PRIVACY, DATA PROTECTION (GDPR) & IT SECURITY POLICY

FOR OFFICE USE ONLY	
Issue No:	3
Issue Date:	26/05/2026
Last Review:	26/05/2026
Classification:	Public

We take your privacy and your data protection and our IT security very seriously. Please read this policy carefully as it contains important information on who we are and how and why we collect, store, use and share your personal information. It also explains your rights in relation to your personal information and how to contact us, or supervisory authorities, in the event you have a complaint.

We collect, use and are responsible for certain personal information about you. When we do so we are subject to the General Data Protection Regulation (GDPR) which applies across the European Union (including in the United Kingdom) and we are responsible as 'Controller' of that personal information for the purposes of those laws.

Key Terms

It would be helpful to start by explaining some key terms used in this policy:-

We, us, our	Cuffe Plc
Our Data Protection Officer	The Financial Controller Telephone 0208 879 5919
Personal information	Any information relating to an identified or identifiable individual
Special category personal information	Personal information revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership; Genetic and biometric data; Data concerning health, sex life or sexual orientation.

Personal Information we collect about you

We may collect and use the following personal information about you:-

- your name and contact information, including email address and telephone number and company details;
- Information to enable us to check and verify your identity, e.g. your date of birth;
- your gender information, if you choose to give this to us;
- location data, if you choose to give this to us;
- your billing information and transaction information;
- your personal or professional interests;
- your professional online presence, e.g.LinkedIn profile;
- your contact history, purchase history and saved items;
- information from accounts you link to us, e.g. Facebook;
- information to enable us to undertake credit or other financial checks on you;
- Information about how you use our website, IT, communication and other systems;
- your responses to surveys, competitions and promotions.

This personal information is required to provide services to you. If you do not provide any personal information we ask for, it may delay or prevent us from providing products to you.

How your Personal Information is collected

We collect most of this personal information directly from you; in person, by telephone, text or email and/or via our website and apps. However, we may also collect information:-

- from publicly accessible sources, e.g. Companies House or HM Land Registry;
- directly from a third party, e.g.:-
  - sanctions screening providers;
  - credit reference agencies;
  - customer due diligence providers;
- from a third party with your consent, e.g. your bank or building society.

How and why we use your Personal Information

Under data protection law, we can only use your personal information if we have a proper reason for doing so, for example:-

- to comply with our legal and regulatory obligations;
- for the performance of our contract with you or to take steps at your request before entering into a contract;
- for our legitimate interests or those of a third party; or
- where you have given consent.

All employees, contractors, and temporary staff who handle personal data must complete GDPR and data protection training.

Training will include:

- UK GDPR principles
- Confidentiality obligations
- Recognising personal and special category data
- Secure handling of information
- Cybersecurity awareness
- Recognising and reporting data breaches
- Subject access requests
- Records management and retention

New starters must complete data protection training:

- As part of induction
- Before accessing sensitive systems where possible
- Within 30 days of commencement

Refresher training will be provided:

- When legislation changes
- Following significant incidents or breaches
- When roles or systems change

Additional training will be provided to staff with higher-risk responsibilities, including:

- HR personnel
- IT administrators
- Managers
- Safeguarding staff
- Finance teams

- Customer service teams

The organisation will maintain records of:

- Attendance
- Completion dates
- Assessment outcomes
- Outstanding training requirements

Failure to complete mandatory training may result in disciplinary action.

A legitimate interest is when we have a business or commercial reason to use your information, so long as this is not overridden by your own rights and interests. The table below explains what we use (process) your personal information for and our reasons for doing so:-

What we use your Personal Information for	**Our reasons**
To provide products to you.	For the performance of our contract with you or to take steps at your request before entering into a contract.
To prevent and detect fraud against you or Cuffe Plc.	For our legitimate interests or those of a third party, i.e. to minimise fraud that could be damaging for us and for you.
Conducting checks to identify our customers and verify their identity; Screening for financial and other sanctions or embargoes; Other processing necessary to comply with professional, legal and regulatory obligations that apply to our business.	To comply with our legal and regulatory obligations.
Gathering and providing information required by, or relating to, audits, enquiries or investigations by Regulatory Bodies.	To comply with our legal and regulatory obligations.
Ensuring business policies are adhered to, e.g. policies covering security and internet use.	For our legitimate interests or those of a third party, i.e. to make sure we are following our own internal procedures so we can deliver the best service to you.
Operational reasons, such as improving efficiency, training and quality control.	For our legitimate interests or those of a third party, i.e. to be as efficient as we can so we can deliver the best service for you at the best price.
Ensuring the confidentiality of commercially sensitive information.	For our legitimate interests or those of a third party, i.e. to protect trade secrets and other commercially valuable information. To comply with our legal and regulatory obligations.
Statistical analysis to help us manage our business, e.g. in relation to our financial	For our legitimate interests or those of a third party, i.e. to be as efficient as we can so we can deliver the best service for you at the best price.

What we use your Personal Information for	Our reasons
performance, customer base, product range or other efficiency measures.	
Preventing unauthorised access and modifications to systems.	For our legitimate interests or those of a third party, i.e. to prevent and detect criminal activity that could be damaging for us and for you. To comply with our legal and regulatory obligations.
Updating and enhancing customer records.	For the performance of our contract with you or to take steps at your request before entering into a contract. To comply with our legal and regulatory obligations. For our legitimate interests or those of a third party, e.g. making sure that we can keep in touch with our customers about existing orders and new products.
Statutory returns.	To comply with our legal and regulatory obligations.
Ensuring safe working practices, staff administration and assessments	To comply with our legal and regulatory obligations. For our legitimate interests or those of a third party, e.g. to make sure we are following our own internal procedures and working efficiently so we can deliver the best service to you.
Credit reference checks via external credit reference agencies.	For our legitimate interests or those of a third party, i.e. to ensure our customers are likely to be able to pay for our products and services.
External audits and quality checks, e.g. for ISO or Investors in People accreditation and the audit of our accounts.	For our legitimate interests or those of a third party, i.e. to maintain our accreditations so we can demonstrate we operate at the highest standards. To comply with our legal and regulatory obligations.

