Data Protection Policy

Related Documents

- Adult Support and Protection Policy
- Disciplinary Policy & Procedure
- Digital Communication Policy
- Equal Opportunities Policy
- Health and Safety Policy
- Recruitment Policy

Policy Statement

Mainstay Trust Ltd takes the security and privacy of the information held in relation to our staff, the individuals supported and others who may be connected to the organisation in a formal manner. To effectively employ and provide support to individuals we need to gather information or 'data' about them as part of our business and to manage the relationships which exist with those individuals. The organisation intends to comply with our legal obligations under the **Data Protection Act 2018** ("the 2018 Act") and the **EU General Data Protection Regulation** ("GDPR") in respect of data privacy and security.

This policy details the steps Mainstay Trust Ltd will take to ensure full compliance with both the 2018 Act and GDPR. To ensure consistency in approach, the policy has been created in line with the Information Commissioners Office (ICO) Guidance (published March 2018).

Policy Aims

Mainstay Trust Ltd is committed to ensuring all private and personal information held is stored in a manner which is secure and can only be accessed and shared by relevant individuals both within and outwith the organisation as will be detailed in this policy.

Mainstay Trust Ltd will ensure compliance with consent to holding and sharing information in line with the necessary actions to maintain and provide both the services provided and the general running of the organisation as per the guidance from ICO.

Scope

This policy covers the following groups where information is held which is both private and personal whether stored electronically, on paper or on other materials:

- Individuals who receive support from the organisation (Service Users and/or their family members, legally appointed representatives)
- Individuals employed by the organisation (Staff)
- Individuals involved in the Governance of the organisation (Board Members)

All records held whether they are stored electronically or physically fall within the scope of the 2018 Act and GDPR. GDPR requires any personal data held should:

- Be fairly and lawfully processed
- Be processed for limited purposes and not in any manner incompatible with those purposes
- Be adequate, relevant and not excessive
- Be accurate
- Not be kept for longer than necessary
- Be processed in accordance with the individuals rights
- Be secure
- Not be transferred to countries without adequate protection

The regulations also give the right to any individual to access personal data held about them.

Definitions

"personal data" means information which relates to a living person who can be identified from the data (a data subject) on its own or when taken together with other information which is likely to come into the organisations possession. It includes any expression of opinion about the person and an indication of the intentions of the organisation or others, in respect of the person. It does not include anonymised data.

"data controller" the organisation and identified person within the organisation responsible for and able to demonstrate compliance with the principles of this policy.

"data subject" the individual whose personal data is being processed, stored or otherwise

"regulatory bodies" the organisation is accountable to a range of regulatory bodies to ensure appropriate compliance with provision of support services, these bodies are the Care Inspectorate, Scottish Social Services Council and Glasgow Health & Social Care Partnership, these regulatory bodies may request access to data held or share data about any of the individuals the organisation supports or employs.

"special category data" information relating to individual racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data, health details; sex life and sexual orientation and any criminal convictions or offences. The organisation may hold and use special category data in accordance with the law.

"processing" means any operation which is performed on personal data such as collection, recording, organisation, structuring or storage; adaptation or alteration; retrieval, consultation or use; disclosure by transmission, dissemination or otherwise making available; alignment or combination and restriction, destruction or erasure. This includes processing personal data which forms part of a filing system and any automated processing.

"authorised personnel" means any service providing staff requiring information about the individuals they will support on a day to day basis, any authorised administrative or line management representatives requiring information about staff to enable them to undertake the legitimate business of their day to day business on behalf of the organisation and senior management representatives requiring information about board members for the day to day business of the organisation.

Managing Service User Information

This policy applies to current and former individuals who have or do receive a support service from the organisation. Each of these categories is recognised by the organisation as a 'data subject' for the purpose of this policy. This policy should be read alongside the agreed service agreement and any other notices issued from time to time in relation to data held by the organisation.

It is intended this policy is fully compliant with the 2018 Act and GDPR. If any conflict arises between those laws and this policy, the organisation intends to comply with the 2018 Act and GDPR.

Mainstay Trust Ltd has separate information within the policy in respect of staff and other data subjects.

The organisation has measures in place to protect the security of data held about service users as follows:

- Electronically stored information is password protected and can only be accessed by authorised personnel employed by the organisation.
- Physically stored information is held within lockable filing cabinets/cupboards and can only be accessed by authorised personnel employed by the organisation and regulatory bodies who engage with the organisation for legitimate reasons in line with the day to day running of the organisation.

Mainstay Trust Ltd is a 'data controller' for the purpose of personal data. This means the organisation determines the purpose and means of the processing of personal data. The person responsible for

ensuring this information is stored in accordance with the regulations for all personal data is Gillian Dow, Director.

