Data Protection Policy

Aims of this Policy

The Crichton Trust needs to keep certain information on its Employees, Residential Tenants, Neuro's Spa Members, Customers, Volunteers and Trustees to carry out its day-to-day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the General Data Protection Regulations (2018) To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also outlines key data protection procedures.

This policy covers employed staff, residential tenants, spa members, customers and trustees.

Definitions

The lawful bases for processing are set out in Article 6 of GDPR. At least one of these must apply whenever personal data is processed:

(a) **Consent:** the individual has given clear consent for their personal data to be processed for a specific purpose

(b) **Contract:** the processing is necessary for a contract which is held with the individual, or because they have requested specific steps before entering into a contract

(c) **Legal obligation:** the processing is necessary for compliance with the law (not including contractual obligations)

(d) **Vital interests:** The processing is necessary to protect someone's life

(e) **Public task:** the processing is necessary to enable the performance of a task in the public interest or for official functions, and the task or function has a clear basis in law

(f) **Legitimate interests:** the processing is necessary for the organisation's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (this cannot apply where a public authority is processions data to perform official tasks).

Type of Information Processed

Employees

- Contact details (email, address and phone number
- An emergency contact
- Date of birth
- Marital status
- Bank Account details
- NI Number
- Tax coding
- Sickness records, including Doctor's certificates

- CVs and references
- Appraisal notes

Most employee data is collected directly from the employee. Data is also collected indirectly from HMRC (annual tax coding) and General Practitioners (sickness certificates)

The Trust shares employee personal data with:

- HMRC (legal requirement)
- The Trust's Banker (for salary payment purposes)
- Dumfries and Galloway Council (as Pensions Authority)
- Westfield Health (for Health Insurance)
- Unum (Life Assurance)
- The Trust's HR Advisor
- The Trust's H&S Advisor

Residential Tenant

- Full name, home address, email address and telephone number
- Lease information

Residential tenant data is collected directly from the individual.
The Trust does not share residential tenant data with third parties.

Trustees

- Full name, home address, email address and telephone numbers (s)
- Date of birth
- Date of appointment
- NI number
- Country of Residence
- Business Occupation
- Directorship of other Companies
- Bank account details (if expenses are claimed)
- CVs and photographs

This data is collected from the individual, and is the subject of a Standing Item at each Board meeting when Trustees are reminded to update it as necessary.

The Trust only shares this data with Companies House.

Neuro's Spa Members

- Full name, home address, email address and telephone number(s)
- An emergency contact
- Date of birth
- Bank Account details (only until first SO or DD payment is set up with the Bank)

The data is collected from the individual and is updated on an "as needs" basis.
The data is not shared with any third parties.

Responsibilities

Overall responsibility for personal data in a "not for profit" organisation rests with the Governing Body. In the case of The Crichton Trust, this is a Board of Trustees of the Crichton Trust Ltd:
Charity registered in Scotland No. SC024797-Company registered in Scotland No. 164601

The Board of Trustees delegates GDPR to an allocated member of the Executive Team. The Trust's Data Protection Officer is Ms Linda Russell, Head of Corporate Services, who is responsible for:

- Understanding and communicating obligations under GDPR
- Identifying potential problem areas or risks
- Encouraging training of staff, and Trustees, as necessary
- Annually renewing latest guidance about data protection

Policy Implementation

To meet our responsibilities staff and Trustees with:
- Ensure any personal data is collected in a fair and lawful way
- Explain why it is needed at the start
- Ensure that only the mimimum amount of information needed is collected and used
- Ensure the information used is up to date and accurate
- Review the length of time information is held
- Ensure it is kept safely
- Ensure the rights people have in relation to their personal data can be exercised.

The Trust will ensure that:
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, Trustee or service provider, knows what to do
- Queries about handling personal information will be dealt with swiftly and politely
- Any disclosure of personal data will be in line with procedures.

Training

Training and awareness raising about GDPR and how it is following in this organisation will take the following forms:

On induction:
- Staff and Trustees will receive a written procedure about handling personal data, even if their contact with personal data is limited.
- Any queries and any training needs should be addressed to the Data Protection Officer
- Any new staff or trustees will be inducted into secure items as appropriate.

General training/awareness raising:
- There will be an annual GDPR monitoring and training session for all staff and Trustees.

Gathering and checking information

Before personal information is collected, the Trust will consider:
- The minimum amount of data that is needed to provide its services
- How the data will be kept
- Security for that information, and who has access to it
- If, and how, the data will be processed

The Trust will inform individuals whose information is gathered about the following:

- That the Crichton Trust has a Privacy policy
- To whom any enquiries or comments about personal data should be addressed

The Trust will take the following measures to ensure that personal information kept is accurate:
- Keep in regular contact with Employees, Volunteers, Trustees and Members

Data Security

The Crichton Trust takes steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary proceedings.

Any unauthorised disclosure of personal data to a third party by a Trustee may result in:
- Possible penalties for the Trustee, including removal from the Board.

Subject Access Requests

Anyone whose personal information is held by the Trust has the right:
- To be informed
- Of access
- Of rectification
- Of erasure/the right to be forgotten
- To restrict processing
- To data portability
- To object
- To make choices about automated decision making and profiling

Individuals have the right under GDPR to access personal data being kept about them by The Crichton Trust. Any person wishing to exercise this right should apply in writing to: ***Linda Russell, Data Protection Officer, The Crichton Trust, Grierson House, Bankend Road, Dumfries DG1 4ZE or by email to: subjectaccess requests@crichton.co.uk***. The Trust will then have one calendar month to respond unless the request is considered to be a particularly onerous one. In those circumstances, the data subject will be informed that an extension has been added to the time allowed to fulfil the request.

The following information will be required before access is granted:
- Full name and contact details of the person making the request
- Their relationship with the organisation (former/current Employee, former/current Spa Member, former/current Trustee, Volunteer, service provider)
- Any other relevant information

The Trust may also require proof of identify before access is granted. The following forms of ID will be accepted:
- Driver's Licence
- Passport

Review

This policy will be reviewed at intervals of every two years to ensure that it remains up to date and compliant with the law.

Approval date	1 June 2018	Version 2
Next Review Date	1 June 2020	