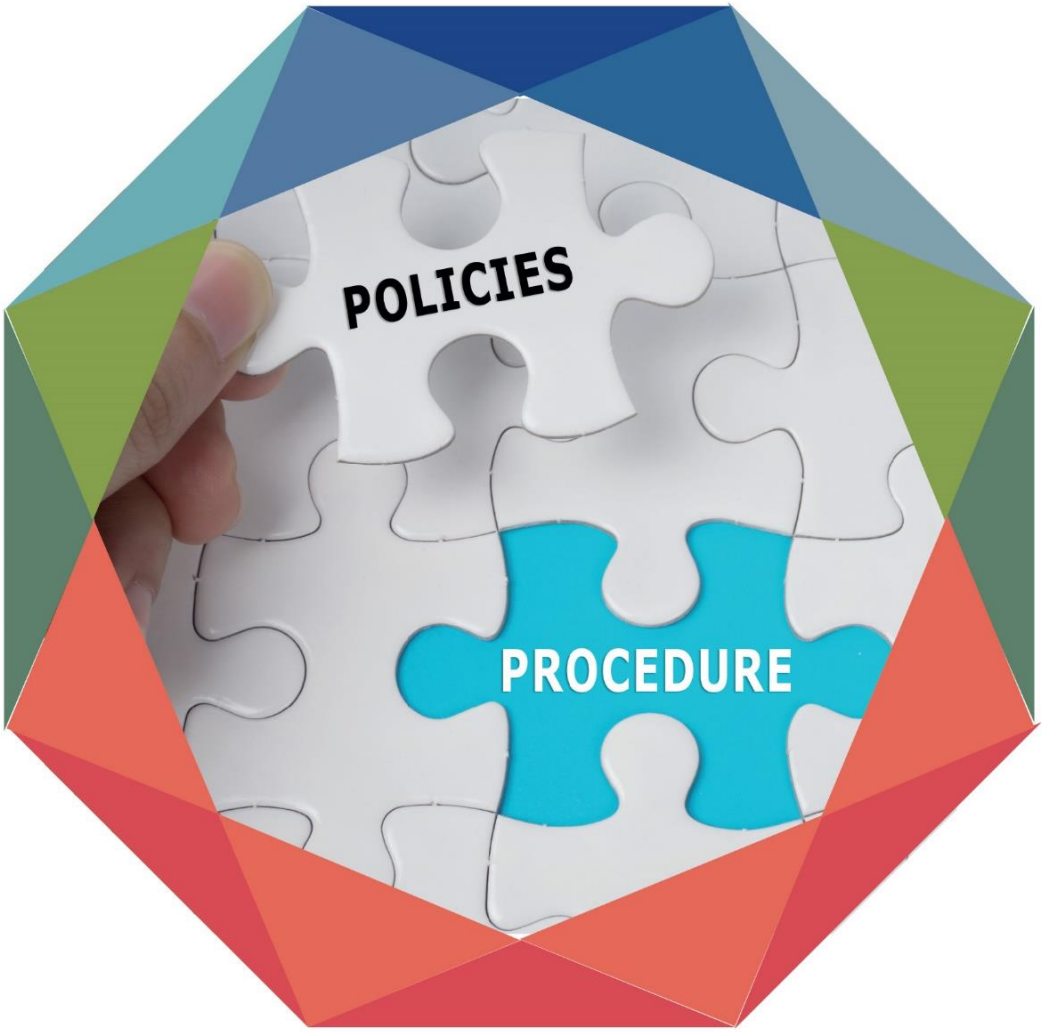
BUSINESS POLICIES

2024



Birdsall

Est. 1975

Business Policies Index

Approval

All seven of these business policies contained in this document have been reviewed and approved by the organisation's board of directors.

Paul Birdsall
Managing Director
Birdsall Services Ltd

Date: 2nd January 2024

1. Quality Policy

Policy Statement

Birdsall take the quality of their service and operations very seriously. We invest in and operate the Company to consistent high standards through our ISO9001 Quality Policy Procedures.

In summary of our ISO9001 procedures, it is the policy of Birdsall Services Limited to operate to the following:

- To fulfil both customer expectations, contractual obligations and any other applicable requirements through the provision of service and support appropriate to specification.
- To establish effective working relationships with key suppliers and sub-contractors.
- To ensure continuity of supply of services and products fit for purpose and which meet statutory and legislative requirements appropriate to the industry.
- To maintain a policy of cost-effective and consistent quality services and products and to be responsive to technological and performance standards appropriate to the industry.

