

C & D Decorators Limited
Data Protection and Security Policy

EXECUTIVE SUMMARY

- The Company needs to hold all personal and sensitive data securely; this policy sets out how and why. It is applicable to all staff and covers use of customer/supplier data as well as data we hold on individuals as employees.
- The policy covers both data held electronically as well as hard copy records.
- We have legal requirements under General Data Protection Regulation (GDPR), as this gives individuals rights to ask us what data we hold. We have to respond to such requests within a strict and challenging timetable. The penalties for non-compliance with GDPR are fines of up to €20million or 4% of sales revenues of the Company.
- Staff are responsible for applying parts of this policy, as they will collect and use Personal Data from customers/employees/suppliers.
- We must be able to show that Personal Data is:
 - fairly, lawfully and transparently processed;
 - processed for specific, explicit and legitimate purposes;
 - adequate, relevant and not excessive for our purpose;
 - kept accurate and up to date;
 - not be kept for longer than is necessary;
 - processed in accordance with individuals' rights;
 - kept securely to prevent unauthorised processing and accidental loss, damage or destruction.
- We will train staff to understand how this impacts on your job role.
- We will put in place arrangements with any external parties (e.g. payroll processors) who use our data to keep it secure.
- We have put in place retention policies to manage what data we retain and for how long staff will be required to comply with these. The periods for which we will hold personal data in respect of employees are set out in Schedule 1.
- Individuals are entitled to request access, deletion or correction of personal data held about themselves. Any such request should be passed immediately to the Registered Office (Schedule 1).
- If our Personal Data security is breached, we are required to notify affected users within 72 hours of the impact. A Data breach may arise from lost papers or laptops, as well as more sophisticated electronic forms of attack. Any Data Breach you become aware of must therefore be reported IMMEDIATELY to a Director.

C & D Decorators Limited
Data Protection and Security Policy

1. Policy Statement

The aim of this policy is to ensure all personal and sensitive data the Company holds is dealt with in a secure, confidential and accurate manner.

The Company's policy is to process personal data in accordance with the applicable data protection laws and rights of individuals as set out below. The Company understands and endorses the requirements of data protection laws and codes of practice.

The Company holds personal data about staff, customers, suppliers and other individuals for a variety of business purposes.

This policy sets out how the Company seeks to protect personal and sensitive data and covers two areas:

- (a) personal data which staff may have access to within the course of their work;
- (b) personal data of staff. The Company respects the rights of its employees to privacy within the workplace and works to balance this with the need to ensure compliance with Company Rules. Access to any data held by the Company will be provided in compliance with data protection laws.

All staff have personal responsibility for the practical application of this policy.

2. Scope

This policy applies to all staff, as defined below. This policy supplements the Company's other policies relating to IT usage and document retention.

This policy does not form part of your contract of employment. The Company will review this policy annually, and issue interim guidelines as required. Present day staff will be required to confirm their acceptance and understanding of this policy on an annual basis.

The Company may ask any member of staff to take part in training on data protection issues at any time and staff must do so when requested.

3. Definitions

In this policy:

- | | |
|----------------------------|--|
| "business purposes" | means the purposes for which personal data may be used by the Company, e.g. personnel, administrative, financial, regulatory, payroll and business development. |
| "Company" | means C & D Decorators Limited registered in England and Wales with company number 6530325 whose registered office is at 146 Spinney Hill Road, Northampton NN3 6DN. |
| "personal data" | means information relating to a living individual, such as job applicants, current and former employees, agency, subcontract, contract and other staff, customers, clients, suppliers, and marketing contacts who can be identified from that data or from that data and other information which the Company has or is likely to have. This can include name, address, email address, financial information, location data, aliases, preferences and |

C & D Decorators Limited
Data Protection and Security Policy

profiles, amongst other things.

- "processing"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, organisation, structuring, storage, adaption or alternation, retrieval, consultation, use, or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "sensitive personal data"/"special categories"** means personal data about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data for the purpose of uniquely identify a person, data concerning physical or mental health or condition, sexual life, criminal offences, or related proceedings. Any use of sensitive personal data must be strictly controlled in accordance with this policy.
- "Staff"** means all directors, employees (current and former), subcontractors, and contract workers, of the Company, including applicants and former applicants.
- "ICO"** means the independent regulatory body responsible for monitoring the application of data protection law in the UK, being the Information Commissioner's Office.

