



# **Umbrella Employee, Worker and Freelance Contractor Data Protection and Privacy Notice**

**Danbro**  
Umbrella

## Contents

1.0	What is the Purpose of this Document? .....	3
2.0	Data Protection Principles .....	3
3.0	The Kind of Information we Hold About you.....	3
4.0	How Is Your Personal Information Collected? .....	4
5.0	Sending Us Personal Information and Documents.....	5
6.0	How We Will Use Information About You.....	5
7.0	How we use Particularly Sensitive Personal Information.....	7
8.0	Information About Criminal Convictions.....	8
9.0	Automated Decision-Making.....	9
10.0	Data Sharing.....	10
11.0	Data Security.....	12
12.0	Data Retention.....	13
13.0	Rights of Access, Correction, erasure, and Restriction .....	13
14.0	Rights to Withdraw Consent.....	14
15.0	Data Protection Officer.....	14
16.0	Changes to this Privacy Notice .....	14

## 1.0 What is the Purpose of this Document?

### Key Points:

Danbro is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the UK General Data Protection Regulation.

It applies to all employees, workers and freelance contractors, and in part to interns and volunteers.

### In More Detail:

Danbro Workforce Solutions Limited (10567033) and Danbro Employment Umbrella Limited (10585274) who are registered in England and Wales, with their registered office at Jubilee House, East Beach, Lytham FY8 5FT are the “data controllers.”

This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and freelance contractors. It will also apply to interns and volunteers, to the extent that data of the types described in this notice is actually processed by Danbro in relation to such individuals.

This notice does not form part of any contract of employment or other contract between us. We may update this notice at any time, but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practicable.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

## 2.0 Data Protection Principles

We will comply with data protection law. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes
- Relevant to the purposes we have told you about and limited only to those purposes
- Accurate and kept up to date
- Kept only as long as necessary for the purposes we have told you about
- Kept securely

## 3.0 The Kind of Information we Hold About you

### Key Points:

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are “special categories” of more sensitive personal data which require a higher level of protection, such as information about a person’s health or sexual orientation. Information about criminal convictions also warrants this higher level of protection.

---

## In More Detail:

We may collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- Date of birth
- Gender
- Marital status and dependents
- Next of kin and emergency contact information
- National Insurance number
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information
- Start date and, if different, the date of your continuous employment/engagement
- Leaving date and your reason for leaving
- Location of employment or workplace
- Copy of driving license
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process)
- Employment records (including job titles, work history, working hours, training records and professional memberships)
- Compensation history
- Performance information
- Disciplinary and grievance information
- CCTV footage and other information obtained through electronic means such as swipe card records
- Telephone calls, emails, or other communications with you
- Information about your use of our information and communications systems
- Photographs
- Passport, visa, “right to work” documents, and/or sponsorship papers
- Results of HMRC employment status check, details of your interest in and connection with any intermediary through which your services are supplied

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership.
- Information about your health, including any medical condition, health and sickness records, including:
  - where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision
  - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and
  - where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes
- Genetic information and biometric data
- Information about criminal convictions and offences

## 4.0 How Is Your Personal Information Collected?

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency/business or umbrella company, from online sources (such as LinkedIn), from CV databases, or from a background check provider. We may sometimes collect additional information from third parties including former

---

employers/engagers, referees, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies or other background check agencies.

We may also collect personal information from the trustees or managers of pension arrangements operated by a group company.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

## 5.0 Sending Us Personal Information and Documents

Please note that we cannot guarantee email to be a secure way to send personal information, such as copies of passport, driving license, or other personal documents.

For this reason, we provide a secure portal on our website, accessible only by username and password, where you can upload documents containing personal information.

If you nevertheless choose to send such documents by email, this will be your own choice, and at your own risk.

