

BALCOMM LIMITED

*Commissioning, Ductwork Cleaning
& Water Treatment*

GDPR

DATA PROTECTION POLICY

The Company	Refers to Balcomm Ltd as responsible as the data controller
The Client	Refers to all organisations doing business with The Company
The Employee	Refers to all persons employed by The Company
The Subcontractor	Refers to all persons or companies employed by The Company to carry out works on The Company's behalf.

Policy Statement

To detail information in respect of Data Protection for all information stored & used by The Company in its communications & processing of information, whether by digital or paper means.

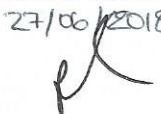
To ensure compliance with the law & follow good practice

To protect The Client, The Employee, the Subcontractor, The Company & any other persons with whom the business may have contact with.

To respect the rights of the individuals in respect of the data held about them. To be open & honest with the individuals about the data we store that relates to them.

To provide training & support for staff who handle personal data.

To notify the Commissioner, voluntarily, in line with reporting procedures.

Policy Operational Date	24/05/2018
Policy Prepared By	Cherie Roberts – Office Manager
Date Approved	27/06/2018
Signed Approval	

Approved by	Paul Hucker – Director
Policy Review Date	24/05/2021

1A Stoke Gardens,
Slough, Berkshire,
SL1 3QB
TEL: 01753 528173

www.balcomm.co.uk
info@balcomm.co.uk
Co. Reg. 3693572
VAT Reg 674 0079 34



Contents

1. Introduction
 - a) Purpose of the Policy
 - b) Types of Data
 - c) Policy Statement
 - d) Key Risks
2. Responsibilities
 - a) The Company Directors
 - b) Data Protection Officer
 - c) Specific Department Heads
 - d) Employees, Volunteers & Subcontractors
 - e) Enforcement
3. Security
 - a) Scope
 - b) Setting Security Levels
 - c) Security Measures
 - d) Business Continuity
 - e) Specific Risks
4. Data Recording & Storage
 - a) Accuracy
 - b) Updating
 - c) Storage
 - d) Retention Periods
 - e) Archiving
5. Right of Access
 - a) Responsibility
 - b) Procedure for making a request
 - c) Provision for verifying identity
 - d) Charging
 - e) Procedure for granting access
6. Transparency
 - a) Commitment
 - b) Procedure
 - c) Responsibility
7. Lawful Basis
 - a) Underlying principles
 - b) Opting Out
 - c) Withdrawing Consent
8. Employee Training & Acceptance of Responsibilities
 - a) Induction
 - b) Continuing Training
 - c) Procedure for Staff Signifying acceptance of policy
9. Policy Review
 - a) Responsibility
 - b) Procedure
 - c) Timing

1. INTRODUCTION

A) Purpose of Policy

The purpose of this policy is to comply with the law, follow good practice, protect clients, employees, subcontractors & other individuals & to protect the company

B) Types of Data

The company stores personal & sensitive data.

We may collect the following data from suppliers & clients: -

Name, Job Title, Contact Information, such as telephone numbers, email addresses & office addresses.

We collect the following data from employees, subcontractors and other persons we employ to carry out works, as well as job applicants and former employees. This information includes: -

Name, Contact Details, Gender, Proof of Identity, Proof of Qualifications, Bank Details, Nationality, Criminal Record Checks, References, Health Questionnaire, Next of Kin.

C) Policy Statement

The Company gather & use certain information about individuals in order to provide services, employment and contractual obligations.

This policy describes how the company protects & makes use of the information provided.

The policy is updated from time to time & is able to be viewed on the company website, or by sending an email to info@balcomm.co.uk where a copy will be emailed back to you.

If you have any questions about anything contained within this policy you can: -

Email: info@balcomm.co.uk

Write: Director
Balcomm Ltd
1A Stoke Gardens
Slough
Berks
SL1 3QB

D) Key Risks

The main risks are data getting into the wrong hands through poor security or inappropriate disclosure of information & Individuals being harmed through data being inaccurate or insufficient.

2. RESPONSIBILITIES

A) The Company Directors

Have overall responsibility for ensuring that the company complies with its legal obligations.

B) Data Protection Officer

Is responsible for: -

- Briefing the directors on data protection responsibilities
- Reviewing the data protection & related policies
- Advising staff on tricky data protection issues
- Ensuring that data protection induction & training takes place
- Notification to the ICO
- Handling subject access requests
- Approval of unusual or controversial disclosures of personal data
- Approving contracts with data processors

C) Specific department heads

Director
IT Manager
Office Manager
Contracts Managers

The person nominated as the Data Protection Officer is responsible for monitoring data processing & compliance, & reporting to the Information Commissioners Office in respect of any breaches.