4. Collection of Personal Data

The Company collects the following personal data:

- (a) in relation to staff:
- name contact details, bank details, equality and diversity details.
 - information before, during and after any application and/or interview process.
 - information during any period of employment or arrangement, including absences, holidays, personal reviews, disciplinary action and back to work interviews, accidents and training.
 - information in connection with payroll, expenses and benefits (e.g. pensions).
 - information on dismissal, redundancy, resignation or retirement.
 - information on driving licences, insurance, previous convictions.
- (b) in relation to other individuals:
- name and contact details of staff family members, emergency contacts and next of kin.
- (c) in relation to customers and suppliers:
- information including name, contact details and bank details.
 - information in connection with the provision of goods, services and credit facilities, contact with such parties in the negotiation for goods and services and as part of managing such relationships.

5. General Principles

In the course of your work you may come into contact with and use confidential personal information about people, such as names and addresses or even information about customers'

C & D Decorators Limited

Data Protection and Security Policy

circumstances, families, health and other private matters. The guidelines set out in this policy are to ensure you do not breach data protection laws.

The Company holds personal data about you, for the stated purposes which are set out in Schedule 1 of this Policy. If this information changes, you should let us know so that our records can be updated.

Data protection laws require that the following principles must be followed in the handling of personal data. These are that personal data must:

- be fairly, lawfully and transparently processed;
- be processed for specific, explicit and legitimate purposes and not in any manner incompatible with those purposes;
- be adequate, relevant and not excessive in relation to the purposes for which it is used;
- be kept accurate and up to date (and where inaccurate are erased and rectified without delay);
- not be kept for longer than is necessary for the purposes for which it is used;
- be processed in accordance with individuals' rights;
- be secure in order to prevent unauthorised processing and accidental loss, damage or destruction, using appropriate technical or organisation measures.

Staff should generally not process personal data unless:

- the individual whose details are being processed has consented to this;
- it is to fulfil a contract with the individual (be this a customer, supplier or member of staff);
- the processing is necessary to perform the Company's legal obligations or exercise legal rights; or
- the processing is otherwise in the Company's legitimate interests and does not unduly prejudice the individual's privacy.

6. Administration

The Company will ensure that all internal staff involved in processing personal data are trained in compliance with the requirements of data protection laws.

The Company will ensure that all personal information will be held in a secure system and access will be restricted only to those staff processing data. Personnel files will be held in a central system; staff personal data will not be held by individual managers. Access to personnel records will be controlled and accessed only by authorised managers. Customer and other sensitive information will be held in a secure system and accessed only by authorised staff. Managers will be informed about their obligations under data protection laws.

From time to time the Company may carry out an audit of all personal data and/or customer records to ensure their handling is in line with the general principles set out above.

7. Accuracy, Adequacy, Relevance and Proportionality

Staff should make sure data processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

Individuals may ask the Company to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal

C & D Decorators Limited
Data Protection and Security Policy

data held is inaccurate, they should nevertheless record the fact that it is disputed and inform a Director.

Staff must ensure that personal data held by the Company relating to them is accurate and updated as required.

8. Security

Information security is a key element of data protection and the Company must ensure that appropriate measures are taken to keep personal and sensitive data secure from loss or unauthorised disclosure or damage.

All staff must ensure they comply with the IT Usage policy when using the Company's IT systems and otherwise when processing personal and sensitive data. Staff have a responsibility to ensure any third parties to whom any personal data is disclosed is transferred securely and kept securely by such third party.

Where the Company uses external organisations (e.g. payroll agencies) to process personal data on its behalf additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. There are also mandatory legal protections which must be included in any contract with such parties.

Staff should consult a Director to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement.

9. Data Retention

Personal data should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data were obtained. Staff should follow the Company's data retention guidelines as set out in the Data Retention policy.

