Data Protection Policy

INTRODUCTION

Cubby Construction Ltd ("Cubby") regards the lawful and correct processing of personal and sensitive data as an integral part of its purpose. Cubby believes this is vital for maintaining the confidence of employees and other stakeholders about whom we process data, and ourselves.

POLICY STATEMENT

This Data Protection Policy explains how Cubby will meet its legal obligations concerning confidentiality and data security standards. The requirements within the policy are primarily based upon the EU General Data Protection Regulation (EU GDPR), which is the key piece of legislation covering data security and confidentiality of personal and sensitive personal data in the European Union.

Cubby will fully implement all aspects of the EU GDPR.

Cubby will ensure all employees and others handling personal data are aware of their obligations and rights under the EU GDPR.

Cubby will implement adequate and appropriate physical and technical measures and organisational measures to ensure the security of all data contained in or handled by its staff and systems.

The main focus of this policy is to provide guidance about the protection, sharing and disclosure of personal data, but it is important to stress that maintaining confidentiality and adhering to data protection legislation applies to anyone handling personal data or personal sensitive data on behalf of Cubby.

REGISTRATION WITH THE INFORMATION COMMISSIONER

The Digital Economy Act 2017 requires every data controller (i.e. organisation) in the UK to pay a fee to the Information Commissioner's Office (ICO) and outline the categories of data they hold about people, and what they do with it.

Cubby is registered with the ICO to '...process personal information to enable us to carry out our business and management services; promote and advertise our services; maintain our own accounts and records; and support and manage our employees'. We also process personal information to enable us to provide education and training to our customers and clients.'?

Definitions of Personal Data and Sensitive Personal Data

All identifiable employee data
All identifiable client data
All identifiable supplier data
All other personal data processed by Cubby

Examples of personal identifiable data Cubby processes include:
Names, addresses, emails, phone numbers and other contact information
Employee numbers
National insurance numbers and payroll data
Photographs, video and audio recordings
Certain types of data are regarded as sensitive and attract additional legal protection. Sensitive personal data is considered to be any data that could identify a person such as:

- The racial or ethnic origin of the individual
- Political opinions or affiliations
- Religious beliefs or other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence
- Any proceeding for any offence committed or alleged to have been committed or disposal of such proceedings or the sentence of court in such proceedings
- Bank account details, any official identification details such as passport or driving licence numbers etc.

DATA PROTECTION PRINCIPLES
The eight Data Protection principles that lie at the heart of the EU GDPR give the Regulation its strength and purpose. To this end, Cubby fully endorses and abides by the principles of data protection. Specifically, the principles require that:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure

Not transferred to other countries without adequate protection

Fairly and lawfully processed in a transparent manner in relation to individuals;

Processed for limited purposes collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

Adequate, relevant and not excessive and limited to what is necessary in relation to the purposes for which they are processed;

Accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that inaccurate personal data, having regard to the purposes for which it was processed, is erased or are rectified without delay;

Not kept for longer than necessary and, kept in a form which permits identification of the data subjects, for no longer than is necessary for the purposes for which the personal data was processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals, and;

Processed in line with your rights data processed is in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Personal data and sensitive personal data must not be used other than for the specific purpose required to deliver a product or service. The individual should always know that their data is being processed. When that data is especially sensitive, consent is required before the data can be processed by Cubby. All data collected from people under the age of 16 (unless there are concerns about mental capacity in which case this should be extended) is to be treated as sensitive personal data.

Not transferred to a country or territory outside the EEA without adequate protection – personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Any transfer of personal date outside the UK shall only take place if it complies with the GDPR.

This means that data can be freely transferred to those non-EEA countries that have been approved by the European Commission as having adequate data privacy laws, including Argentina, Canada, Switzerland, the Channel Islands, Isle of Man, Israel and New Zealand. Data can only be freely transferred to any US businesses that have signed up to the EU-US Privacy shield framework. If none of those apply, then the data controller must assess whether the protection afforded to data subjects in the recipient's country is "adequate in all the circumstances of the case".

RECORDS

A record can be in computerised and/or in a physical format. It may include such documentation as:

- Manually stored paper files e.g. membership records, employee records
- Hand written notes
- Letters to and from Cubby
- Electronic records
- Printouts
- Photographs
- Videos and tape recordings
- Backup data (i.e. archived data or disaster recovery records) also falls under the DPA; however, a search within them should only be conducted if specifically asked for by an individual as an official Subject Access Request

RIGHTS OF ACCESS BY INDIVIDUALS

The EU GDPR gives every living person (or their authorised representative) the right to apply for access to the personal data which organisations hold about them irrespective of when and how they were compiled,

i.e. hand written records, electronic and manual records held in a structured file. This is called a Subject Access Request. The EU GDPR treats personal data relating to employees, clients and suppliers alike.

PRACTICAL IMPLICATIONS

Understanding and complying with the eight Data Protection Principles is the key to understanding and complying with Cubby's responsibility as the data controller. Therefore, Cubby will, through appropriate management, and strict application of criteria and controls:

- Ensure that there are lawful grounds for using the personal data
- Ensure that the use of the data is fair and meets one of the specified conditions
- Only use sensitive personal data where we have obtained the individual's explicit consent (unless an exemption applies)
- Only use sensitive personal data, if it is absolutely necessary
- Explain to individuals, at the time their personal data is collected, how that information will be used
- Only obtain and use personal data for those purposes which are known to the individual
- Ensure personal data is only used for the purpose it was given. If we need to use the data for other purposes, further consent will be obtained.
- Only keep personal data that is relevant to Cubby
- Keep personal data accurate and up to date
- Only keep personal data for as long as is necessary
- Always adhere to our Subject Access Request Procedure and be receptive to any queries, requests or complaints made by individuals in connection with their personal data
- Ensure individuals are given the opportunity to 'opt in' to receiving mass communications
- Take appropriate technical and organisational security measures to safeguard personal data.
- There is an employee appointed as the Security Information Risk Owner with specific responsibility for Data Protection in Cubby. This is currently **the Human Resource Manager**.