We are committed to continually improve our management system and in order to do so our aims and objectives include:

- To operate a Quality Management system in accordance with the requirements of ISO 9001, recognising the contribution that all personnel make to quality and to provide the necessary information, resources and training to enable them to achieve and maintain the required standards.
- To establish and maintain a set of management system objectives which are directly aligned with our Business strategy, which are reviewed on a periodic basis.
- To maintain a policy of integrated management, encompassing quality, health & safety and environment based on clear definition of procedures assigned to key personnel with clearly defined roles and responsibilities.
- To ensure that the Company's policies are understood, implemented and maintained, the Directors and staff are advised of their responsibilities for the implementation of our Quality Policy by training. All of Birdsall Policies are incorporated into four documents, available to all employees and customers via our website.

2. Ethical Code of Practice Policy

As a responsible employer, Birdsall Services Ltd maintain ethical policies appropriate to the business activities of the Company.

Birdsall operate under financial controls appropriate to Limited Company status, including the preparation and submission of annual accounts that are subject to independent audit.

The company comply with all associated financial commitments including P.A.Y.E. and VAT and maintain appropriate levels of both Employers' Liability and Public Liability compulsory insurance.

To establish and maintain acceptable working practices, the Company are members of a number of Professional and Trade Associations including ECA, REFCOM, F Gas, GasSafe and Safe Contractor.

The Company complies with both Central and Local Government Regulations as applicable to our business activities which currently include:

- Employment Rights Act 1996
- Employment Protection (Consolidation) Act
- Equality Act 2010
- Working Time Regulations
- The Health & Safety at Work Act
- EU Regulation 2016/679 General Data Protection Regulation ("GDPR").
- Trades Description Act

Birdsall Services actively encourages ethical business management practices including:

- Appropriate use of business resources
- Supply chain management
- Awareness and resolution of conflicts of interest
- Environment Policy
- Guidelines on the acceptance of gifts & hospitality
- Establishment & maintenance of procedures to ensure acceptable staff conduct
- The establishment and maintenance of procedures to prevent harassment
- Establishment & maintenance of procedures to accommodate employees with special needs
- The establishment and maintenance of procedures to enable customers, staff and interested Third Parties to report unethical conduct.

3. Anticorruption & Bribery Policy

1. Policy Statement

1.1 It is the Company's policy to conduct all our business in an honest and ethical manner. We take a zero-tolerance approach to bribery and corruption and are committed to acting professionally, fairly and with integrity in all our business dealings and relationships wherever we operate. We enforce effective systems to counter bribery.

The purpose of this policy is to:

(a) set out our responsibilities, and of those working for us, in observing and upholding our position on bribery and corruption; and

(b) provide information and guidance to those working for us on how to recognise and deal with bribery and corruption issues.

1.2 Bribery and corruption are punishable for individuals by up to ten years' imprisonment and if we are found to have taken part in corruption, we could face an unlimited fine, be excluded from tendering for public contracts and face damage to our reputation. We therefore take our legal responsibilities very seriously.

1.3 In this policy, third party means any individual or organisation you come into contact with during the course of your work for us, and includes actual and potential clients, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies, including their advisors, representatives and officials, politicians and political parties.

2. Who is Covered by the Policy?

This policy applies to all individuals working at all levels and grades, including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, agents, or any other person associated with us (collectively referred to as workers in this policy).

3. What is Bribery?

A bribe is an inducement or reward offered, promised or provided to gain any commercial, contractual, regulatory or personal advantage.

Examples:

Offering a bribe

You offer a potential client monetary reward, but only if they agree to do business with us.

This would be an offence as you are making the offer to gain a commercial and contractual advantage. We may also be found to have committed an offence because the offer has been made to obtain business for us. It may also be an offence for the potential client to accept your offer.

Receiving a bribe

A supplier gives your nephew a job but makes it clear that in return they expect you to use your influence in our organisation to ensure we continue to do business with them.

It is an offence for a supplier to make such an offer. It would be an offence for you to accept the offer as you would be doing so to gain a personal advantage.

4. Gifts and Hospitality

4.1 This policy does not prohibit normal and appropriate hospitality (given and received) to or from third parties.

4.2 The giving or receipt of gifts is not prohibited, if the following requirements are met:

(a) it is not made with the intention of influencing a third party to obtain or retain business or a business advantage, or to reward the provision or retention of business or a business advantage, or in explicit or implicit exchange for favours or benefits.

(b) it complies with local law.

(c) it is given in our name, not in your name.

(d) it does not include cash or a cash equivalent (such as gift certificates or vouchers)

(e) it is appropriate in the circumstances. For example, in the UK it is customary for small gifts to be given at Christmas time.