In relation to a member of staff's personal data held by the Company, please refer to the retention periods set out in paragraph 4 of, and the Appendix to Schedule 1 of this policy.

10. Rights of Individuals

Individuals are entitled (subject to certain exceptions) to request access, rectification, deletion, restriction and portability in relation to information held about them. All such requests should be referred immediately to a Director. This is particularly important because the Company must respond to a valid request within the legally prescribed time limits.

The rights of staff in respect of their personal data are set out at Schedule 1 to this policy.

11. Reporting Breaches

Staff have an obligation to report actual or potential data protection compliance failures to a Director. This allows the Company to:

- investigate the failure and take remedial steps if necessary; and
- make any applicable notifications.

You may be requested as part of your duties to support the Company in any such investigation.

12. Consequences of Failing to Comply

The Company takes compliance with this policy very seriously. Failure to comply puts both staff and the Company at risk.

Staff with any questions or concerns about anything in this policy including any of its Schedules and Appendices should not hesitate to discuss these with a director.

SCHEDULE 1

EMPLOYEE PERSONAL DATA

PART 1

PRIVACY NOTICE

Any personal data processed as part of a staff member's recruitment or employment with the Company will be processed in line with this policy and in accordance with Part 2 of this Schedule 1.

PART 2

PRIVACY POLICY

1. INTRODUCTION

- 1.1 The Company values the privacy of our staff. This part of the policy sets out in more detail our practices in relation to the collection and use of your personal data.
- 1.2 The controller of your personal data is the Company, being your employer as set out in your employment contract / terms of employment.
- 1.3 The Company is responsible for ensuring the application of this policy and protecting your personal data. If you have any questions or concerns around how your personal data is being collected, used or stored, please discuss this with a Director.
- 1.4 The Company processes your personal data in order to discharge its obligations as an employer (for both our own legitimate interests and yours) and to fulfil our contract with you.
- 1.5 Your personal data will only be processed in accordance with data protection laws and for the purposes set out in paragraph 1.6 and the Company will not process your personal data in any manner incompatible with those purposes unless we are required by law to do so. We will also endeavour to comply with any ICO code of practice on the use of personal data in employee/employer relationships.
- 1.6 The Company holds and processes the personal data of staff (and next of kin) for human resources administration and management purposes, including:
 - 1.6.1 recruitment;
 - 1.6.2 discipline and complaints;
 - 1.6.3 training and development;
 - 1.6.4 other employment benefits, such as death in service and medical insurance and pensions, which may include processing the personal data of next of kin, family or friends;

C & D Decorators Limited
Data Protection and Security Policy

- 1.6.5 performance reviews and management;
- 1.6.6 remuneration payments including payroll, tax and national insurance;
- 1.6.7 health and safety;
- 1.6.8 sickness, family, maternity and paternity leave;
- 1.6.9 promotions or career development;
- 1.6.10 to fulfil statutory reporting requirements;
- 1.6.11 in the case of next of kin, family or friends for emergency contact purposes;
- 1.6.12 all other applications of the Company's policies and other terms and conditions of employment.

1.7 Please note that a refusal by you to provide the Company with the relevant personal data required to carry out the purposes listed above, will significantly hinder the Company's ability to provide you with your employment rights and benefits.

2. COLLECTION, USE AND ACCURACY

2.1 Good employment practice and the efficient running of the business require the Company to hold certain personal details about you on file. These personal details may include special categories of personal data about you, such as information on your health, racial or ethnic origin or marital status.

2.2 The Company obtains personal information about you from a number of sources including the application form or CV you submitted when you applied to join, from interview notes and from any details you subsequently provide us. We will also keep records of, for example, your absence history, your regular performance reviews and any actions or decisions taken as a result of applying any of our policies (in accordance with the terms of the relevant policy).

2.3 Within the Company, Director's and HR personnel will have access to your personal information. Access to your personal information will only be given to those who strictly need such access.

2.4 The Company will use the information held about you for purposes connected to your employment. For the purposes set out in paragraph 1.6 the Company may transfer personal data to third parties.

These third parties include: insurers and insurance brokers; legal advisors; professional advisors; auditors, pension schemes, payroll suppliers and tax authorities.