D) Workers (Employees, Volunteers & Subcontractors, etc)

Must read, understand, & accept any policies & procedures that relate to the personal data they may handle during the course of their employment. They must further agree not to store this information after termination of their employment. Should any persons, no longer employed by the company, use information gained whilst employed, then the company reserves the right to bring a prosecution to those responsible.

E) Enforcement

Failure by any person to follow procedures or policies whilst working for the company will be subject to the disciplinary procedure as per the disciplinary policy document.

Any data breach, unauthorised sharing of data, or misuse of data may constitute a criminal offence. The company will comply & work with law enforcement where required.

3. SECURITY

A) Scope

Data security is not wholly a data protection issue. The company will make every effort to ensure that all data held is not compromised or accessed by unauthorised persons.

We will never lease, distribute, or sell your personal information to any third parties unless we have your express permission, or the law requires us to.

It may be necessary to share certain types of data amongst those employed by the company. This data would be limited to only that required to carry out the course of their works.

We also share contract information with other service providers for the purposes of fulfilling a contract of works, for example, we will share a site address and site contact details with the local water authority when seeking to obtain a discharge licence, a hire company when hiring equipment, etc. A full list can be provided on request at the commencement of a contract where an analysis of need has been carried out by the contract manager.

The client's instruction to commence works will be taken as legitimate consent to share this data to enable contract completion.

We share employee personal data only where it is required to fulfil our statutory obligations, such as paying salaries, tax, national insurance, health & safety in the workplace, which may also involve sharing information with third parties such as, but not limited to, insurers, professional advisors, recruitment agencies, HMRC, DWP, pension and life assurance companies, and other relevant parties.

B) Setting Security Levels

The company will continually monitor & adjust security levels to ensure full compliance with the law. As digital data security is constantly evolving the latest & most effective measures will be used as appropriate. This will be monitored by the IT manager & implemented as required. This includes the update of anti-viral, anti-spam, anti-phishing real time protection programs.

C) Security Measures

As a minimum password protection will be installed on all electronic devices used to store data.

A lock will be fitted on all cabinets used to store paper data.

Training will be provided to staff in respect of how to handle data requests received by telephone. All data requests should be made in writing & no data requests via telephone will be accepted.

D) Website

Our website may contain links to other relevant websites, which are out side of the control of the company. If you provide information to these websites we are not responsible for its protection & privacy. You should make your own checks prior to submitting any data.

E) Business Continuity

The company makes use of a cloud storage facility to create a back up of its server system. This cloud facility is password protected as per the security measures.

The company further backs up all payroll & accounts information to a data key. The information is stored as encrypted data & requires a two-part password login to decrypt the data.

F) Specific Risks

Working At Home

Working at Client Offices/Site Offices

Phishing & Vishing emails

Telephone Trickery

4. DATA RECORDING & STORAGE

A) Accuracy

The company primarily gather data from emails sent by clients (name, job title, telephone number, email address & company address).

The company primarily gathers employee sensitive data during the job offer process, whereby an employee completes all relevant forms.

You have the right to ask us to delete or amend any inaccurate data we hold about you.

B) Updating

The company checks all recorded data, at least yearly, to ensure its accuracy.

If the data is found to be outdated it is destroyed. In the case of electronic data this is by shredding software as implemented by the IT manager. In the case of hard copy data, a 'cross' cut security shredding device will be used.

C) Storage

In the most part, the data the company holds is stored electronically on the server.

In some cases, data is stored on hardcopy (paper) in locked filing cabinets.

D) How the Data is Used

Data we collect from clients is used for internal information only under legitimate interests. It is used to make contact with the person in order to conduct the business agreement, for example: To contact in response to a specific enquiry.

Data we collect from workers is used to fulfil our statutory obligations, such as the payment of salaries, tax, national insurance, health & safety in the work place.

E) Retention Periods

Information we hold will be retained for a period of no longer than 7 years after final correspondence with you, except in order to meet legal, tax or accounting requirements.

Information provided during a job application process will be retained by the company as part of the employee files for the duration of employment, plus 7 years following the end of employment. This includes criminal records declaration, fitness to work, accidents at work, records of any security vetting applications, references, and eligibility to work in the UK.

If any job applicant is unsuccessful at any stage of the process, the information provided will be destroyed and deleted from the company's system after 6 months. We do not collect more data than is necessary to fulfil our stated purpose and we will not retain it for longer than is necessary.

F) Archiving

After 1 year data is moved from active files to archive files.