(f) considering the reason for the gift, it is of an appropriate type and value and given at an appropriate time.

(g) it is given openly, not secretly.

(h) gifts should not be offered to, or accepted from, government officials or representatives, or politicians or political parties, without the prior approval of the compliance manager.

4.3 The test to be applied is whether in all the circumstances the gift or hospitality is reasonable and justifiable. The intention behind the gift should always be considered.

5. What is Not Acceptable?

It is not acceptable for you (or someone on your behalf) to:

(a) give, promise to give, or offer, a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given.

(b) give, promise to give, or offer, a payment, gift or hospitality to a government official, agent or representative to "facilitate" or expedite a routine procedure.

(c) accept payment from a third party that you know, or suspect is offered with the expectation that it will obtain a business advantage for them.

(d) accept a gift or hospitality from a third party if you know or suspect that it is offered or provided with an expectation that a business advantage will be provided by us in return.

(e) threaten or retaliate against another worker who has refused to commit a bribery offence or who has raised concerns under this policy; or

(f) engage in any activity that might lead to a breach of this policy.

6. Donations

We do not make contributions to political parties. We only make charitable donations that are legal and ethical under local laws and practices. No donation must be offered or made without the prior approval of the Managing Director.

7. Your Responsibilities

7.1 You must ensure that you read understand and comply with this policy.

7.2 The prevention, detection and reporting of bribery and other forms of corruption are the responsibility of all those working for us or under our control. All workers are required to avoid any activity that might lead to, or suggest, a breach of this policy.

7.3 You must notify your manager as soon as possible if you believe or suspect that a conflict with this policy has occurred or may occur in the future. For example, if a client or potential client offers you something to gain a business advantage with us or indicates to you that a gift or payment is required to secure their business.

7.4 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for gross misconduct. (We reserve our right to terminate our contractual relationship with other workers if they breach this policy).

8. Record-Keeping

8.1 We must keep financial records and have appropriate internal controls in place which will evidence the business reason for making payments to third parties.

8.2 You must declare and keep a written record of all hospitality or gifts accepted or offered, which will be subject to managerial review.

8.3 You must ensure all expenses claims relating to hospitality, gifts or expenses incurred to third parties are submitted in accordance with our expenses policy and specifically record the reason for the expenditure.

8.4 All accounts, invoices, memoranda and other documents and records relating to dealings with third parties, such as clients, suppliers and business contacts, should be prepared and maintained with strict accuracy and completeness. No accounts must be kept "off-book" to facilitate or conceal improper payments.

9. How to Raise a Concern

You are encouraged to raise concerns about any issue or suspicion of malpractice at the earliest possible stage. If you are unsure whether a particular act constitutes bribery or corruption or if you have any other queries, these should be raised with your line manager. Concerns should be reported by following the procedure set out in our Whistleblowing Policy. A copy of our Whistleblowing Policy can be found in your Company Handbook.

10. What to Do If You Are a Victim of Bribery or Corruption

It is important that you tell your manager as soon as possible if you are offered a bribe by a third party, are asked to make one, suspect that this may happen in the future, or believe that you are a victim of another form of unlawful activity.

11. Protection

11.1 Workers who refuse to accept or offer a bribe, or those who raise concerns or report another's wrongdoing, are sometimes worried about possible repercussions. We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken.

11.2 We are committed to ensuring no one suffers any detrimental treatment because of refusing to take part in bribery or corruption, or because of reporting in good faith their suspicion that an actual or potential bribery or other corruption offence has taken place or may take place in the future. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment

connected with raising a concern. If you believe that you have suffered any such treatment, you should inform HR immediately. If the matter is not remedied, and you are an employee, you should raise it formally using our Grievance Procedure, which can be found in the Company Handbook.

12. Training and Communication

12.1 Training on this policy forms part of the induction process for all new workers. All existing workers will receive regular, relevant training on how to implement and adhere to this policy.

12.2 Our zero-tolerance approach to bribery and corruption must be communicated to all suppliers, contractors and business partners at the outset of our business relationship with them and as appropriate thereafter.

13. Who Is Responsible for the Policy?

13.1 The (board of directors) has overall responsibility for ensuring this policy complies with our legal and ethical obligations, and that all those under our control comply with it.

13.2 HR has primary and day-to-day responsibility for implementing this policy, and for monitoring its use and effectiveness and dealing with any queries on its interpretation. Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this policy and are given adequate and regular training on it.

14. Monitoring and Review

14.1 HR will monitor the effectiveness and review the implementation of this policy, regularly considering its suitability, adequacy and effectiveness. Any improvements identified will be made as soon as possible. Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in countering bribery and corruption.