Everyone managing and handling personal data and sensitive personal data understands that they are legally responsible for following good data protection practice and has read and signed Cubby's Data Protection Policy.

Everyone managing and handling personal data and sensitive personal data is appropriately supervised by their line manager.

Enquiries about handling personal data and sensitive personal data are dealt with promptly.

Methods of handling personal data and sensitive personal data are clearly described in polices and guidance.

A review and audit of data protection arrangements is undertaken annually. This will take place each year in **May.**

Methods of handling personal data and sensitive personal data are regularly assessed and evaluated by the Security Information Risk Owner and relevant members of the Management Team.

Performance with personal data and sensitive personal data handling is regularly assessed and evaluated by the Security Information Risk Owner and relevant members of the Management team.

Formal written Data Processing Agreements are in place before any personal data and sensitive personal data is transferred to a third party.

ROLES AND RESPONSIBILITIES

Maintaining confidentiality and adhering to data protection legislation applies to everyone at Cubby. Cubby will take necessary steps to ensure that everyone managing and processing personal data understands that they are responsible for following good data protection practice. Employees will receive training and sign Cubby's Data Protection Policy as part of their induction. Contractors will also be asked to sign the policy and will undertake **an online training course(?)**

All employees, clients, suppliers and contractors have a responsibility to:

- Observe all guidance and codes of conduct in relation to obtaining, using and disclosing personal data and sensitive personal data
- Obtain and process personal data and sensitive personal data only for specified purposes
- Only access personal data and sensitive personal data that is specifically required to carry out their activity or work
- Record data correctly in both manual and electronic records
- Ensure any personal data and sensitive personal data is held is kept secure
- Ensure that personal data and sensitive personal data is not disclosed in any form to any unauthorised third party
- Ensure personal data and sensitive personal data is sent securely
- Read and sign the policy, directing any questions to the **Human Resource Manager**.

All Managers are responsible for:

- Determining if their operational area holds personal data and sensitive personal data and ensuring that the data is adequately secure, access is controlled and that the data is only used for the intended purposes
- Providing clear messaging to their teams about data protection requirements and measures
- Ensuring personal and sensitive personal data is only held for the purpose intended
- Ensuring personal and sensitive personal data is not communicated or shared for non-authorised purposes
- Ensuring personal and sensitive personal data is password protected when transmitted or appropriate security measures are taken to protect when in transit or storage.

Security Information Risk Owner – The Human Resource Manager holds the post of Security Information Risk Owner. Responsibilities include:

- Ensuring compliance with legislation principles
- Ensuring notification of processing of personal data and sensitive personal data to the ICO is up to date
- Providing guidance and advice to employees in relation to compliance with legislative requirements
- Auditing data protection arrangements annually
- Reporting on any breaches of Data Protection legislation
- Ensuring those handling personal data are aware of their obligations by producing relevant policies, auditing the arrangements and ensuring the relevant people receive training
- Overall responsibility for Data Protection within Cubby. Cubby has a duty to ensure that the requirements of the DPA are upheld.

The Information Commissioner's Office (ICO)
The Information Commissioner's Office is responsible for overseeing compliance e.g. investigating complaints, issuing codes of practice and guidance, maintaining a register of Data Protection Officers. Any failure to comply with DPA may lead to investigation by the ICO which could result in serious financial or other consequences for Cubby.

Breach of Policy
In the event that an employee fails to comply with this policy, the matter may be considered as misconduct and dealt with in accordance with Cubby's Disciplinary Policy.

Any individuals or organisations with whom Cubby data has been shared may be personally liable for any breach of the EU GDPR.

Dealing with a Data Breach
If a data breach is suspected, the person who identified the breach should immediately:
Notify the Human Resource Manager
Complete and return the Data Incident Reporting Form, which is available from the Security Information Risk Owner.
Following notification of a breach, the Security Information Risk Owner will take the following action as a matter of urgency:
Implement a recovery plan, which will include damage limitation
Assess the risks associated with the breach
Inform the appropriate people and organisations that the breach has occurred
Review Cubby's response and update our information security

GLOSSARY OF TERMS
Data Subject. An individual who is the subject of personal data or sensitive personal data. This includes employees, members, volunteers, clients, residents and tenants.

Data Controller. A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data and sensitive personal data are, or are to be processed. The data controller is Cubby.

Data Processor. In relation to personal data or sensitive personal data, this refers to any person who processes that data on behalf of the data controller but it is not employed by them. Data Processors include but are not limited to mailing houses to which Cubby sends mailing lists and external companies who have access to Cubby's data.

Third Party. In relation to personal data or sensitive personal data, this refers to any person other than the data subject, the data controller, or any data processor or other person authorised to process data for data controller or processor. For example, the Police or HMRC.

Processing. Recording or holding data or carrying out any operations on that data including organising, altering or adapting it; disclosing the data or aligning, combining, blocking or erasing it.

Data Extractor. The person who takes data from a data source, such as a database, which may then be used for further activity. For example, an employee querying the database to print a list of address labels for letters.

Data Breach. A failure leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or sensitive personal data.

Subject Access Request. A written, signed request (which includes email and other written formats) from an individual to see data which Cubby holds about them. The Data Controller must provide all such information in a readable form within 1 month of receipt of the request.

Failure to adhere to any guidance in this policy could mean an individual(s) being criminally liable for deliberate unlawful disclosure under the EU GDPR. This may result in criminal prosecution and/or disciplinary action.