The data held by the organisation may have been provided to it by the service user or someone else (such as a representative of the GHSCP) or it may have been created by the organisation. The information may have been provided or created during the assessment process or during the course of the service provision or after its termination.

The organisation will collect and use the following types of personal data about a service user, please be advised this list is reflective (but not exhaustive) of the personal data likely to be held for any service user supported by the organisation:

- Photographs
- Contact details of service users and their family/guardians
- Date of birth
- CHI Number, Care First Number and NI Number
- Contact details for all professionals involved in the support, ie health, social work, other providers
- Information about staff known to the individual
- Information about the day to day activities undertaken by the individual and how to support them to achieve these activities
- Details of the outcomes the individual has achieved and is working toward and how these will be supported by the organisation
- Information in relation to reviews of the service provided including opinions in relation to the quality of service experienced
- Personal image information and support details to ensure this is achieved by the individual
- Hospital passport containing all information in relation to the persons health needs including all medication and brief medical history information
- Medication administration records (MAR) sheets, bowel movement charts, fluid intake/output charts, sleep charts any other recordings of personal care requirements
- Information about the risks which may be required to be managed on a day to day basis and how best to manage the risks
- Financial information – where the organisation has been asked to undertake this role, this will include banking information for managed accounts, all benefit information and correspondence, details of payments made and income received for and on behalf of the individual. In these cases the organisation will either by the Corporate Benefit Appointee for the individual or will have been asked to manage limited funds by the Financial Guardian of the individual.
- Information from other organisations known to the person receiving the service this will include Social Work Department, other provider organisations and health services
- Information in relation to any service concerns, complaints or incidents which have occurred involving the individual and staff from the organisation
- Any Adult Support and Protection (AP1) information relevant to the support provided to the individual.
- Images of service users involved in organisational activities (whether captured on CCTV, by photograph or video)
- Any other category of personal data which the organisation may notify service user of from time to time.

The organisation will process service user personal data (including special category data) in accordance with its obligations under the 2018 Act.

The organisation will use service user personal data for the following reasons:

- Performing the full extent of the service provision agreement
- Complying with any legal obligation

- If it is necessary for the organisations legitimate interests (or the legitimate interests of someone else). However the organisation can only do this if the service users interests and rights do not override its own (or other organisation). The service user has the right to challenge the organisations legitimate interest and request the organisation stop processing.
- Details of service users rights can be found in the Data Subject Rights section of this policy.

The organisation can process the personal data of service users for these purposes without the knowledge or consent of the service user. The organisation will not use the personal data of a service user for an unrelated purpose without first informing the service user and confirming the legal basis for its use outside of the reasons given above.

Service users may choose not to provide certain personal data however service users should be aware the organisation may not be able to carry out certain parts of the required provision without full details of specific areas of support needs. For example, withholding essential health needs information may lead to the service user not being appropriately supported.

The organisation will use service users personal data (and special category data – marked with *) for processing purposes in various situations during the course of providing support to the individual:

- To decide whether to provide a service
- To carry out the support provision agreed by the two parties, including where relevant its termination
- To monitor diversity and equal opportunities*
- To monitor and protect the security (including network security) of the organisation, staff, service users and others
- To monitor and protect the health and safety of staff, service users and others*
- To manage the finances including benefits of the person supported (if part of the service provided)*
- Monitoring compliance by the organisation and others with the organisations policies and contractual obligations*
- To comply with health and safety law, adult protection laws and other laws which affect the organisation*
- To answer any questions from insurers in respect of any insurance policies which relate to the service user*
- Running the business of the organisation and planning for the future
- The prevention and detection of fraud or other criminal offences
- To defend the organisation in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*
- For any other reason which the organisation may notify service users of from time to time

The organisation will only process special category data in certain situations in accordance with the law. For example, the organisation can do so if it has explicit consent. In the event the organisation asks for service user consent to process a special category data, it would explain the reasons for the request. The service user does not have to consent and can withdraw consent later if they choose to by writing to Gillian Dow, Director.

The organisation does not need service user consent to process special category data when processing it for the following purposes:

- Where it is necessary to protect the service users vital interests or those of another person where service user/other person are physically or legally incapable of giving consent
- Where the service user has made the data public
- Where processing is necessary for the establishment, exercise or defence of legal claims

The organisation does not take automated decisions about service users, using their personal data or use profiling in relation to service users.