14.2 All workers are responsible for the success of this policy and should ensure they use it to disclose any suspected danger or wrongdoing.

14.3 This policy does not form part of any employee's contract of employment and it may be amended at any time.

Potential risk scenarios: "red flags"

The following is a list of possible red flags that may arise during the course of you working for us and which may raise concerns under various anti-bribery and anti-corruption laws. The list is not intended to be exhaustive and is for illustrative purposes only.

If you encounter any of these red flags while working for us, you must report them promptly using the procedure set out in the whistleblowing policy:

(a) you become aware that a third party engages in, or has been accused of engaging in, improper business practices.

(b) you learn that a third party has a reputation for paying bribes, or requiring that bribes be paid to them, or has a reputation for having a "special relationship" with foreign government officials.

(c) a third party insists on receiving a commission or fee payment before committing to sign up to a contract with us or carrying out a government function or process for us.

(d) a third-party requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made.

(e) a third-party request that payment is made to a country or geographic location different from where the third party resides or conducts business.

(f) a third party requests an unexpected additional fee or commission to "facilitate" a service.

(g) a third party demands lavish entertainment or gifts before commencing or continuing contractual negotiations or provision of services.

(h) a third-party request that a payment is made to "overlook" potential legal violations.

(i) a third-party request that you provide employment or some other advantage to a friend or relative.

(j) you receive an invoice from a third party that appears to be non-standard or customised.

(k) a third party insists on the use of side letters or refuses to put terms agreed in writing.

(l) you notice that we have been invoiced for a commission or fee payment that appears large given the service stated to have been provided.

(m) a third party requests or requires the use of an agent, intermediary, consultant, distributor or supplier that is not typically used by or known to us.

(n) you are offered an unusually generous gift or offered lavish hospitality by a third party.

4. Corporate Social Responsibility Statement

It is the Birdsall policy to ensure that our business contribution is sustainable development.

At Birdsall, we consider our economic, social and environmental impact in the way we operate the Company, in order to maximize the benefits and minimize the downsides.

At Birdsall, we encourage our Research & Development activities to keep community and environmental improvement at the forefront of their thinking.

At Birdsall, we would encourage voluntary actions that the business can take over and above its compliance and legal obligations in the interests of the wider society.

Birdsall respect its employee, sub-contractor and supplier relationships. Our operational offices respect and involve within their local community.

5. Business Continuity Policy

1. Introduction

This Business Continuity Plan has been devised to enable Birdsall Services Limited to ensure, as far as reasonably practical, the continuity of the business through the identification and management of significant risks, and to continue with minimum disruption in the event of a "major" unplanned incident such as fire, flood, explosion, theft, power failure, I.T. or communications failure or other significant event.

2. Strategy

The company's strategy is to:

- Implement and maintain effective systems in respect to commercial, quality assurance, health & safety and environmental management
- Implement appropriate measures to reduce the likelihood of incidents occurring
- Reduce the potential effects of those incidents
- Provide continuity for critical activities during and following an incident
- Take into account all other activities not initially considered critical
- Take into account the company's resilience to potential threats

To ensure the provision of consistent levels of customer service Birdsall Services utilise an integrated database management system, with independent I.T. support to maintain information system reliability and security.

The company's Quality Management system is registered to BS EN ISO 9001:2015 and is subject to both internal and external audit to monitor compliance and facilitate continual improvement in the provision of equipment and services.

Standard Operating Procedures have been compiled and implemented companywide to ensure consistency in the organisation's procedures and controls.

It is the responsibility of the Managing Director in conjunction with the Financial Director to compile and maintain an Asset Register for both the Head Office and Regional Offices. The Asset Register will be used as a reference for the replacement of critical equipment, and the evaluation of loss in the event of a major incident.

It is the responsibility of the Managing Director to periodically carryout an exercise programme to evaluate the effectiveness the Business Continuity Plan and to ensure:

- The planned arrangements are effective in maintaining business continuity
- Data and systems are restored with minimal disruption to the business
- That all critical organisational activities are managed effectively
- Responsibilities of key personnel are clearly defined and understood
- Confidence of management and key personnel is enhanced by the effectiveness of the Business Continuity Plan
- Continual improvement of the plan based on exercise results and experience

It is the responsibility of the Managing Director to periodically review and update this plan, and a current copy of the plan will be accessible by all staff electronically.

3. Premises

3.1 Buildings

The company's Head Office is a two-storey leased office and storage unit in 13 Avebury Court, Mark Road, Hemel Hempstead. We also operate from an office located in Romford.

