 [www.childandfamilysolutions.org.uk](http://www.childandfamilysolutions.org.uk/)

**Data Protection Policy**

**Policy Summary**

The company processes a high volume of personal data relating to its workforce and stakeholders (known collectively as data subjects). External third parties also process such personal data on behalf of the company. The company has a legal duty under data protection law to ensure the privacy of all data subjects by ensuring that their personal data is protected against unauthorised or unlawful processing and against accidental disclosure, loss, destruction or damage. All individuals and organisations who process personal data for or on behalf of the company are expected to comply with the company’s data protection policies and procedures.

**Purpose/Objectives**

This policy outlines the company’s commitment to the aims of data protection law and best practice. Compliance with this policy will therefore avoid and mitigate any data protection breaches by any individuals and organisations who process personal data for or on behalf of the company.

**Scope**

This policy applies to all individuals and organisation who process personal data for or on behalf of the company. This includes the workforce (i.e. employees, casual workers, agency workers and contractors), as well as external third parties (for example, suppliers to the company such as auditors). To that end, this policy applies (a) where the company is the Data Controller and/or joint Data Controller, and (b) where an external third party is the Data Processor and/or joint Data Controller. This policy has contractual status.

**Types of data**

Personal data is information which relates to a living person who can be identified from that data on its own, or when that data taken together with other information. For example, name, address, date of birth. It also includes any expression of opinion about that person and any indication of the company’s or others’ intentions in respect of that person. It does not include anonymised data.

Special category data is a type of personal data which is more sensitive than other personal data and which therefore requires additional protection. Special category data includes information about:

• racial or ethnic origin;

• political opinions;

• religious or philosophical beliefs;

• trade union membership;

• genetic or biometric data;

• health;

• sex life and sexual orientation; and

• criminal convictions and offences.

The company is committed to achieving a high standard of data protection for all personal data and special category data. (Both types of data are collectively referred to as “personal data” in the rest of this document unless specified otherwise).

**Principles**

All personal data will be processed in accordance with six ‘Data Protection Principles’ outlined in data protection law. As such, all personal data will:

• be processed fairly, lawfully and transparently;

• be collected and processed only for specified, explicit and legitimate purposes; • be adequate, relevant and limited to what is necessary for the purposes for which it is processed;

• be accurate and kept up to date. Any inaccurate data will be deleted or rectified without delay;

• not be kept for longer than is necessary for the purposes for which it is processed; and

• be processed securely.

The company will comply with these principles and will implement such processes and practices so as to prove compliance with these principles. Such compliance will also ensure the upholding of data subjects’ rights (see below).

**Data subject rights**

Data protection law gives data subjects certain rights in respect of their personal data. Data subjects therefore have the right:

• to be informed how their personal data will be processed (for example, via accessible privacy notices – see below) in language which is plain, concise, transparent and intelligible;

• of access to their personal data;

• to rectify their personal data if it is incorrect or incomplete;

• to erase their personal data;

• to restrict the processing of their personal data;

• to be given their personal data in a portable form to be able to reuse their personal data for their own purposes across different services;

• to object to the processing of their personal data;

• not to be subject to automated decision making (i.e. where decisions are made solely by automated means and without any human involvement).

Some of the rights are not absolute and therefore will not automatically apply when a data subject seeks to exercise their rights. The company will implement procedures to facilitate the exercise of these rights by data subjects, although the company will give written reasons if it believes that any given does not apply.

**Accountability**

The company will implement appropriate technical and organisational measures to ensure compliance with data protection law and also to prove such compliance. These include:

• producing clear, comprehensive data protection and data security policies and procedures;

• implementing data protection by design so as to pre-empt data protection breaches using Data Protection Impact Assessments where appropriate;

• putting written agreements in place with external third parties who act in the capacities of Data Processors or Data Controllers and/or Joint Data Controllers;

• maintaining documentation of processing activities;

• implementing appropriate cyber and IT security measures;

• recording, and where necessary, reporting data breaches;

• appointing a Data Protection Officer where necessary;

• providing data protection training; and

• writing privacy notices (which, among other things, explain to data subjects how The company will process and protect their personal data).

**Responsibilities**

**Board and Company Directors**

The Board and company directors have overall responsibility for ensuring that the organisation complies with its legal obligations.

**Data Protection Officer**

The Data Protection Officer occupies an important place in the governance of data protection in the company. The duties include:

• informing and advising the Board and staff of their obligations to comply with data protection law and other data protection laws;

• monitoring compliance with data protection law and with our data protection policies, including internal data protection activities, raising awareness of data protection issues, training staff and conducting internal audits;

• advising on and monitoring Data Protection Impact Assessments; and

• acting as the first point of contact for the Information Commissions Office (ICO) including the reporting of breaches.

**The workforce (i.e. employees, casual workers, agency workers and contractors)**

Any member of the workforce who processes personal data will abide by this policy so as to ensure that any personal data with which they work, is protected.

**Definitions and Abbreviations**

**Data Controller:** the individual or organisation which determines the purpose for which, and the manner in which, personal data is processed.

**Data Processor:** the individual or organisation which processes personal data on behalf of a Data Controller.

**Joint Data Controller:** the individuals or organisations who jointly determine the purposes for which, and the manner in which, personal data is processed.

**Processing:** subjecting personal data to any form of activity (including collecting, storing, analysing, transferring, archiving or destroying).