## 6.0 How We Will Use Information About You

### Key Points:

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract we have entered into with you, or to take steps to enter a contract with you or under which you will perform services
- Where we need to comply with a legal obligation
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests
- Where we are legally permitted to do so and we have your informed or (in certain circumstances) explicit consent

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests)
- Where it is needed in the public interest or for official purposes

### Situations in which we will use your Personal Information

We need all the categories of information in the list above (see [The Kind of Information we Hold About you](#)) primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases, we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment or engagement
- Seeking, placing you in, and managing your assignments
- Determining the terms on which you work for us
- Checking you are legally entitled to work in the UK
- Paying you and, if you are an employee or deemed employee for tax purposes, or if we are otherwise legally required to do so, deducting tax and National Insurance contributions ("NICs")
- Providing benefits to you, including (where applicable):

- Inviting you to participate in any share plans operated by a Group Company
- Granting awards under any share plans operated by a Group Company
- Administering your participation in any share plans operated by a Group Company, including communicating with you about your participation and collecting any tax and NICs due on any share awards
- Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties
- Liaising with the trustees or managers of a pension arrangement operated by a Group Company, your pension provider and any other provider of employee benefits
- Administering the contract we have entered into with you
- Business operation, management, and planning, including accounting and auditing
- Conducting performance reviews, managing performance and determining performance requirements
- Making decisions about salary reviews and compensation
- Assessing qualifications for a particular job or task, including decisions about promotions
- Gathering evidence for possible grievance or disciplinary hearings
- Making decisions about your continued employment or engagement
- Making arrangements for the termination of our working relationship
- Education, training and development requirements
- In order to check any instruction or information given to us
- To improve the quality of our service
- Dealing with legal disputes and insurance claims involving you, or other employees, workers and contractors, including accidents at work
- Ascertaining your fitness to work
- Managing sickness absence
- Complying with health and safety obligations
- To prevent fraud or other criminal activity
- To monitor your use of our information and communication systems to ensure compliance with our IT policies
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- To conduct data analytics studies to review and better understand employee retention and attrition rates
- To demonstrate our own compliance with legal obligations, to third parties who themselves have legitimate interests in satisfying themselves as to our compliance
- To manage and maintain any applicable insurance policies
- Equal opportunities monitoring
- Depending on the circumstances, we rely on one or more of the following lawful bases when processing your personal data:
  - Performance of a contract
  - Compliance with a legal obligation
  - Legitimate interests
  - Consent (where specifically obtained)
  - Substantial public interest (for special category data)
  - Establishment, exercise or defence of legal claims
- To comply with our obligations under tax, employment intermediaries, off-payroll working (IR35), National Minimum Wage, Agency Worker Regulations and other applicable legislation
- To conduct identity verification, right to work checks, anti-money laundering checks, fraud prevention checks and (where appropriate) credit reference checks

Where we rely on legitimate interests as the lawful basis for monitoring or network security activities, we have carried out a balancing assessment to ensure that our interests in protecting our business, clients, workers and

systems are not overridden by your rights and freedoms. Monitoring is conducted in a proportionate manner and in accordance with our IT policies

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

Depending on the circumstances, we will rely on one or more of the following lawful bases when processing your personal data:

- Performance of a contract
- Compliance with a legal obligation
- Legitimate interests
- Consent (where specifically obtained)
- Substantial public interest (for special category data)
- Establishment, exercise or defence of legal claims

### **If you fail to provide Personal Information**

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

### **Change of Purpose**

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

## **7.0 How we use Particularly Sensitive Personal Information**

### **Key Points:**

“Special categories” of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent
- Where we need to carry out our legal obligations and in line with our Data Protection policy
- Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme, and in line with our Data Protection policy
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else’s interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about employees, workers and contactors or former employees, workers and contactors in the course of legitimate business activities with the appropriate safeguards.

We maintain an Appropriate Policy Document as required under Schedule 1 of the Data Protection Act 2018, which sets out our procedures for securing compliance with the data protection principles when processing special category data. This ensures that all processing is lawful, necessary, and proportionate.

### **Our Obligations:**

We may be required to use your particularly sensitive personal information in the following ways:

- We may use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws
- We may use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits, including statutory maternity pay, statutory sick pay, pensions and permanent health insurance
- If you are employed and if you leave employment, and under any share plan operated by a Group Company the reason for leaving is determined to be ill-health, injury or disability, we will use information about your physical or mental health, or disability status in reaching a decision about your entitlements under the share plan
- If you apply for an ill-health pension under a pension arrangement operated by a Group Company, we will use information about your physical or mental health in reaching a decision about your entitlement
- We may use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting
- We may use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations

### **Do we need your Consent?**

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

## **8.0 Information About Criminal Convictions**

### **Key Points:**

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our Data Protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about employees, workers and contactors or former employees, workers and contactors in the course of legitimate business activities with the appropriate safeguards.