Potential threats to Head Office are considered to be:

- Fire
- Explosion
- Power failure
- Telecommunications failure
- Termination of lease

The current premises are occupied on a 5-year lease basis.

In the event that temporary/permanent relocation is required the following actions will be taken:

- Transfer Head Offices activities to the Second office
- Obtain short-term alternative premises in the Hemel Hempstead area
- Enable key personnel to work from home

3.2 Fire

The company has appointed and trained a Fire Safety Warden (Sean Kane) responsible for fire prevention and control at Head Office. Responsibility for the Romford Office is Lee Matthews.

With the exception of electrical safety, there are no significant fire risks in administration areas. Small quantities of potentially flammable substances, including pressurised gases, are stored externally in a secure compound at the rear of the premises.

Fire extinguishers of the correct type are strategically placed on both the ground and first floors, serviced and maintained under contract.

Emergency Escape routes are clearly signed, and periodic Emergency Evacuation drills are carried out to ensure the building can be evacuated safety by all personnel in the event of fire or other emergency.

Detailed procedures for fire prevention and control are confirmed in the Health & Safety Codes & Practices manual.

3.3 Explosion

In addition to external sources, potential explosion threats include mains gas supply and small quantities of pressurised gases.

Detailed procedures for electrical safety are confirmed in the Health & Safety Codes & Practices manual.

Essential computer data is backed up daily and can be readily restored following a significant power failure.

Actions confirmed in 3.1 would be taken in the unlikely event of long-term mains power disruption.

3.5 Building security

Head Office is located on a small industrial estate with a relatively low incidence of crime. Normal office hours are maintained, with little or no requirement for Out-of-hours or weekend working, except for engineers on call and cleaning staff.

The building is provided with an electronic security system, which includes PIR sensors, and is activated outside normal office hours. Nominated key holders and other designated personnel are

approved for access including use of security system codes. It is the responsibility of the last person to leave the building each day to activate the alarm system.

Responsibility for Regional Office security is that of the estate company.

In the event of a break in or vandalism:

- The security of data is assured (Refer to Section 4.0)
- Potential loss of portable, electrical equipment (including computers) would not pose a significant medium/long-term threat and can be readily replaced
- Consumable stocks held in the warehouse are of limited commercial value and can be readily replaced
- In the event of significant damage or vandalism resulting from a break in rendering Head Office unserviceable, arrangements confirmed in Section 3.1 would apply

4. Information security & telecommunications

- The Company's server is located in a security-controlled Telecommunications Room subject to restricted access. Much of the company's data has now been relocated to the cloud.
- Accounts data is backed up daily onto the one drive and onto the cloud server.
- SQL and the Exchange server are backed up daily on to the cloud server.
- Individual PC's and laptops are protected by individual user passwords.
- Remote access to the server is provided for directors, contract managers, offices, engineers
- In the event of system failure or need for ongoing support, Birdsall retain the services of an external IT support company.
- All key personnel, including Installation, Service and Maintenance Engineers are provided with mobile telephones which would be used in the event of a significant telecommunications failure.

5. Personnel

Job descriptions and Standard Operating Procedures have been compiled for all critical functions in Birdsall Services. Potential employees are subject to interview to ascertain the required level of competence and experience. References will be verified if considered appropriate.

It is the responsibility of the Director/Manager in conjunction with the HR to ensure that all personnel receive appropriate induction, technical, product, systems and health & safety training.

It is the responsibility of the Director/Manager in conjunction with the HR Manager to ensure that all engineers employed in a security environment are screened in accordance with Police and Local Authority requirements.

In addition to employed installations and service engineers, the company maintain an approved list of suppliers and contractors who can be utilised in the event of significant labour shortage.

It is company policy that materials, products and services will be sourced from suppliers and contractors on the approved suppliers list.

Refer to BS EN ISO 9001:2015 Quality Assurance Process Documents PD/025 – Supplier/Contractor Evaluation.

7. Compliance with statutory requirements

7.1 Administration and Finance

It is the responsibility of the financial director to ensure that Birdsall services limited comply with all statutory requirements in respect to the administration and financial control of the company.

7.2 Personnel and Human Resources

It is the responsibility of the Human Resources Manager to ensure that Birdsall Services Limited comply with all statutory requirements in respect to the recruitment, employment and dismissal of employees, including the establishment and maintenance of compliant procedures for:

- Grievance
- Disciplinary
- Equal opportunities
- Disability discrimination
- Hours of work
- Holiday entitlement
- Termination of employment
- Redundancy

It is the responsibility of the Manager in conjunction with the HR Manager to ensure that Installation and Service Engineers are technically qualified in regard to industry requirements for the tasks to which they are assigned.