Third party organisations who undertake legitimate activities and have specific information shared of service user personal data undertake the following roles:

- Regulating the services provided
- Paying for the services provided
- Provision of benefits to service users supported with finance management by the organisation

The organisation does not send service users personal data outside the European Economic Area. If this changes, service users will be notified of this and the protections which are in place to protect the security of the data held will be explained.

Managing Staff Information
This policy applies to current and former employees, workers, contractors, self-employed persons, staff, apprentices and consultants. Each of these categories is recognised by the organisation as a "data subject" for the purpose of this policy. This policy should be read alongside the agreed contract of employment and any other notices issued from time to time in relation to data held by the organisation.

This policy does not form part of the terms and conditions of employment (or contract for services if relevant) and can be amended by the organisation at any time. It is intended this policy is fully compliant with the 2018 Act and GDPR. If any conflict arises between those laws and this policy, the organisation intends to comply with the 2018 Act and GDPR.

Within this policy there is additional information in respect of job applicants, service users and other categories of data subject.

The organisation has measures in place to protect the security of data held about staff as follows:

- Electronically stored information is password protected and can be accessed by authorised personnel employed by the organisation.
- Physically stored information is held within lockable filing cabinets/cupboards and can only be accessed by authorised personnel employed by the organisation and regulatory bodies who engage with the organisation for legitimate reasons in line with the day to day running of the organisation.

Mainstay Trust Ltd is a 'data controller' for the purpose of personal data. This means the organisation determines the purpose and means of the processing of staff members personal data. The person responsible for ensuring this information is stored in accordance with the regulations for all staff information is Gillian Dow, Director.

The data held by the organisation may have been provided to it by the staff member or someone else (such as a former employer, medical professional or a credit reference agency) or it may have been created by the organisation. The information may have been provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. The information could be created by representatives of line management or colleagues.

The organisation will collect and use the following types of personal data about a staff member:

- Recruitment information such as application form and CV, references received/given, qualifications and membership of any professional bodies and details of any pre-employment assessments
- Contact details for staff and emergency contacts
- Date of birth
- Gender
- Details of marital status and family details
- Information about terms and conditions of employment including start, continuous employment and end dates of employment, role and location, working hours, details of any promotion, training, salary (including details of previous remuneration), pension, benefits and holiday entitlement;

- Health declaration information
- Bank details and information in relation to tax status including National Insurance number
- Information in relation to registration with SSSC
- Information in relation to the PVG checks undertaken
- Copies of ID documentation including passport and driving licence and information in relation to immigration status and the right to work in the UK
- Information relating to disciplinary or grievance investigations and any other proceedings involving staff, such as complaints, duty of candour procedures (whether or not the staff member was the main subject of those proceedings)
- Information relating to performance and conduct at work (support and supervision)
- Electronic information in relation to use of IT systems / swipe cards / telephone systems
- Images of staff involved in organisational activities (whether captured by photograph or video)
- Any other category of personal data which the organisation may notify staff from time to time.

The organisation will process staff personal data (including special category data) in accordance with its obligations under the 2018 Act.

The organisation will use staff members personal data for the following reasons:

- Performing the contract of employment between the organisation and staff
- Complying with any legal obligation
- If it is necessary for the organisations legitimate interests (or the legitimate interests of someone else). However, the organisation can only do this if staff interests and rights do not override its own (or other organisation). Staff have the right to challenge the organisations legitimate interest and request the organisation stop processing.
- Details of staff rights can be found in the Data Subject Rights section of this policy.

The organisation can process the personal data of staff for these purposes without the knowledge or consent of staff. The organisation will not use the personal data of staff for an unrelated purpose without first informing staff and confirming the legal basis for its use outside of the reasons given above.

Staff may choose not to provide certain personal data however staff should be aware the organisation may not be able to carry out certain parts of the contract between them and the member of staff. For example, withholding bank account details would mean the organisation will not be able to pay the staff member. It may also stop the organisation from complying with certain legal obligations and duties required of the organisation such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability a staff member may suffer from.

Should staff refuse, at any time during their employment, to provide the necessary personal data for the organisation to comply with its legal obligations, the organisation may consider termination of contract based on Some Other Substantial Reason.

