status, next of kin and emergency contacts (including your GP)
- Nationality
- Whether you have a current driver's licence
- Whether you are registered as disabled
- Bank account details (employees only)
- So that we can request a DBS check (employees only)

We also process sensitive categories of personal information that may include:

- racial and ethnic origin
- trade union membership (employees only)
- information about your mental or physical health (to assist in the provision of accommodation and support services for young people; insofar as this pertains to your job role for employees)
- Sexual orientation

We collect your information in both physical and digital formats through the following means:

- Telephone
- Email
- Face to face by a member of staff
- Online forms

How do we get the personal information and why do we have it ?

Most of the personal information we process is provided to us directly by you for one of the following reasons:

- So that you can be contacted in routine situations (advised of changes in service, changes to the charity's operations, etc.)
- So that you can be contacted in emergency situations
- So that your next of kin or another person you have identified can be contacted in an emergency
- So that we can make arrangements to pay money owed to you (salary, rent or licence fee rebates, etc.)
- So that we can advise you of changes related to benefit payments, HMRC payments, tax, National insurance, pensions, etc.
- So that we can ensure that we can act appropriately on any health and safety issues that may affect you (Personal Emergency Evacuation Plans, etc.)
- So that we can help identify accommodation for you to move on to (young people only)
- So that we can make salary payments to you (employees only).

How do we use your personal information ?

Your privacy is of the utmost importance to us, and data protection is built into our processing at every stage. This means that while may not require your consent in order to process your personal data, we will only retain and use personal data when we have a legally justifiable reason for doing so that balances our interests as an organisation providing accommodation and support services, or as an employer with your rights as a tenant, licensee or an employee.

Your personal data is shared only with those staff members, and external organisations who also have a legal basis for using it in order to fulfil our obligations to you as someone we provide support services to, or as an employee.

We collect and use your personal information so we can provide services, regulatory functions and administrative activities. Which of those services or activities your personal information is used for depends on the reason you contact us or come into contact with us, but it may include:

- Providing a service you have asked for.
- Providing employment to you.

- Communicating and providing services and information appropriate to your needs.
- Preventing fraud and the protecting public funds
- Protecting you from harm or injury
- For law enforcement when we are legally obliged to contact the relevant Safeguarding Board and/or the Police.
- Monitoring our performance in responding to you and the quality of our services
- Helping to investigate any concerns or complaints and answering enquiries
- Improving the customer experience and the experience of visitors to our websites
- Delivering services and providing support to you by ensuring other organisations with whom we are working, are able to deliver 'joined up' services to you
- Where there is a substantial public interest and this is authorised by law
- Managing our employment relationships and duties including recruitment and ensuring the health and safety of our staff
- When it is in our legitimate interests or the interest of a third party who could be providing a service to you
- Making sure that the charity meets all its legal duties and statutory functions and where it is necessary for exercising or defending legal rights
- Processing and monitoring financial transactions including making payments to HMRS and administering grants
- Archiving, research and statistical purposes - this helps us to prioritise activities, target and plan when to provide services

Where do we store your personal information ?

We store all of your information on secure servers within the European Economic Area (EEA).

How long do we store your personal information ?

We use a 'record Retention Schedule' which outlines how long we keep certain types of information. Unless stated otherwise, we only keep your personal information for as long as it takes to complete the job we needed your information for.

Are there any reasons why we would share your personal information ?

We will respect and protect your privacy and the confidentiality of what you tell us. But you need to know that there are specific circumstances when, without your consent, we may have to pass information to other people:

1. Where a child's safety may be at risk, we are obliged to tell Social Services. A child is considered to be anyone up to 18 years of age.

2. If we are asked by a senior ranking police officer to give information in connection with a serious crime e.g. serious assault, street theft.

3. If we believe that there is risk of serious harm to yourself or others.

We would only give out information in these circumstances on a strictly need to know basis i.e. we only tell them the bare minimum.

We may also disclose your personal information to other organisations who assist us in providing services:

- Funders, regulators and commissioners may ask to view information to check that we are doing what we are paid or expected to do or to monitor the support we provide.
- You may have given our details to others so that we can provide a reference for you (to potential landlords, employers, financial agencies if you have applied for a loan, etc.)

When we use or share your information more widely, we ensure that you can't be identified when it is not necessary. We anonymise and de-personalise your information by removing personal details as soon as possible.

For young people:

- what you tell your Support Worker will remain confidential to you both. Other members of the team will only learn those things that they need to know to do their job. No one will talk about anything to do with you to anyone outside the team, unless you first give your consent e.g. if you want us to help with your claim for benefit or with a housing application, or if you want us to talk to another agency about you. (You will be given a Disclosure Consent Form to sign for this.)
- You have a right to look at any information that we have about you including case notes, the record of the meetings between you and your Support Worker or other members of BACKUP team. Please tell us if you want to do this and your Support Worker will help you to complete the short form '*Request for a copy of information held on a young person*'. We ask you to give us 5 working days if you wish to read your file on site and 40 days if you require a copy of it. We will delete any information in these notes that is confidential to a third party.

Finally, we use your records when we prepare reports about our work, but we never use names so you cannot be identified.

You can always say "no", if you do not want anyone else to see your file.

What happens if you don't want to provide your information ?

If you decide not to provide the information we ask you for, we may not be able to perform the service you have asked us for such as paying you or providing a benefit. Alternatively, we may be prevented from carrying out our legal duties such as ensuring the health and safety of our workers.

Every young person is asked to complete a Disclosure Consent Form when they start to receive a service from BACKUP; this form can be amended at any time and consent withdrawn if they change their mind about sharing information with any of the organisations listed on the form.

What are your data protection rights ?