7.3 Health and Safety

It is the responsibility of the Managing Director in conjunction with the OPERATIONS Director and Fire Safety Officer to ensure that the company comply with the Health and Safety at Work Act and associated Regulations and Codes of Practice applicable to Birdsall Services.

To ensure the effective management of health and safety, the company has implemented a fully documented Health and Safety Management system, which is subject to periodic review and audit (Refer to Safety Codes & Practices Manual).

7.3 Environment

Birdsall Services are in the process of implementing a documented Environmental Management system compliant with the requirements of ISO 14001.

It is the responsibility of the Manager to ensure that controlled waste (e.g. Refrigerant / Oil / Asbestos/Electrical equipment etc) is identified and handled as appropriate by licensed Trade Waste contractors, including completion of Controlled Waste Transfer Notes as required.

8. Action plan in the event of a significant incident

The following is a checklist of actions, some of which may not need to take place, depending on the nature of the incident. The order in which actions need to be taken, and those who take them, may be varied according to circumstances.

The overall co-ordinator will be the Managing Director, with any nominated Director deputising. If a recovery team is needed, the membership will be decided by the Directors. The aim of the Action Plan will be to recover 80% of capability within 5 days.

- The Managing Director to be informed of the nature of the incident immediately by whoever discovers the disruption to the business
- Information gathered about nature and extent of the incident
- HR Manager assisted by Administration staff to inform all staff
- Recovery team nominated
- Recovery Team assess damage/loss
- Recovery Team arrange recovery of remaining records and equipment
- Financial Director to advise insurance companies, bank and other interested Third Parties (Refer to contact details in Appendix)
- Managers and Engineers to notify customers if appropriate
- Recovery Team to confirm ongoing and future action plans
- Purchase, hire and borrow the necessary capital equipment required to establish an acceptable facility at alternative or new premises
- Ensure security of alternative/ new premises
- Enable phones, post and e-mail at alternative/new premises
- Managing Director – Updates Chairman, Directors, and Management Team as appropriate
- Contracts Managers and Design Engineers to update customers as appropriate

APPENDICES

Directors			
Name	**Position**	**Email**	**Mobile**
Barry Birdsall	Chairman	barry.birdsall@birdsall.co.uk	07973 845 046
Paul Birdsall	Managing Director	paul.birdsall@birdsall.co.uk	07813 133 447
Kathy Chambers	Financial Director	kathy.chambers@birdsall.co.uk	07957 436 873
Lynne Culliton	HR Director	lynne.culliton@birdsall.co.uk	07979 535 195
Mitchell Clarke	Operations Director	mitchell.clarke@birdsall.co.uk	07966 288042

Offices			
Location	**Contact**	**Telephone**	**Mobile**
Romford	Keeley Gibbs	020 3198 6477	07875 537 568
Hemel Hempstead	Lynne Culliton	01442 212 501	07811 100 713

Insurance Details			
Policy No.	**Insurance Cover**	**Contact**	**Tel. No.**
202500609	Employers Liability	Heath Crawford	020 8421 7030
202500609	Public/Products Liability	Heath Crawford	020 8421 7030
9432/22/E9	Professional Indemnity	Heath Crawford	020 8421 7030

Emergency Contacts			
Supplier	Scope of Supply	Account Number	Tel. No.
British Gas	Gas	600055588	0800 111 999
British Gas	Electricity	4803728943	0800 783 8838
Three Valleys Water	Water	2004335-1	0845 782 3333
Chubb Fire	Fire Extinguishers		0800 32 1666
ADT	Security system	741146	0870 600 600 5
MK IT	I.T. Support		01525 214944
Health & Safety Executive	Incident Contact Centre		0845 300 9923
Environment Agency			01707 632420
Heath Crawford	Insurance		01727 850707

6. Information Security Policy

It is the policy of Birdsall Services Limited:

- To effectively manage information security within the organization including determination of realistic objectives, targets, processes and controls.
- To provide the necessary resources to develop, implement, operate and maintain the Company's Information Security management system.
- To allocate responsibilities for the management of information security and ensure that only competent persons have access to and utilize information security systems.
- To ensure that procedures and controls comply with legislative and contractual requirements, and that computer systems and data essential for ensuring product quality and safety are maintained at all times.
- To ensure that specific requirements imposed by customers in respect to the protection of intellectual property rights and data provided to facilitate project management and continuity of supply are acknowledged and adhered to at all times.
- To ensure that where there is a contractual requirement for Third Parties to have access to the Company's computer systems and data, such access is subject to risk assessment to determine any security implications and control requirements.
- To establish and maintain effective security management controls in respect to system access, the introduction and use of approved software, password control and protection against computer viruses from whatever source.
- To establish and maintain documented processes in respect to information security systems.
- To monitor and review systems, procedures and controls and take corrective and preventive actions as appropriate to identified levels of risk.
- To maintain a policy of continual performance improvement in respect to both computer systems and data and the Company's Information Security management system.
- To ensure that the Company's policies are understood, implemented and maintained, and the Directors and staff are advised of their responsibilities for the management of information security by training, access to the Business Policy Manual, Process Documents and Standard Operating Procedures referenced within it.