The organisation will use staff personal data (and special category data – marked with *) for processing purposes in various situations during recruitment, employment and following termination of the employment as follows:

- To decide whether to offer a contract of employment
- To decide how much to pay staff and the other terms of employment with the organisation
- To check staff have the legal right to work in the UK
- To carry out the contract between the two parties, including where relevant, its termination
- Training and reviewing performance*
- To decide whether to offer a promotional opportunity
- To decide whether and how to manage performance, absence or conduct*

- To carry out a disciplinary or grievance investigation or procedure in relation to the staff member or someone else
- To determine whether the organisation needs to consider reasonable adjustments for the staff members workplace or role because of a physical or mental health condition*
- To monitor diversity and equal opportunities*
- To monitor and protect the security (including network security) of the organisation, staff, service users and others
- To monitor and protect the health and safety of staff, service users and others*
- To pay staff and provide pension and other benefits in accordance with the organisations terms and conditions of employment*
- To pay tax and National Insurance;
- To provide a reference on request from another employer
- To pay Trade Union subscriptions*
- Monitoring compliance by staff, the organisation and others with the organisations policies and contractual obligations*
- To comply with employment law, immigration law, health and safety law, tax law, and other laws which affect the organisation*
- To answer any questions from insurers in respect of any insurance policies which relate to staff*
- Running the business of the organisation and planning for the future
- The prevention and detection of fraud or other criminal offences
- To defend the organisation in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*
- For any other reason which the organisation may notify staff of from time to time

The organisation will only process special category data in certain situations in accordance with the law. For example, the organisation can do so if it has explicit consent. In the event the organisation asks for consent to process special category data it would explain the reasons for the request. Staff do not have to consent and can withdraw consent later if they choose to by writing to Gillian Dow, Director.

The organisation does not require consent to process special category data when they are processing it for the following purposes:

- Where it is necessary for carrying out rights and obligations under employment law
- Where it is necessary to protect staff vital interests or those of another person where staff member/other person are physically or legally incapable of giving consent;
- Where the staff member has made the data public;
- Where processing is necessary for the establishment, exercise or defence of legal claims; and
- Where processing is necessary for the purposes of occupational medicine or the assessment of the staff members working capacity.

The organisation will process information about criminal convictions via the Protection of Vulnerable Adults scheme in accordance with the organisations Protection of Vulnerable Adults Policy.

The organisation might process special category data for the purposes of those items marked above with an asterisk (*) beside them. In particular, the organisation will use information in relation to:

- Age, disability, gender reassignment, marriage/civil partnership, pregnancy/maternity, race, religion/belief, sex or sexual orientation to monitor equal opportunities
- Sickness absence, health and medical conditions to monitor absence and attendance, assess fitness for work, to pay benefits, to comply with the organisations legal obligations under employment law including consideration of reasonable adjustments and to support health and safety
- Trade Union membership to pay any subscriptions and to comply with the organisations legal obligations in respect of trade union members.

The organisation does not take automated decisions about using staff personal data or use profiling in relation to staff.

The organisation will share staff personal data with group companies or contactors and agents to carry out the organisations obligations under the contract of employment and for the organisations legitimate interests.

The third party organisations who undertake legitimate activity for the business and have specific information shared of staff personal data undertake the following roles:

- Payroll processing, including calculation of salary payments, tax and NI payments, sickness benefit payments, annual leave payments, pension deductions, loan deductions, salary deductions from legal sources
- Pension calculation and management
- Death in service calculation and management (restricted group)
- Counselling
- Occupational Health
- HR

The organisation does not send personal data outside the European Economic Area. If this changes staff will be notified of this and the protections which are in place to protect the security of the data held will be explained.

Managing Board Members Information

This policy applies to current and former board members. This group is recognised by the organisation as a data subject for the purpose of this policy. This policy should be read alongside the organisations Memorandum and Articles of Association and any other notices issued from time to time in relation to data held by the organisation.

It is intended this policy is fully compliant with the 2018 Act and GDPR. If any conflict arises between those laws and this policy, the organisation intends to comply with the 2018 Act and GDPR.

The organisation has measures in place to protect the security of data held about board members as follows:

- Electronically stored information is password protected and can be accessed by authorised personnel employed by the organisation.
- Physically stored information is held within lockable filing cabinets/cupboards and can only be accessed by authorised personnel employed by the organisation and regulatory bodies who engage with the organisation for legitimate reasons in line with the day to day running of the organisation.

Mainstay Trust Ltd is a data controller for the purpose of board member personal data. This means the organisation determines the purpose and means of the processing of board member personal data. The person responsible for ensuring this information is stored in accordance with the regulations for all board members information is Gillian Dow, Director.

The data held by the organisation may have been provided to it by the board member or it may have been created by the organisation. The information may have been provided or created during the recruitment process to the board or during the tenure of the board member or after their termination.

The organisation will collect and use the following types of personal data about a board member:

- Contact details
- Date of birth
- Gender
- Copies of ID documentation including passport and driving
- Information about the suitability of the individual to undertake the role of board member and trustee of the organisation as required by Companies House
- Images of board members involved in organisational activities (whether captured by photograph or video);
- Any other category of personal data which the organisation may notify board members of from time to time.

