



Data Protection & Subject Access Policy

RIGHTS:

In order to operate efficiently, we must collect information about people with whom we work. These may include members of the public, current, past and prospective employees, customers, clients and suppliers. In addition, we may be required by law to collect and use information in order to comply with the requirements of central government. Data [specifically photographs and video] may also be collected as a record in relation to works.

This personal information must be handled properly under legislation which regulates the way that we handle personal data that we collect in the course of our business and gives certain rights to people whose personal data we may hold. Under GDPR (and Data Protection Acts 1998 & 2018), Individuals have rights enshrined in EU and UK Law:

These rights are:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

We consider that the correct treatment of personal data is integral to our successful operations and to maintaining trust of the persons we deal with. As an ethical business, we fully appreciate the underlying principles of the relevant laws and support and we are committed to full compliance of their requirements.

The Acts use the term 'personal data' and 'personally identifiable information'. For information held by us, this means any recorded information held by us and from which a living individual can be identified. It will include a variety of information including names, addresses, telephone numbers, photographs of people and other personal details. It may also include any expression of opinion about a living individual or any indication of our intentions about that individual.

PRINCIPLES:

We will comply with the eight enforceable data protection principles by making sure that personal data is:

1. captured in an open manner, adequate, relevant and not excessive
2. fairly and lawfully processed in accordance with the individual's rights, for limited / specific purposes
3. held securely, maintained as accurate and up-to-date, but held for no longer than necessary



4. not stored in, or transferred to, countries outside the European Economic area unless the country to which the data is to be transferred has adequate protection for the individuals

and that at least one of the following conditions are met before we process any personal data:

1. the individual has consented to the processing
2. the processing is necessary for the performance of a contract with the individual, or required under a legal obligation
3. the processing is necessary to protect vital interests of the individual or carry out public functions e.g. administration of justice
4. the processing is necessary in order to pursue our legitimate interests or those of third parties (unless it could unjustifiably prejudice the interests of the individual)

SUBJECT ACCESS RIGHTS

Any individual who makes a valid subject access request is entitled to be:

1. told whether their personal data is being processed
2. given a description of the personal data, reason for processing and whether it has been shared with any other organisations or persons
3. given details of the source of the data (where this is available)
4. given a copy of the information comprising the data

A register of these requests is required to be held, together with the result of the requests. Individuals are entitled only to their own personal data, and not to information relating to other people unless they are acting on behalf of that person. In all circumstances, written consent incl by email from a verifiable account will be required.

EXEMPT INFORMATION

We may not be able to release some information. Information which is exempt from a subject access request includes:

1. personal data where disclosure could prejudice the prevention or detection of crime
2. management forecasts/management planning
3. legal professional privilege (advice received from solicitors, for example)
4. personal data identifying another person (a third party) whose details cannot be disclosed without their permission

OUR COMMITMENT

We will take all necessary steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and everyone managing and handling personal information understands that they are responsible for following good data protection practice. We will ensure that:

1. there is someone with specific responsibility for data protection in the organisation
2. staff who handle personal information are appropriately supervised and trained



3. queries about handling personal information are promptly and courteously dealt with
4. methods of handling personal information are regularly assessed and evaluated
5. any disclosure of personal data will be in compliance with approved procedures.

Approve By:

Jim Gildea, Managing Director
01 August 2019