7. Data Protection Policy (GDPR)

Introduction

This Policy sets out the obligations of Birdsall Services Ltd ("the Company") regarding data protection and the rights of customers, suppliers & business contacts ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

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 limited to what is necessary in relation to the purposes for which it is processed.

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

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research 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 the data subject.

Processed 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.

The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

The right to be informed (Part 12)

The right of access (Part 13)

The right to rectification (Part 14)

The right to erasure (also known as the 'right to be forgotten') (Part 15)

The right to restrict processing (Part 16)

The right to data portability (Part 17)

The right to object (Part 18) and

Rights with respect to automated decision-making and profiling (Parts 19 and 20).

Lawful, Fair, and Transparent Data Processing

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

The data subject has given consent to the processing of their personal data for one or more specific purposes

The processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering a contract with them

The processing is necessary for compliance with a legal obligation to which the data controller is subject

The processing is necessary to protect the vital interests of the data subject or of another natural person

The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

[If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so)

The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

The processing relates to personal data which is clearly made public by the data subject.

The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity.

The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;

The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Specified, Explicit, and Legitimate Purposes

The Company collects and processes the personal data set out in Part 21 of this Policy. This includes:

Personal data collected directly from data subjects

Personal data obtained from third parties.

The Company only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the GDPR).

Data subjects are kept informed always of the purpose or purposes for which the

Company uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

Adequate, Relevant, and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

Accuracy of Data and Keeping Data Up to Date

The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up to date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Data Retention

The Company shall not keep personal data for any longer than is necessary considering the purpose or purposes for which that personal data was originally collected, held, and processed.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

Accountability and Record-Keeping

The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors.

The purposes for which the Company collects, holds, and processes personal data.

Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates.

Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards

Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy); and

Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

Keeping Data Subjects Informed

The Company shall provide the information set out in Part 12.2 to every data subject:

Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

- if the personal data is used to communicate with the data subject, when the first communication is made; or
- if the personal data is to be transferred to another party, before that transfer is made; or
- as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

The following information shall be provided:

Details of the Company including, but not limited to, the identity of its Data Protection Officer.

- The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing.

- Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data.
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed.
- Where the personal data is to be transferred to one or more third parties, details of those parties.
- Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);
- Details of data retention.
- Details of the data subject's rights under the GDPR.
- Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time.
- Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR).
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

Data Subject Access

Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection Officer at our Head Office.

Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

All SARs received shall be handled by the Company's Data Protection Officer.

The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data

Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any affected personal data has been disclosed to third parties, those parties shall be

informed of any rectification that must be made to that personal data.

Erasure of Personal Data

Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed
- The data subject wishes to withdraw their consent to the Company holding and processing their personal data.
- The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);
- The personal data has been processed unlawfully
- The personal data needs to be erased for the Company to comply with a legal obligation.
- Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
- In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

Restriction of Personal Data Processing

Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

If any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Data Portability

Where data subjects have given their consent to the Company to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following format, Excel spreadsheet.

Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

Objections to Personal Data Processing

Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy):

Data Ref.	Type of Data	Purpose of Data
Mkt data	Name, tel, email, work address, website	Marketing of Birdsall services

Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

All emails containing personal data must be marked "confidential".

Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.

Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.

Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.

Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.

Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient.

All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

Data Security - Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

All electronic copies of personal data should be stored securely using passwords.

All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar.

All personal data stored electronically should be backed up with backups stored onsite AND/OR offsite.

No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy.

Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from John Halls.

No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the appropriate authorisation.

Personal data must always be handled with care and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time.

If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of John Halls to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.

Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

All software (including, but not limited to, applications and operating systems) shall be kept up to date. The Company's IT staff shall be responsible for installing any and all security-related updates.

No software may be installed on any Company-owned computer or device without the prior approval

of the IT team.

Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy and shall be provided with a copy of this Policy.

Only employees, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company.

All employees, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.

All employees, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised.

All employees, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise.

Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.

All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy.

The performance of those employees, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.

All employees, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract.

All contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR.