The organisation will process board members personal data (including special category data) in accordance with its obligations under the 2018 Act.

The organisation will use board members personal data for the following reasons:

- Complying with any legal obligation
- Compliance with the requirements of regulatory bodies (Care Inspectorate, GHSCP, Companies House and OSCR)
- If it is necessary for the organisations legitimate interests (or the legitimate interests of someone else). However, the organisation can only do this if the board members interests and rights do not override its own (or other organisation). The board member has the right to challenge the organisations legitimate interest and request the organisation stop processing.
- Details of board members rights can be found in the Data Subjects Rights section of this policy.

The organisation can process the personal data of board members for these purposes without the knowledge or consent of the board member. The organisation will not use the personal data of a board member for an unrelated purpose without first informing the board member and confirming the legal basis for its use outside of the reasons given above.

Board members may choose not to provide certain personal data, however board members should be aware the organisation may not be able to carry out certain parts of their governance compliance if information is withheld. For example, withholding ID information may mean the organisation cannot correctly register the board member with Companies House. It may also stop the organisation from complying with certain legal obligations and duties required of the organisation.

The organisation will use board member personal data (and special category data – marked with *) for processing purposes in various situations during the board member recruitment, tenure and following termination of the tenure as follows:

- To decide whether to invite the board member to join the board of directors
- To determine whether the organisation need to make a reasonable adjustment for the board member role because of a disability*
- To monitor diversity and equal opportunities*
- To monitor and protect the security (including network security) of the organisation, board members, service users and staff
- To monitor and protect the health and safety of board members, service users and staff*
- Monitoring compliance by the board member and staff members with the organisations policies and contractual obligations*
- To comply with employment law, immigration law, health and safety law, tax law, and other laws which affect the organisation*
- To answer any questions from insurers in respect of any insurance policies which relate to the board member*
- Running the business of the organisation and planning for the future

- The prevention and detection of fraud or other criminal offences
- To defend the organisation in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*
- For any other reason which the organisation may notify board members of from time to time

The organisation will only process special category data in certain situations in accordance with the law. For example, the organisation can do so if it has the board members explicit consent. In the event the organisation asks for the board members consent to process a special category data it would explain the reasons for the request. The board member does not have to consent and can withdraw consent later if they choose to by writing to Gillian Dow, Director.

The organisation does not need board member consent to process special category data when they are processing it for the following purposes, which the organisation may do:

- Where it is necessary for carrying out rights and obligations under employment law
- Where it is necessary to protect the board member vital interests or those of another person where the board member/other person are physically or legally incapable of giving consent
- Where the board member has made the data public
- Where processing is necessary for the establishment, exercise or defence of legal claims

The organisation does not take automated decisions about board members using personal data or use profiling in relation to board members.

The organisation will share board members personal data with regulatory bodies; Care Inspectorate, GHSCP, Companies House and OSCR. These companies are only permitted to process board member data for the lawful purpose for which it has been shared and in accordance with the organisations instructions.

The organisation does not send board members personal data outside the European Economic Area. If this changes board members will be notified of this and the protections which are in place to protect the security of the data held will be explained.

Managing the Confidentiality of Personal Data

Everyone who works for or on behalf of the organisation has a responsibility for ensuring data is collected, stored and handled appropriately.

The organisations Data Protection Officer (Gillian Dow, Director) is responsible for reviewing this policy and updating the Board of Directors on the organisations data protection responsibilities and any risks in relation to the processing of data. Any questions in relation to this policy or data protection should be raised in writing to this person.

Only authorised personnel will have access to any personal data covered by this policy. Authorised personnel will need information to enable them to undertake the work they do for or on behalf of the organisation. Authorised personnel will only use the data available to them for the specified lawful purpose for which it has been obtained.

The following practices will apply:

- No personal data should be shared informally
- All personal data held should be regularly reviewed and updated in the event of changes to the information held
- Copies of information should only be made if absolutely necessary and should be stored securely, with any unnecessary copies being disposed of securely

- Password protection for all electronic access should include the use of capital letters, symbol, letters and numbers of between 8 and 20 characters and should not be easily identifiable by any party
- Access to electronic devices should be locked when not in use and shut down at the end of each period of use to prevent unauthorised access
- Where possible anonymise personal data using separate keys/codes so the data subject is not easily identified (for example CHI Numbers or Care First Numbers for communication with health and social work)
- Personal data should not be stored on personal computers or other devices
- Personal data should not be removed from the organisations premises without authorisation from line manager or the Data Protection Officer
- Personal data should be shredded and disposed of securely when it is no longer required
- In the event any staff member requires clarification on the organisations data protection regulations or notices areas where data protection may be at risk or could be improved they should speak to the Data Protection Officer
- Any deliberate or negligent breach of this policy by any individual working with or on behalf of the organisation may result in disciplinary action being taken in accordance with the Disciplinary Policy & Procedure
- It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see Subject Access Requests section of this policy). Conduct of this nature would amount to gross misconduct under the Disciplinary Policy & Procedure, which could result in dismissal.

