Data Protection Policy

Policy information	
Organisation	The Derby & Sandiacre Canal Trust (hereinafter The Trust)
Scope of policy	This policy applies to all areas of The Trust, together with all volunteers and employees of the Trust
Policy operational date	3rd February 2021
Policy prepared by	Derek Troughton, Director & Treasurer
Date approved by Board/ Management Committee	3rd February 2021
Policy review date	This Data Protection policy will be reviewed every three years.
Introduction	
Overview	The Trust needs to gather and use certain information about individuals. This includes, members, volunteers, employees, suppliers, business contacts. The policy describes how this personal data must be collected, handled and stored to meet the Trust's data protection standards and comply with the law
Purpose of policy	This policy ensures that The Trust: • Complies with data protection law and good practice • Protects the rights of volunteers, staff and other individuals • is open about how it stores and processes individual's data • Protects itself from the risks of a data breach
Brief introduction to Data Protection Legislation	The Data Protection Act 1998 & UK GDPR legislation describe how a company , including The Trust, must collect, handle and store personal information These rules apply regardless of whether data is stored electronically, on paper or on other materials To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully
Data Protection Principles	The Data Protection Act is underpinned by 8 important principles. These state that personal data must: • Be processed fairly and lawfully • Be obtained only for specific, lawful purposes • Be adequate, relevant and not excessive • Be accurate and kept up to date • Not be held for any longer than necessary • Processed in accordance with the rights of data subjects • Be protected in appropriate ways • Not be transferred outside the UK, unless to a country which also has adequate levels of protection in place
Personal data	This policy applies to all data that The Trust holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection 1998 & UK GDPR legislation. This can include • Names of individuals • Postal addresses • Email addresses • Telephone numbers (including mobile phone numbers) • Any other relevant information regarding the individual

Key risks	This policy helps to protect The Trust from some very real data security risks, including: • **Breach of confidentiality** - information being given out inappropriately • **Failing to offer choice** – e.g. all individuals should be free to choose how The Trust uses data relating to them • **Reputational damage** – e.g. The Trust could suffer if hackers successfully gained access to sensitive data
Responsibilities	
Trustees	They have overall responsibility for ensuring that The Trust complies with its legal obligations.
Volunteers/employees	They have a responsibility for ensuring data is collected, stored and handled in line with this policy and data protection principles
Data Protection Officer	Their responsibilities include: • Briefing the board on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other staff on tricky Data Protection issues • Ensuring that Data Protection induction and training takes place • Notification (see notes) • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors (see notes)
Trust Chairman	Is responsible for: • Approving any data protection statements attached to communications such as emails and letters • Addressing any data protection queries from journalists or media outlets like newspapers
Trust Officers	Each Trust officer who handles personal data is responsible for drawing up their own operational procedures to ensure that good Data Protection practice is established and followed. They must also ensure that the Data Protection Officer is informed of any changes in their uses of personal data that might affect the organisation's Notification.
Staff & volunteers	All staff and volunteers should be required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. They also need to follow the following guidelines: • The only people able to process data covered by this Policy should be those who need it for their work • Data should not be shared informally • All data should be kept secure, by taking sensible precautions, e.g. using strong passwords, which should not be shared • Data should not be disclosed to unauthorised people, either within out outside the Trust • Data should be regularly reviewed and updated if it is found to be out of date • Data that is no longer required should be deleted and disposed of in accordance with the Document Retention requirements

Data	
Storage	These rules describe how and where data should be safely stored. Questions about storing data safely should be directed to the Data Protection Officer. When data is stored on paper, this should be kept securely where unauthorised people cannot see it The following guidelines also apply to data that is usually stored electronically, but has been printed out for some reason: • When not being used, the paper of riles should be kept securely • Paper and printouts should not be left where they can be seen by unauthorised individuals • Paper printouts should be shredded when no longer needs Where data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts: • Data should be protected by strong passwords, which are never shared between individuals • If data is stored on removeable media (e.g. memory sticks, external hard drives) these should be kept securely when not in use • Wherever possible data stored on an individual's laptop/desktop should be backed up on a regular basis and uploaded to The Trust's approved cloud storage • All personal laptops, desktops, tablets etc., should be protected by security software and a firewall
Use	Personal data is of no use to The Trust unless it can be made use of. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft. Therefore: • Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure • Where data is stored on an officer's own laptop, then they must ensure the security of the data – see previous section on storage
Accuracy	The law requires that The Trust takes reasonable steps to ensure data is kept accurate and up to date. The more important the data is, the greater the effort is that is put in to ensure its accuracy It is the responsibility of all individuals who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible • Data should be kept in as few places as is necessary • Data should be regularly checked to ensure it is updated as required • The Trust will make it easy for data subjects to update the information the Trust holds about them, e.g. via the website • Data should be updated as inaccuracies are discovered
Data retention	The period the Trust retain its data and documentation is detailed in the Document Retention Periods document

Subject access	
Subject entitlement	All individuals who are the subject of personal data held by The Trust are entitled to: • Ask what information the Trust holds about them and why • Ask how to gain access to it • Be informed how to keep it up to date • Be informed how the Trust is meeting its data protection obligations
Procedure for making request	Subject access requests must be in writing – letter or email. Email requests should be made via the website using the info@derbycanal.org.uk address.
Provision for verifying identity	Where the person managing the access procedure does not know the individual personally they should verify their identity before handing over any information.
Charging	The Trust will make a charge of £10 for each subject access request.
Timescales	The necessary information will be provided to the subject within 14 days of the request being made
Procedure for granting access	The normal provision is for the required information to be provided "in permanent form" – i.e. by letter
Other items	
Disclosing data for other reasons	In certain circumstances, the Data Protection legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject Under the above circumstances, the Trust will disclose requested data. However, the Trust will ensure that the request is legitimate, seeking assistance from the trustees and from the Trust's legal advisors, where necessary
Providing information	The Trust aims to ensure that individuals are aware that their data is being processed, and that they understand: • How the data is being used • How to exercise their rights To these ends, the Trust has a Privacy Statement, setting out how data relating to individuals is used by the Trust, which is available on the Trust's website