2.5 Personal data may be shared with other third parties at a member of staff's own request.

2.6 In line with the policy, the Company will make every effort to ensure that the information held about each member of staff is accurate and, where necessary, kept up to date. It is your responsibility to ensure that your information contained with HR is accurate and kept up to date. In the absence of evidence to the contrary the Company shall assume that the information provided by you is accurate. If there is any reasonable doubt as to the accuracy of the data, the Company shall contact you to confirm the information. Should

C & D Decorators Limited
Data Protection and Security Policy

you inform us, or the Company otherwise becomes aware, of any inaccuracies in the information, the inaccuracies shall be rectified promptly.

2.7 A member of staff must not pass any personal data relating to a colleague to any other person unless specifically authorised to do so by that person.

2.8 Personal data may be shared between:

2.8.1 the parties listed in paragraph 2.3 above; and / or

which may involve the sharing of your personal data outside of the EEA.

2.9 The Company is able to share your personal data as set out above as it has:

2.9.1 an agreement in place between the Company and third-party suppliers of the Company in relation to where personal data is to be, on terms which protect such data and allow it to be shared outside of the EEA with such parties; and

3. MONITORING AND SECURITY

3.1 The Company may monitor electronic communications by staff.

3.2 The Company is ultimately responsible for all business communications but, so far as possible; staff members' privacy will be respected.

3.3 Any emails which are not stored in your "Personal" folders in your mailbox and which are not marked "PERSONAL" in the subject heading will be treated, for the purpose of monitoring, as business communications.

3.4 The Company has put in place measures to ensure the security of the information collected and its correct use. These are appropriate to the nature of the information and to prevent unauthorised access.

4. RETENTION

4.1 The Company keeps staff members' personal employment files in soft/online format and hard copy.

4.2 The employment records/pensions and benefits records extract from the Retention Policy is set out within the Appendix to this Schedule 1. A copy of our Retention Policy can be found on request from a Director.

5. DATA PORTABILITY

5.1 You are entitled to receive the personal data concerning you, which you have provided to the Company, in a structured, commonly used and machine-readable format

5.2 You have the right to transmit the personal data to another data controller, without hindrance where the processing is based on consent or the processing is carried out by automated means.

5.3 We do not consider that you will have a specific right to data portability in the context of your employment or engagement as processing will not be carried out on the basis of consent, and no automated processing is carried out in respect of staff.

PART 3

YOUR RIGHTS – STAFF QUESTIONS AND ANSWERS

To exercise your rights as employees under this Schedule 1, you should apply in writing to a Director.

1. ACCESS YOUR PERSONAL DATA

What happens next?

Your request will be dealt with promptly and the information to which you are entitled will be provided to you no later than one month (except in extenuating circumstances) from when we receive your request, subject to the requirements and exemptions of data protection laws. If such extenuating circumstances mean we are unable to comply with your request within one month, we will tell you as soon as possible about this delay.

Examples of exceptions, where the Company (by law) does not provide access to data include:

- References written by the Company;
- Any data from which a third party can be identified, unless it is possible to remove the identifying elements (e.g. by way of redaction);
- Any data held for the purposes of management forecasting or planning if access to the same is likely to prejudice the conduct of the Company's business;
- Any data prejudicing ongoing negotiations with the employee;
- Any data protected by legal professional privilege; and/or
- Any data regarding an employee's health which an appropriate health professional considers likely to cause serious harm to the employee's physical or mental health or of any other person.

2. REQUEST YOUR DATA IS RECTIFIED

When?

You should request that your data is rectified either where the personal data is inaccurate or to request we complete any incomplete information (e.g. by way of supplementary statement).

What happens next?

Your request will be dealt with promptly and without undue delay.

3. REQUEST YOUR DATA IS DELETED

When?

You have a right to request the Company deletes information held about you in certain circumstances (e.g. where we no longer have the right to process the information). If you wish the Company to delete some (or all) of your personal data, you should apply in writing to the Registered Office.

What happens next?