Homeworking Data Protection

For any member of staff who works from home for part or all of their contractual hours whether defined as a "homeworker" under the HSE definition or not, all terms of this policy remain and apply at all times. Any breach of this policy may result in the disciplinary procedure being instigated.

All devices including PCs, laptops, tablets, smart televisions and smart phones must be secured when not in use. If devices are accessible by other household members, access to any material, programme, application, website, document and any other data which may fall under the terms of this policy must be password protected.

In the circumstance of shared or sole access to devices, it remains essential no passwords are auto-filled, auto-completed or stored.

Physical information such as paperwork, files or otherwise containing personal data must be kept secure when not in use. A lockable case, cabinet, drawer, briefcase or otherwise should be utilised to ensure access to personal data cannot be obtained by any other member of the household or any potential visitor.

Subject Access Requests

Data subjects can make a 'subject access request' ('SAR') to find out what data is held by the organisation about them. This request must be in writing. If such a request is received it should be forwarded immediately to the Data Protection Officer who will coordinate the response.

To make a SAR in relation to personal data, the individual requesting the information should make this in writing to Gillian Dow, Director. The organisation must respond within **one month** unless the request is complex or numerous in which case the period can be extended by a further two months. The Data Protection Officer will be required to confirm the need to extend the period to the individual requesting the information.

The organisation will not charge a fee for making a SAR. However, if the request is manifestly unfounded or excessive the organisation may charge a reasonable administrative fee or refuse to respond to the request.

Data Subject Rights
The individual whose data the organisation holds/processes (service users, staff members, board members) have the following rights:

- To be given information about what personal data the organisation holds/processes, how and on what basis the organisation will use this as set out in this policy
- To access the personal data information held by way of a subject access request as detailed in subject access requests section above
- To correct any inaccuracies in the personal data held, contact Gillian Dow, Director
- To request the organisation erase personal data held where the organisation were not entitled under the 2018 Act or GDPR to process it or it is no longer necessary to process it for the purpose it was collected. To do this the individual should contact Gillian Dow, Director.
- While requesting personal data held is corrected or erased or being contested for the lawfulness of the organisations processing, the individual can apply for its use to be restricted while the application is made. To do this the individual should contact Gillian Dow, Director.
- To object to data processing where the organisation are relying on a legitimate interest to do so and the individual believes their rights and interests outweigh those of the organisations and the individual wishes this to stop.
- To object if the organisation processes their personal data for the purposes of direct marketing.
- To receive a copy of the personal data held and to transfer this to another data controller. There will be no charge for this and in most cases the organisation aim to do this within one month.
- To be notified of a data security breach concerning your personal data.
- To complain to the Information Commissioner. An individual can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on the individuals rights and the organisations obligations.

Data Protection Breaches
The organisation has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur, the organisation must take notes and keep evidence of the breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then the organisation must also notify the Information Commissioner's Office within 72 hours of the breach occurring.

If any individual supported, employed or involved with the organisation is aware of a data breach they must contact Gillian Dow, Director immediately and keep any evidence in relation to the breach.

A data protection breach occurs when personal data (which includes any information which allows an individual to be identified), is processed without authorisation, and which may result in its security being compromised. For the purpose of this policy, data protection breaches include both confirmed and suspected breaches.

This procedure is concerned with the management of such data protection breaches, which involves the detection and reporting of breaches as well as learning from the breach and implementing appropriate remedial actions.

Most commonly, data protection breaches occur as a result of human error, theft, unauthorised access, equipment failure, hacking or loss.

Examples of common breaches are:

a) Technical – data corruption, malware, corrupt code, hacking

b) Physical – unescorted visitors in secure areas, break-ins to sites, theft from secure sites, theft from unsecured vehicles/premises, loss in transit/post, loss/misplacing of memory stick/flash drive, confidential papers left on public transport
c) Other – data input errors, non-secure disposal of hardware or paperwork, unauthorised disclosures (including verbal)

When a data protection breach has been discovered, whatever the reason for the breach the following procedure will be implemented.