The above table does not apply to special category personal information, which we will only process with your explicit consent.

Promotional Communications

We may use your personal information to send you updates (by email, text message, telephone or post) about our products, including exclusive offers, promotions or new products.

We have a legitimate interest in processing your personal information for promotional purposes (see above '**How and why we use your Personal Information**'). This means we do not usually need your consent to send you promotional communications. However, where consent is needed, we will ask for this consent separately and clearly.

We will always treat your personal information with the utmost respect and never sell OR share it with other organisations outside Cuffe Plc.

Who we share your Personal Information with

We routinely share personal information with:-

- third parties we use to help deliver our products to you, e.g. payment service providers, warehouses and delivery companies;
- other third parties we use to help us run our business, e.g. consultants;
- third parties approved by you, e.g. social media sites you choose to link your account to or third party payment providers;
- credit reference agencies;
- our insurers and brokers;
- our bank.

We only allow our service providers to handle your personal information, if we are satisfied, they take appropriate measures to protect your personal information. We also impose contractual obligations on service providers to ensure they can only use your personal information to provide services to us and to you. We may also share personal information with external auditors, e.g. in relation to ISO or Investors in People accreditation and the audit of our accounts.

We may disclose and exchange information with law enforcement agencies and Regulatory Bodies to comply with our legal and regulatory obligations.

We may also need to share some personal information with other parties, such as potential buyers of some or all our business, or during a re-structuring. Usually, information will be anonymised but this may not always be possible. The recipient of the information will be bound by confidentiality obligations.

We will not share your personal information with any other third party.

Where your Personal Information is held

Information may be held at our offices, third party agencies, service providers, representatives and agents as described above (see above: '**Who we share your Personal Information with**').

How long your Personal Information will be kept

We will keep your personal information while you have an account with us or we are providing products to you. Thereafter, we will keep your personal information for as long as is necessary:-

- to respond to any questions, complaints or claims made by you or on your behalf;
- to show that we treated you fairly;
- to keep records required by law.

We will not retain your personal information for longer than necessary for the purposes set out in this policy. Different retention periods apply for different types of personal information.

When it is no longer necessary to retain your personal information, we will delete or anonymise it.

Your rights

You have the following rights, which you can exercise free of charge:-

Access	The right to be provided with a copy of your personal information (the right of access).
Rectification	The right to require us to correct any mistakes in your personal information.

To be forgotten	The right to require us to delete your personal information - in certain situations.
Restriction of processing	The right to require us to restrict processing of your personal information - in certain circumstances, e.g. if you contest the accuracy of the data
Data portability	The right to receive the personal information you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party - in certain situations.
To object	The right to object:- ▪ at any time to your personal information being processed for direct marketing (including profiling); ▪ in certain other situations to our continued processing of your personal information, e.g. processing carried out for the purpose of our legitimate interests.
Not to be subject to automated individual decision-making	The right not to be subject to a decision based solely on automated processing (including profiling), that produces legal effects concerning you or similarly significantly affects you.

For further information on each of those rights, including the circumstances in which they apply, please contact us or see:-

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

If you would like to exercise any of those rights, please:-

- email, call or write to us OR our Data Protection Officer—see below: '**How to contact us**'; and;
- let us have enough information to identify you (e.g. our full name, address and customer or matter reference number);
- let us have proof of your identity and address (a copy of your driving licence or passport and a recent utility or credit card bill); and;
- let us know what right you want to exercise and the information to which your request relates.

Keeping your Personal Information secure

- We have appropriate security measures to prevent personal information from being accidentally lost, used or accessed unlawfully. We limit access to your personal information to those who have a genuine business need to access it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.
- We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach, where we are legally required to do so.
- If you want detailed information from Get Safe Online on how to protect your information and your computers and devices against fraud, identity theft, viruses and many other online

problems, please visit. https://www.getsafeonline.org. Get Safe Online is supported by HM Government and leading businesses.

Our IT Security

It is essential that all electronic information is maintained and does not jeopardise business relationships with a failure in technology. Increasingly, business is done via the internet or other forms of electronic communication. It is important that our staff respect the equipment that they are given and ensure that it is kept safe and secure. They should not download any software (from the internet or from emails) or place any hardware into company IT equipment without authorisation from their Line Manager.

When they leave their personal computer (PC) or laptop, they must lock the computer with an effective password. Passwords should not be written down or shared with other employees, unless a Senior Manager requests your password.

At the end of each working day our staff must restart your desktop computer that are connected to our network, but not log in. This is because the account must not be left logged in overnight for security reasons, as maintenance and upgrading will take place overnight.

Laptops should be locked away securely when not in use and kept safe when working from home or out of the office.

How to complain

We hope that we OR our Data Protection Officer can resolve any query or concern you may raise about our use of your information.

The General Data Protection Regulation https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ also gives you right to lodge a complaint with a supervisory authority, in particular in the European Union (or European Economic Area) state where you work, normally live or where any alleged infringement of data protection laws occurred. The supervisory authority in the UK is the Information Commissioner who may be contacted at https://ico.org.uk/make-a-complaint or telephone: 0303 123 1113.

Name Simon Cook

Signed

Position Managing Director

Date 26/05/2026