South Tees Development Corporation

Data Protection Policy

May 2020

South Tees Development Corporation

Contents

1. Introduction

This document covers South Tees Development Corporation's (STDC) policy on data protection. It outlines the principles of data protection and outlines the processes STDC follows to ensure information used by STDC is collected, stored, processed and disclosed in accordance with the law. It also outlines the important rights that the Data Protection Act provides all individuals (including members of staff), including the right to find out what personal information is held on computer and paper records. This Policy includes the requirements of the General Data Protection Regulation (GDPR) which replaced the current Data Protection Act 1998 on 25th May 2018.

2. Policy Statement

STDC will ensure that its policy upholds the rights and protects the interests of all those with whom the organisation has contact with, by protecting data and information in accordance with legislative and regulatory requirements and provisions. This will be achieved by ensuring that data processing and information exchange systems comply with the six principles of data protection.

STDC recognises that information relating to the activities of the organisation and its working practices should be made as widely available as possible in the interests of freedom of information (please refer to our FOI policy for further information). However whilst operating this policy, we must also recognise that some information may be sensitive or confidential and its release may prejudice the activities of STDC and the privacy of its employees. There are exceptions to Data Protection and exceptions to the rule when an individual exercises one of their 'Rights'.

STDC will ensure that all staff are trained to a high standard to enable them to carry out all their duties in line with legislation and this policy.

3. Regulation and Legislation

The Data Protection Act 2018 is in place to protect the personal data that organisations hold on staff and other individuals. To comply with the Act, STDC must act in accordance with six principles, which aim to ensure that personal information is:

a. Processed lawfully, fairly and in a transparent manner
b. Collected for specified, explicit and legitimate purposes
c. Adequate, relevant and limited to what is necessary
d. Accurate and, where necessary, kept up to date
e. Retained only for as long as necessary
f. Processed in an appropriate manner to maintain security

Under the Data Protection Act "personal data" means:

"Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller".

For the majority of information that we hold, STDC acts as the "Data Controller", i.e. we process information on behalf of staff and other individuals, and decide how best to process, store and secure that information. As a data controller we are registered with the ICO and our registration reference number is TBC. Further details can be accessed at www.ico.org.uk

STDC may also instruct others to process data on our behalf. This is called a “Data Processor” and is any company acting *on behalf* of STDC to process information. Where this is the case, STDC will have a contract with the company which clearly sets out how we expect them to process the information.

4. Roles and Responsibilities

The table below summarises the roles and responsibilities in relation to the Policy. It is important to note that the role of the Data Protection Officer is to provide advice to the organisation and to encourage effective processes. The responsibility for adhering to the regulations lies with each team, to ensure that they have full ownership of the data they process.

Roles	Responsibility
Directors	Accountable for ensuring: • adequate resource is available in the organisation to deal with the requirements of Data Protection and its procedures; • this Policy is implemented effectively and adhered to; • all staff are appropriately trained.
Data Protection Officer	Responsible for: • providing advice to the organisation; • encouraging effective implementation of the policy and its procedures; • ensuring the processes are updated according with the law.
All staff	Should have an awareness of this Policy and act in accordance with the procedures.

5. Records

Data Asset Register and Privacy Notices

In line with the regulations, STDC has produced an internal data asset register, and uses this information to produce and publish privacy notices, as appropriate. The information within the asset register and privacy notices has been developed by and is owned by each of the teams processing the data. They include the following information:

- WHY the personal data is processed i.e. the reason we process.
- WHO the information is about.
- WHAT specific information we are processing.
- WHEN are we processing that information from, and how long for.
- WHERE we are storing that information.
- If the information is shared outside of STDC, who it is shared with.
- Data subject rights.

Note that if information is stored outside of the European Economic Area (EEA), the location is checked against the countries that GDPR considers ‘adequate’, and if this is not the case, the issue is raised with the Data Protection Officer for consideration as to what information is stored, how sensitive it is and the risks considered.

The data asset register informs the risk register for STDC and is reviewed regularly.

Data Protection Impact Assessments (DPIAs)

Organisations are required to undertake DPIAs when undertaking any significant changes to the way they process personal data or when it may be about to take on a new set of personal data. This ensures that it upholds the principles of "privacy by design" and any new project considers and implements the principles of data protection from the beginning. The approach should be proportionate and therefore STDC will carry out DPIAs as and when required.

Note that in some circumstances the change may be assessed as so significant that it requires the approval of the Information Commissioner's Office. The Data Protection Officer will co-ordinate such discussions.

6. Subject Rights

Individuals have access to a set of 'Subject Rights' and can exercise them at any time. However, the rights of data subjects differ depending upon the legal basis for the processing of the information. The specific rights will be set out clearly in the privacy notices that STDC publish on their website separately to this policy. The full list of rights are as follows:

- Right to be notified
- Right to access
- Right to rectification
- Right to be forgotten
- Right to restrict processing
- Right to portability
- Right to object
- Right to restrict automated decision-making including profiling

In line with the regulations, most of the Subject Rights will be completed within 30 days (1 calendar month) and will be provided free of charge.

Those wishing to submit a data subject access request can do so by contacting:

Data Protection Officer
South Tees Development Corporation
Cavendish House
Teesdale Business Park
Stockton-on-Tees
TS17 6QY

or

DPO@southteesdc.com

7. Breach Management

There is a requirement under Data Protection to have a documented process to deal with a data breach. All breaches must be logged, and under certain circumstances, a breach must be reported to the Information Commissioner's Officer with 72 hours of STDC becoming aware of the breach. Having this

process in place helps in the understanding, damage limitation, evidence gathering, resolution and communication of a breach.

Staff should communicate with the Data Protection Officer immediately if a breach has taken place.

8. Monitoring and review

This Data Protection Policy will be reviewed every three years, or in line with legislation.

The accountability for this Policy lies with the Chief Executive Officer and responsibility for providing advice on, and updating this Policy, lies with the Data Protection Officer.

This policy may be subject to an audit in line with the internal audit plan. Elements of Data Protection activities across STDC are subject to management review and audit at any time to ensure that the Policy is being adhered to.