Where any contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Data Breach Notification

All personal data breaches must be reported immediately to a Director of the Company.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), a Director must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, a Director must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

The categories and approximate number of data subjects concerned

The categories and approximate number of personal data records concerned

The name and contact details of the Company's contact point where more information can be obtained)

The likely consequences of the breach

Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Implementation of Policy

This Policy shall be deemed effective as of 02/01/2024. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

8. Data Retention Policy

1. Introduction

This Policy sets out the obligations of Birdsall Services Ltd, a company registered in the UK under company number 1210655 whose registered office is at 13 Avebury Court, Mark Road, Hemel Hempstead, Hertfordshire HP2 7TA ("the Company") regarding retention of personal data collected, held, and processed by the Company in accordance with the Data Protection Legislation. "Data Protection Legislation" means all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation.

The Data Protection Legislation defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The Data Protection Legislation also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the Data Protection Legislation, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the Data Protection Legislation to protect that data).

In addition, the Data Protection Legislation includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above).

When the data subject withdraws their consent.

When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest.

When the personal data is processed unlawfully (i.e. in breach of the Data Protection Legislation).

When the personal data has to be erased to comply with a legal obligation; or

Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Company for business purposes, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the Data Protection Legislation, please refer to the Company's Data Protection Policy.

2. Aims and Objectives

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the Data Protection Legislation.

2.2 In addition to safeguarding the rights of data subjects under the Data Protection Legislation, by ensuring that excessive amounts of data are not retained by the Company, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

3.1 This Policy applies to all personal data held the Company and by third-party data processors processing personal data on the Company's behalf.

3.2 Personal data, as held by the Company is stored in the following ways and in the following locations:

a) In the cloud via Sharepoint.

b) In Iomart hosting our Eagle CAFM.

c) Physical records stored in our Hemel Hempstead office.

4. Data Subject Rights and Data Integrity

All personal data held by the Company is held in accordance with the requirements of the Data Protection Legislation and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

4.1 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Company's use of their personal data, and further rights relating to automated decision-making and profiling.

5. Technical and Organisational Data Security Measures

5.1 The following technical measures are in place within the Company to protect the security of personal data.

a) All emails containing personal data must be marked "confidential".

b) Personal data may only be transmitted over secure networks.

c) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient.

d) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from a Director.

e) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely.

f) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation.

g) Personal data must be handled with care at all times and should not be left unattended or on view.

h) Computers used to view personal data must always be locked before being left unattended.

i) No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise [without the formal written approval of <<insert position>> and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.

j) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company's Data Protection Policy and the Data Protection Legislation.

k) All personal data stored electronically should be backed up daily with backups to the cloud.

l) All electronic copies of personal data should be stored securely using passwords.

m) All passwords used to protect personal data should be multi factor authenticated (MFA) and should be secure.

n) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

o) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after.

p) No software may be installed on any Company-owned computer or device without approval.

5.2 Security of personal data

The following organisational measures are in place within the Company to protect the security of personal data. Please refer to the Company's Data Protection Policy for further details:

a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Data Protection Legislation and under the Company's Data Protection Policy.

b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company.

c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so.

d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised.

e) All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times.

f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.

g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.

h) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the Data Protection Legislation and the Company's Data Protection Policy.

i) All contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the Data Protection Legislation and the Company's Data Protection Policy.

6. Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

6.1 Personal data stored electronically (including any and all backups thereof) shall be deleted.

6.2 Special category personal data stored electronically (including any and all backups thereof) shall be deleted.

6.3 Personal data stored in hardcopy form shall be shredded.

6.4 Special category personal data stored in hardcopy form shall be shredded.

7. Data Retention

7.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account.

a) The objectives and requirements of the Company.

b) The type of personal data in question.

c) The purpose(s) for which the data in question is collected, held, and processed.

d) The Company's legal basis for collecting, holding, and processing that data.

e) The category or categories of data subject to whom the data relates.

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

8. Roles and Responsibilities

8.1 The Company's Directors are responsible.

8.2 The Directors are responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the Data Protection Legislation.

8.3 The Directors shall be directly responsible for ensuring compliance with the above data retention periods throughout the Company.

8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of Data Protection Legislation compliance should be referred to the Directors.

9. Implementation of Policy

This Policy shall be deemed effective as of 02/01/2024. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Head Office:
13 Avebury Court
Mark Road
Hemel Hempstead
Hertfordshire
HP2 7TA
Tel: 01442 212501

Romford Office:
Unit B3 Seedbed Centre
Davidson Way
Romford
Essex
RM7 0AZ
Tel: 020 3198 6477