Under data protection law, you have rights including:

- **Your right of access** - you have the right to ask us for copies of your personal information.
- **Your right to rectification** - you have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
- **Your right to erasure** - you have the right to ask us to erase your personal information in certain circumstances.
- **Your right to restriction of processing** - you have the right to ask us to restrict the processing of your personal information in certain circumstances.
- **Your right to object to processing** - you have the right to object to the processing of your personal information in certain circumstances.
- **Your right to data portability** - you have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You will not be charged for exercising these rights. If you make a request, we have one month to respond to you.

We never sell or share your information with any organisations for marketing purposes.

BACKUP do not use your personal data for any automatic profiling or decision making.

Can I see the information BACKUP holds on me ?

You have the right to see what personal information BACKUP processes about you, and to know our reasons for doing so. In turn, BACKUP has an obligation to keep information about you accurate and up-to-date. If you become aware of any information we hold about you that is inaccurate, or if any of your personal details have recently changed, please notify us and we will update our records accordingly.

You have the right to request to see all your personal information that BACKUP records and processes, by:

- If you are a young person who BACKUP provides accommodation or support services to:

  Filling in a Request for a copy of information held on a young person (a Subject Access Request). You can ask a Support Worker, your Social Worker, someone from the Citizens Advice Bureau, or anyone you know to help you to do this.

- If you are an employee:

  Filling in a Request for a copy of information held on a member of staff (a Subject Access Request).

If you have any questions about BACKUP and your personal information, please contact our Data Protection Officer (DPO), which is our Director of Business.

How to complain

If you have any concerns about our use of your personal information, you can make a complaint to us at:
Data Protection Officer

BACKUP NORTH WEST

Bridgeman House

77 Bridgeman Street

Bolton BL3 6BY

T: 01204 520183

E: businesssupport@backup-charity.org.uk

You can also complain to the ICO if you are unhappy with how we have used your data:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire SK9 5AF

Helpline number: 0303 123 1113 ICO

website: https://www.ico.org.uk

APPENDIX B

Young Person's Disclosure Consent Form

Part 1

Name	
Date of birth	

I agree that information can be shared with the following (tick and sign all that you authorise to)

Housing Welfare	☐	Signature:	
Previous landlords	☐	Signature:	
Benefits Agencies	☐	Signature:	
YOT / Probation Service	☐	Signature:	
Leaving Care Team	☐	Signature:	
GP / Dentist / Health Worker	☐	Signature:	
Connexions	☐	Signature:	
Supporting People	☐	Signature:	

Bolton MBC (Commissioners)	☐	Signature:	
Ofsted	☐	Signature:	
Police	☐	Signature:	
Family members	☐	Signature:	

Please give the name(s) of your family members that we can share information about you with:

Signature:

Please give the name(s) of any other people that we can share information about you with:

Signature:

I understand that I can withdraw this consent at any time by completing Part 2 of this form:

Name:	
Signature	
Date	

Part 2

To be completed when consent to share information is withdrawn

I wish to withdraw my consent for disclosure of information as of:

Date:	
Signature	

Note you can either complete another form if you just want to remove some of the people / officers listed above, or you can give details below:

APPENDIX C

Request for a copy of information held on a young person

Subject Access Request

As part of BACKUP's compliance with the Data Protection legislation, everyone who has a relationship with the charity has the right to be provided with a copy of the current personal information held on them for data processing.

We will endeavour to provide a copy of the data requested within five working days of receipt of a written request; however, some requests may require more time to collate all the information. In all instances we will respond promptly and, in any event, no later than one month from receipt of the written request, as stipulated in the legislation.

Date of request	
Name of person making the request	
Please list any other names you may have been known by in your dealings with BACKUP	
Address	
Postcode	

Email	
Phone number	
How would you like to receive this information (electronically, or printed and sent by post ?)	
Do you need the information to be sent by large font, or do you have any other accessibility requirements ?	

What information do you want a copy of ?
(*Please be specific about the information you're asking for, and where relevant say what information you don't need.*)

Details or dates that will help the organisation find the information you want.

The reason you want the information (you don't have to include this but it will help BACKUP find what you need).

Your Signature

Date received by Director of Business	

Action/Outcome:

This policy is due for renewal on the
1st August 2027

BACKUP NORTH WEST
Bridgeman House, 77 Bridgeman Street, Bolton, BL3 6BY
www.backup-charity.org.uk
Registered Charity Number 1064698. Company Number 3399617.

APPENDIX D

Request for a copy of information held on a member of staff

Subject Access Request

As part of BACKUP's compliance with the Data Protection legislation, everyone who has a relationship with the charity has the right to be provided with a copy of the current personal information held on them for data processing.

We will endeavour to provide a copy of the data requested within five working days of receipt of a written request; however, some requests may require more time to collate all the information. In all instances we will respond promptly and, in any event, no later than one month from receipt of the written request, as stipulated in the legislation.

Date of request	
Name of person making the request	
Please list any other names you may have been known by in your dealings with BACKUP	
Address	
Postcode	

Email	
Phone number	
How would you like to receive this information (electronically, or printed and sent by post ?)	
Do you need the information to be sent by large font, or do you have any other accessibility requirements ?	

What information do you want a copy of ?
(*Please be specific about the information you're asking for, and where relevant say what information you don't need.*)

Details or dates that will help the organisation find the information you want.

The reason you want the information (you don't have to include this but it will help BACKUP find what you need).

Your Signature

Date received by Director of Business	

Action/Outcome:

This policy is due for renewal on the
1st August 2027

BACKUP NORTH WEST
Bridgeman House, 77 Bridgeman Street, Bolton, BL3 6BY
www.backup-charity.org.uk
Registered Charity Number 1064698. Company Number 3399617.