### **In More Detail:**

We envisage that we may hold information about criminal convictions.

We will only collect information about criminal convictions where it is appropriate given the nature of the role, assignment or services to be provided, and where we are legally permitted to do so. This may include where:

- A client requires a criminal record check (for example, a DBS check) as a condition of an assignment
- The role involves working with vulnerable individuals, in regulated environments, or in positions of financial trust
- We are required to do so to comply with a legal or regulatory obligation
- You voluntarily disclose such information to us

Where appropriate, we will collect information about criminal convictions as part of the onboarding or assignment approval process, or we may be notified of such information directly by you during the course of your engagement with us.

We will use information about criminal convictions and offences in the following ways:

- To assess your suitability for particular assignments or client engagements
- To comply with legal or regulatory requirements placed upon us or our clients
- To satisfy client due diligence requirements where legally permitted
- To protect our business, clients, and other workers from fraud, dishonesty, safeguarding risks or other unlawful activity
- To establish, exercise or defend legal claims

We are allowed to use your personal information in this way because:

- It is necessary for carrying out our obligations and exercising specific rights in the field of employment and social security law (Schedule 1, Part 1 of the Data Protection Act 2018)
- It is necessary for reasons of substantial public interest (including preventing or detecting unlawful acts, safeguarding individuals at risk, or preventing fraud)
- It is necessary for the establishment, exercise or defence of legal claims
- It is necessary to comply with a legal obligation to which we are subject

We have in place an appropriate policy document and safeguards as required under the Data Protection Act 2018 when processing criminal convictions data. Access to such information is strictly limited to those who have a legitimate need to know it for the purposes described above.

We will not retain information about criminal convictions for longer than is necessary and will process it in accordance with our Retention Policy.

## 9.0 Automated Decision-Making

### Key Points:

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

- Where appropriate safeguards are in place, including the right to obtain human intervention, to express your point of view, and to contest the decision
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights
- If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights

### **In More Detail:**

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

## **10.0 Data Sharing**

### **Key Points:**

We may have to share your data with third parties, including third-party service providers and other entities in the Group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK.

If we do, you can expect a similar degree of protection in respect of your personal information.

### **Why might you share my Personal Information with Third Parties?**

We may share your personal information with third parties:

- where required by law
- to seek, place you in, or manage your assignments
- where it is necessary to administer the working relationship with you
- to demonstrate our own compliance with legal obligations, to third parties who themselves have legitimate interests in satisfying themselves as to our compliance, including any agency or client through / for whom you may be working
- to manage and maintain any applicable insurance policies
- where we have your informed consent, or
- where we have another legitimate interest in doing so

### **Which Third Party Service Providers process my Personal Information?**

The following activities may be carried out by third party service providers:

- payroll
- payslip verification
- tax and other relevant compliance checking and confirmation services
- pension provision and related administration
- benefits provision and administration
- IT services

We will share personal data regarding your engagement with us and your remuneration with the following third-party service providers:

- for providing payroll services
  - our current payroll software service provider
  - any other third-party service provider we may from time to time use to provide such services
- for providing payslip verification, and tax compliance checking and confirmation services, any one or more of the following:
  - FCSA veriPAYE

- Saferec
  - Any other third-party service provider we may from time to time use to provide such services
- for providing tax and other relevant compliance checking and confirmation services, any one or more of the following:
  - FCSA
  - An Auditor appointed by another party in a supply chain via which workers engaged by us provides services, in circumstances where that appointing party has a legitimate interest in satisfying itself as to our compliance
  - Any other third party service provider we may from time to time use to provide such services
- for providing pension and related administration services
- for ensuring compliance with government and regulatory bodies, including:
  - HM Revenue & Customs (HMRC)
  - The Department for Work and Pensions (where required)
  - Regulators including the Information Commissioner's Office (ICO)
  - Law enforcement agencies where required

We may share personal data relating to your participation in any share plans operated by a Group Company with third party administrators, nominees, registrars and trustees for the purposes of administering the share plans.

### **How Secure is my Information?**

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies.