Discovery
All staff are responsible for data protection and should be alert to any actual, suspected, threatened or potential data protection breaches. As soon as a data protection breach or potential breach has been discovered, where possible, a Data Protection Breach Reporting Form should be completed to the fullest extent possible at the time, which provides full details concerning the breach or potential breach. This form should then be passed to Gillian Dow, Director as soon as possible and in any event within two hours of discovery of the breach.

In the event there is difficulty in completing a form the reporting should not be delayed and instead the matter should be reported immediately, either verbally or using electronic means, such as email.

Once the data breach has been reported, an initial assessment will be made concerning the content, quality of data involved and the potential impact and risk of the breach.

This is achieved by interviewing the key individuals involved in the breach and collecting as much information as possible to determine how the breach occurred, what actions have been taken, whether outside agencies are involved and whether the data subjects have been notified.

Not all data protection breaches will result in formal ICO Reporting action. Some will be false alarms or 'near miss' events which do not cause immediate harm to individuals or the organisation. These should still be reported, as analysis of these instances will provide valuable process feedback and opportunity for continual improvement in managing personal data.

Reporting
Following a discovery of a breach and the receipt of such a report, consideration will be made regarding whether the matter needs to be reported to the Information Commissioner's Office (ICO) and whether individuals who are potentially affected need to be informed.

Current legislation states any data protection breaches (irrespective of their severity) should be reported to the ICO as soon as possible and no later than 72 hours after their discovery, unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned.

In addition to this, the individuals affected by the breach should be informed if the breach is likely to pose a high risk to them. The individuals should be informed of the nature of the data breach and the steps taken by the organisation to protect their data.

Where the breach includes information which includes other parties including contractual agreements with local authorities the breach must be reported within 12 hours of discovery to the relevant authority.

The incident should also be logged in the Data Protection Breach Register.

Containment and Recovery

As soon as possible after the discovery of an actual or suspended data protection breach, consideration will be given to:

- Whether the breach has been contained as far as possible and whether any further steps can be take to contain the data from further loss
- Whether any steps can be taken to mitigate the impact and risk of the loss
- Whether anything can be done to recover the data

Investigation

Following the initial discovery/reporting of an incident, an investigation will be initiated to understand the full facts regarding the data protection breach. The extent of the investigation will be a matter for the organisation to decide and may involve the collation of documents or may involve interviewing of individuals (those supported/staff members) involved in the breach, collecting witness statements etc.

Remedial Actions

Once the full facts have been ascertained and the investigation has been concluded consideration will be given to what can be learned from the breach and most importantly what remedial actions the organisation needs to take to prevent a recurrence of the incident, this may include any disciplinary action for individuals implicated in the breach.

Actions should be documented on an action plan, which is reviewed on a regular basis thereafter to ensure that the actions have been carried out.

During and/or at the end of the completion of the investigation the Data Protection Reporting Form and the Data Protection Breach Register will be updated to ensure that all the details of the events have been properly documented.

Any employees who act in breach of this policy or who do not implement it, may be subject to formal disciplinary proceedings, which may involve dismissal depending on the relevant circumstances.

Data Retention/Disposal

The organisation is committed to managing and handling personal data in line with best practice and data protection principles as detailed in this policy. As such the following information details the organisations procedures to ensure timely and secure disposal of documents and records are no longer required for business purposes.

The organisation holds a wide variety of personal data about the individuals supported, staff members and board members, including financial data, HR data, service provision data. The information is held in various formats including letters, emails, contracts, forms, software systems in both hard copy and electronic form.

It is essential the procedure for retention/disposal is adhered to, as destruction of documents could result in an inability to defend claims, business difficulties and failure to comply with data protection legislation, whilst appropriate destruction and disposal will ensure the storage space is maximised and the organisation is not keeping documents for an unnecessarily long period of time which would breach data protection legislation.

This procedure applies to all information held by the organisation and also any personal data which may be held by data processors (other organisations) where they are processing information on the organisations behalf.

Everyone connected to the business of the organisation is responsible for ensuring the records they create/maintain are accurate, maintained and disposed of in accordance with this procedure. It is recognised the documentation created and maintained by the organisation will change over time and therefore the data held will be reviewed regularly (at least annually unless otherwise specified) to ensure

there is a sound business reason for retaining the information held, where there is no business reason to hold information (after relationship between the organisation and data subjects detailed) this will be securely destroyed.

In exceptional circumstances the organisation may hold information for longer than all periods stated per group affected, in such cases the organisation will explain the legal basis for retaining the data upon request.