After 7 years data is destroyed. In the case of electronic data this is by shredding software as implemented by the IT manager. In the case of hard copy data, a 'cross cut' security shredding device will be used.

5. RIGHT OF ACCESS

A) Responsibility

The company office staff will have access to client data held, name, job title, address, phone number, email address.

The Director, Office Manager & Accounts Administrator will have access to all client information & employee information.

B) Procedure for Making Request

Should any person, or company, wish to make a request to view data held about them by the company they should send a written request to

The Director
Balcomm Ltd
1A Stoke Gardens
Slough
Berks
SL1 3QB

Where a director, or if appointed by the director, the office manager, will prepare a full response detailing all information held by the company.

The response will be posted back to the person making the enquiry.

C) Procedure for Verifying Identity

If the company feel that it is necessary, it reserves the right to take further legal advice to prove the identity of the person requesting the information.

Requests that specifically ask for all the details of an individual, including that considered of a sensitive nature, will be subject to independent checking of identity prior to the information being released.

D) Charging

All Information will be provided free of charge.

The company reserves the right to charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if repetitive & may make a charge if it's a request for the same data previously supplied.

The companies fee will be based on the cost of the administration only & will be sent via invoice to the requesting party. Settlement of the invoice will need to be made in full prior to the release of the data.

E) Procedure for Granting Access

The data provided will be in electronic format where ever possible & will be provided in a commonly used format.

We may send the data on CD or on Data stick. In both instances the data will be password protected & a separate letter with the password details will be sent.

6. TRANSPARENCY

A) Commitment

The company are committed to ensuring the safe storage of all data held & to prevent, where reasonably practicable to do so, the misuse of such data.

B) Procedure

In order to ensure all persons are informed of the company's policy on data protection a copy of this document will be provided to any persons whom request it. It will also be published on the company's website.

All new employees will be given a copy of the policy prior to joining, & all staff who have access to the data stored will be trained.

C) Responsibility

Every employee of the company has the responsibility to ensure that any data used in performing their roles is done so responsibly & without detriment to the individual they are contacting or to the company.

Where an employee is unsure of any aspect of the processing, use, or viewing of any personal data stored they should not access this data & should contact the Director or the office manager for clarification about how they can use such data.

7. LAWFUL BASIS

A) Underlying Principles

The company stores client information for legitimate reasons. These are for maintaining communication with the client for the purposes of the contract works being carried out as requested by them.

The company stores employee information for legal reasons, in respect of payroll processing for example.

The company stores client head office addresses for the legitimate purposes, this being the once yearly marketing that is carried out, this takes the form of a company branded calendar being sent to the client.

B) Opting Out

The company relies on implied consent from the initial contact of the person contacting us. This implied consent refers only to the retention of Name, Job Title, Email Address, Phone Number & the address of the company they work for.

C) Objection

You have the right to object to the processing of your data. We will consider and evaluate all such requests received. Requests should be made in writing.

D) Withdrawing Consent

The company acknowledge that once given, consent can be withdrawn at any time. It should be noted that the withdrawal cannot be applied retrospectively.

Some data cannot be withdrawn or deleted, due to legal requirements to retain the information, for example, payroll records must be kept for not less than 3 years, the company retains the data for 7 years.

Should any person who wishes to opt out/withdraw consent of any data being stored, they should contact: -

The Director
Balcomm Ltd
1A Stoke Gardens
Slough
Berks
SL1 3QB

Where all data pertaining to that person will be removed from the company's internal storage.

8. EMPLOYEE TRAINING & ACCEPTANCE OF RESPONSIBILITIES

A) Induction

The policy will be issued to all new employees who will be required to read & understand its contents.

Where required & identified by the company, training will be provided to those who handle sensitive data.

B) Continuing Training

Ongoing training will be provided where required to employees who are responsible for handling the storage of sensitive data. This will include any legislation updates.

C) Procedure for Staff Signifying Acceptance of Policy

It is intended that all employees of the company will be issued with the data protection policy, alongside the specific policy in relation to employment. The issued policy will have a signed acceptance or rejection slip & the employee will be required to return this slip to the company.

The company will also commit to publishing the policy on their website, with exception of the specific employee section, which is available to all current, previous, and potential employed staff members only.

9. POLICY REVIEW

A) Responsibility

The director of the company has overall responsibility to ensure that the review is carried out.

B) Procedure

Department heads should be consulted during the process.

Information should be obtained from the ICO to ensure all current best practices are adhered to.

C) Timing

This document should be reviewed, at minimum, every 3 years.

It is advised that the information gathering process, consultation with department heads, & checking with official bodies should commence not less than 3 months before the review date.

This will allow sufficient time for each department head to review & comment as necessary.