- We do not allow our third-party service providers to use your personal data for their own purposes
- We only permit them to process your personal data for specified purposes and in accordance with our instructions

### **When might you share my Personal Information with Other Entities in the Group?**

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data. We will share personal data relating to your participation in any share plans and pension arrangements operated by a Group Company with other entities in the Group for the purposes of administering the share plans.

### **What about Other Third Parties?**

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business.

- In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes
- Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction

We may also need to share your personal information with a regulator or to otherwise comply with the law. This may include:

- making returns to HMRC
- compliance with Gender Pay Gap reporting requirements
- disclosures to stock exchange regulators (including a Regulatory News Service) and
- disclosures to shareholders such as directors' remuneration reporting requirements.

## Transferring Information Outside the UK

### Key Points:

We do not routinely transfer your personal data outside the UK.

However, in limited circumstances, it may be necessary for us to transfer your personal data outside the UK, for example where:

- A client, end client, agency or service provider is based outside the UK
- We use IT systems, software providers, payroll platforms, cloud storage or professional advisers that host or access data from outside the UK
- You are engaged on an assignment outside the UK
- A Group Company, insurer, auditor or professional adviser is located overseas

Where this occurs, we will ensure appropriate safeguards are in place in accordance with UK Data Protection Law.

### In More Detail:

We do not as standard transfer your personal information outside the UK. However, if it becomes necessary to do so in connection with your engagement, assignment, payroll processing, provision of benefits, insurance arrangements, IT systems, or in order to perform our contract with you, we may transfer your personal information to countries outside the UK.

Some countries benefit from “adequacy regulations” issued by the UK Government, meaning they are considered to provide an adequate level of protection for personal data. Where we transfer personal data to a country covered by adequacy regulations, we will rely on that decision.

Where a country does not have adequacy regulations, we will ensure that appropriate safeguards are implemented to protect your personal data. These safeguards may include:

- The use of UK-approved International Data Transfer Agreements (IDTAs) or the UK Addendum to the EU Standard Contractual Clauses
- Binding corporate rules (where applicable)
- Contracts requiring the recipient to comply with UK data protection standards
- Transfers to organisations participating in recognised international data protection frameworks (where applicable)
- Additional technical and organisational security measures where required

In very limited circumstances, and where no other lawful transfer mechanism is available, we may rely on a specific derogation under UK data protection law, for example, where the transfer is necessary for the performance of a contract between us, for the establishment or defence of legal claims, or where you have provided your explicit consent to the proposed transfer after being informed of any potential risks.

If you would like further information about international transfers or the safeguards we have in place, you may request this from our Data Protection Officer.

## 11.0 Data Security

### Key Points:

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

### **In More Detail:**

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Data Protection Officer.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

## **12.0 Data Retention**

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our Data Retention Policy which is available from the Data Protection Officer.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. Where we may be considered to be an employment business, we are required by law to retain candidates' personal data for at least one year after we last provided services to them. For payroll and tax purposes, we are generally required to retain records for a minimum of 6 years following the end of the relevant tax year.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and in due course securely destroy your personal information in accordance with our Data Retention Policy or applicable laws and regulations.

## **13.0 Rights of Access, Correction, Erasure, and Restriction**

### **Your Duty to Inform us of Changes**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

### **Your Rights in Connection with Personal Information**

Under certain circumstances, by law you have the right to:

- **Request Access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it
- **Request Correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected
- **Request the Erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask

us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to Processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes
- **Request the Restriction** of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it
- **Request the Transfer** of your personal information to another party (data portability)
- **Complain to the ICO**, the UK supervisory authority for data protection issues, if you believe your data has been mishandled

Please note that some of these rights may be limited in the employment or worker context where exemptions apply under Data Protection Law.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Protection Officer on [data.officer@danbro.co.uk](mailto:data.officer@danbro.co.uk).

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

## 14.0 Rights to Withdraw Consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Officer on [data.officer@danbro.co.uk](mailto:data.officer@danbro.co.uk).

Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

## 15.0 Data Protection Officer

We have appointed a Data Protection Officer to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the Data Protection Officer on [data.officer@danbro.co.uk](mailto:data.officer@danbro.co.uk).

## 16.0 Changes to this Privacy Notice

This privacy notice is not contractual; we reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact the Data Protection Officer.