Your request will be dealt with promptly and without undue delay, subject to the requirements and exemptions of the data protection laws. In some circumstances the Company will be unable to comply with your request, for example if the Company has legal duties or obligations to continue processing the data. It is unlikely the Company will be able to erase certain information whilst you remain an employee of it, as it will be necessary for the purposes of your continuing employment and to meet our obligations in relation to tax and other regulatory duties. This will be addressed on a case by case basis following a request for erasure.

4. RESTRICT OR OBJECT TO PROCESSING

When can I obtain from the Company a restriction of processing?

You may request a restriction of processing your personal data where:

- you contest the accuracy of the personal data (and so processing will be restricted for a period of time which will enable the Company to verify the accuracy of the personal data);
- the processing is unlawful, and you oppose the erasure of personal data and request restriction instead;
- the Company no longer needs the personal data for the purposes of the processing, but they are required by you for the establishment, exercise or defence of a legal claim;
- you have objected to the processing on the basis of the Company's legitimate interests pending the verification of whether such legitimate grounds override yours.

What does restriction mean?

With the exception of data storage, the Company will only be able to process the personal data with your consent or for the establishment, exercise or defence of legal claims or for the protection of another natural or legal person or for reasons of important public interest.

When can I object to the Company processing my Personal Data?

You can object to the Company processing your personal data where the Company is processing your personal data on the basis of its legitimate interests, including profiling. To the extent the Company cannot demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms the Company will no longer process your personal data for these purposes.

5. COMPLAIN

To the Company

C & D Decorators Limited
Data Protection and Security Policy

If you have a complaint or concern around the use of your personal data in the context of your employment or engagement with the Company, please discuss this with a Director.

To the ICO

In the event you are dissatisfied with the response of the Company, you have the right to complain to the ICO as set out below.

Information Commissioner (ICO):

Website/email: <https://ico.org.uk/concerns/>

Address: Wycliffe House, Water Lane, Wilmslow SK9 5AF

Helpline: 0303 123 1113.

APPENDIX

RETENTION PERIODS FOR STAFF PERSONAL DATA

Employment records	
Employee files including disciplinary cases records	For the duration of employment and 6 years after employment ceases.
Employee welfare records	For the duration of employment and 6 years after employment ceases.
Annual leave records	For the duration of employment and 6 years after employment ceases.
Travel and subsistence records - claims and authorization	For the duration of employment and 6 years after employment ceases.
Statutory Maternity Pay records	For the duration of employment and 6 years after employment ceases.
Other maternity pay documentation	For the duration of employment and 6 years after employment ceases.
Statutory paternity pay records	For the duration of employment and 6 years after employment ceases.
Unsuccessful candidates: application forms, CVs, references, interview notes, correspondence	Delete after 12 months from the date of appointment of the successful candidate.
Successful candidates: all other recruitment documentation	For the duration of employment and for 6 years after employment ceases.
Identification documents of foreign nationals (ensuing from the obligation to retain copies of documents used to perform immigration checks)	For the duration of employment and 6 years after employment ceases.
Redundancy details, calculations of payments, refunds	6 years from date employment ceases
Wages and Salary data	At least 6 years after the end of the financial year to which the records relate.
Written particulars of employment, contracts of employment, and changes to terms and conditions	For the duration of employment and for 6 years after employment ceases.
Consents for the processing of sensitive personal data (where applicable)	For as long as the data is processed + 6 years
Pensions and benefits records	
Record of advances.	6 years after repayment

C & D Decorators Limited
Data Protection and Security Policy

Employer pension records re, automatic enrolment, additional information for jobholders and worker's joining notice and details regarding any personal pension schemes	6 years
Jobholder's opt-in notice, date worker became an active member, details of pension scheme	6 years (must be retained in original format)
Jobholder's opt-out notice	4 years (must be retained in original format)
Pension scheme records including all pension scheme trust deeds and rules and revenue approvals	Life of the scheme (originals must be retained)
Pension scheme investment policies	12 years after final cessation of any benefit payable under the policy
Disputes procedures	For the duration of employment and 6 years after employment ceases.
Occupation pension scheme – minutes of meetings of trustees	12 months after meetings

CONFIRMATION

I have read and understood this policy.

Signed.....

Dated.....