Service User Information

People who use services can be confident:

- The information held by the organisation about them is reflective of only information which is necessary to allow the appropriate level of care and support in accordance with the social work assessment carried out prior to engagement of the organisation and with regular review of those service needs both by the organisation (six monthly) and the GHSCP where appropriate (annually or bi-annually)
- Both social care records and financial information (where relevant) for adults are kept or disposed of in accordance with the 2018 Act and will be destroyed six years from last date of entry (or end of service). After this period, the organisation will dispose of the records in a safe, confidential manner. It can have them destroyed, eg by confidential shredding or, if they are in electronic form, deleted from the computer archive. This will be supported by the organisations IT Support organisation.
- Where a service user transfers to another service, it can be assumed their care records will be transferred with them.
- When the service ends all hard copy information will be scanned and stored electronically and retained for six years in an electronic format. All hard copy information will be securely destroyed (once stored electronically) by confidential shredding.

Staff (or Applicants for Positions) Information
Staff who have been employed by or who have applied to be employed by the organisation can be confident:

- The information held by the organisation about them is reflective of only information which is necessary for the employment, decision about employment and direct support of the individual staff member.
- All personal information stored for staff or applicants is kept and disposed of in accordance with the 2018 Act and will be destroyed in compliance with the following:
    - Employee files and Personal Development Records will be held for 6 years after the end of employment
    - Disciplinary and Grievance, Examination and Testing, Accident Information and Ill Health will be held for 6 years from last action
    - Job Descriptions and Terms and Conditions will be held for 6 years from last action
    - PAYE records and records of hours worked for minimum wage purposes will be held for 6 years from end of financial year
    - General Annual Leave information will be held for 3 years from end of annual leave year
    - Parental Leave records will be held for 5 years from birth/adoption, or until child is 18 years old if receiving disability allowances
    - Statutory Maternity, Adoption, Paternity and Sick Leave records will be held for 4 years from financial year end
    - Data relating to ex-employee employment tribunal claims/SAR held for 2 years after claim/SAR concluded or 5 years post-employment whichever is later
    - Pension records held for 12 years after benefit ceases

- Candidate application forms/CV's and accompanying documentation (unsuccessful applicants) will be held for six months post date of recruitment decision and if necessary longer in the event of dispute of decision
- Disclosure Scotland data will be held six months post-date of check
- Redundancy details held for 6 years from date of redundancy
- Eligibility to work in the UK documents will be held for 2 years after employment ceases

After the periods detailed above, the organisation will dispose of the records in a safe, confidential manner. It can have them destroyed, eg by confidential shredding or, if they are in electronic form, deleted from the computer archive. This will be supported by the organisations IT Support organisation.

Board Member Information
Individuals who are or have been board members of the organisation can be confident:

- All personal information is kept or disposed of in accordance with the 2018 Act and will be destroyed 3 years from resignation from the board.
- Board members are advised the following information will be held electronically, permanently by the organisation:
  - Trustees minutes
  - Trust deeds and rules
- Reporting information for regulatory bodies in the event of any dispute, criminal action on the part of the board member will be held until resolution of dispute and for a further 3 years.

After the periods detailed above, the organisation will dispose of the records in a safe, confidential manner. It can have them destroyed, eg by confidential shredding or, if in electronic form, deleted from the computer archive. This will be supported by the organisations IT Support provider.

Health & Safety Information (all data subject groups)
The following retention periods will apply to data which is relevant to the health and safety of any data subject supported, employed or governing the organisation:

- Control of Major Accident Hazard Regulations, all assessments, evaluation reports, practice drills etc for the duration of involvement plus 20 years
- Fire Safety Regulations, all assessments, maintenance records, training etc for the duration of involvement plus 5 years
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR), normal physical accident information stored for duration of involvement plus 3 years following accident, health related illness held for duration of involvement plus 40 years
- Display Screen Equipment Assessments (where relevant) held for 3 years
- Control of Substances Hazardous to Health Regulations (COSHH) for the duration of involvement plus 40 years

Further Sources of Information
The following organisations and legislation also offer a range of guidance and support to assist with ensuring best practice in relation to the protection of individuals data:

Information Commissioner's Office
www.ico.org.uk

Care Inspectorate
www.careinspectorate.com

Glasgow Health and Social Care Partnership
www.glasgowcity.hscp.scot

OSCR Scottish Charity Regulator
www.oscr.org.uk

Scottish Council for Voluntary Organisations
www.scvo.org.uk

Companies House
www.gov.uk/government/organisations/companies-house

Advisory, Conciliation and Arbitration Service (ACAS)
www.acas.org.uk

Version Control			
Version	Author	Date	Changes
0.1	Natasha Gordon	06/07/23	First Draft
0.2	Natasha Gordon	24/07/23	Approved by Director: Gillian Dow
1.0	Natasha Gordon	25/07/23	Approved by Board

Reviewed July 2023
Review By July 2026