PINEAPPLE PARTNERS

# Data Protection and Information Governance Policy

| | |
|---|---|
| **Title of Policy Document**<br><br>**Issue Date and Version** | Data Protection and Information Governance<br><br>January 2026 (Version 1) |
| **Author / Department** | Compliance Manager |
| **Signed off by** | <br>Director |
| **Next review date** | January 2027 |
| **Distribution** | All services |
| **First issue date** | January 2026 |

## 1. Purpose

Recruitment runs on personal data: CVs, references, vetting records, payroll details. This policy explains how Pineapple Partners collects, uses, protects and disposes of personal information, and what rights the people behind that data have. It applies to everyone who processes personal data on our behalf: directors, office staff, and any contractor or supplier acting for us.

## 2. The law we work to

We comply with the UK General Data Protection Regulation and the Data Protection Act 2018, together with the Privacy and Electronic Communications Regulations for our marketing, and the Conduct of Employment Agencies and Employment Businesses Regulations 2003 for our recruitment records. Pineapple Partners is registered with the Information Commissioner's Office (ICO) under registration reference ZC197897.

## 3. The principles

All processing follows the seven data protection principles. Personal data is: processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; adequate, relevant and limited to what is necessary; accurate and kept up to date; kept no longer than necessary; processed securely; and handled under our demonstrable accountability, records, training and this policy.

## 4. What we process and why

For candidates: identity, contact details, work history, qualifications, right-to-work evidence,

references, vetting outcomes including DBS status where the role requires it, and pay details for temporary workers. For clients: business contact details and the vacancy information needed to fill roles. For our own staff: normal employment records. Our lawful bases are, variously, taking steps to enter into and perform a contract, our legal obligations as an employment business, and our legitimate interests in running a recruitment service, with consent used where nothing else fits, and always revocable.

## 5. Special category and criminal records data

Health information, and criminal records data gathered through DBS checks, receive extra protection. We process them only where the law allows, for example to meet safer recruitment obligations for care and other regulated roles, or to make reasonable adjustments, keep them strictly access-controlled, and never use them for any other purpose. Our handling of DBS certificates follows our dedicated DBS handling policy and the DBS Code of Practice.

## 6. Individual rights

Everyone whose data we hold has the right: to be informed about how it is used; of access (a subject access request); to rectification of inaccurate data; to erasure where there is no continuing reason to hold it; to restrict processing; to data portability; to object, including to direct marketing, which we always honour; and not to be subject to purely automated decisions with significant effects, we make no such decisions. Requests can be made informally to any member of staff and cost nothing. We respond within one calendar month, extendable only for complex requests and always with an explanation.

## 7. Security and data protection by design

Personal data lives in access-controlled systems, protected by strong authentication, encrypted devices and locked storage for the little paper we keep. Access is limited to the people who need it for their role. New systems and processes are assessed for privacy impact before we adopt them, and data protection is considered at the design stage, not bolted on. Suppliers who process data for us do so under written contracts meeting UK GDPR Article 28.

## 8. Sharing

We share candidate data with clients only as needed to progress a placement, and with referees, vetting providers, payroll and HMRC where the process requires. We never sell personal data. Transfers outside the UK happen only with adequate safeguards in place.

## 9. Retention

Recruitment records are kept for the periods required by employment agency legislation and tax law, and otherwise no longer than needed. Where there is no legal minimum, we apply our documented retention schedule and delete securely, digital data erased, paper cross-cut shredded.

## 10. Breaches

Anyone who suspects a personal data breach, loss, theft, wrong recipient, unauthorised access, reports it to the Compliance Manager immediately. We contain, assess and record every breach, report to the ICO within 72 hours where the breach risks people’s rights and freedoms, and tell the affected individuals without undue delay where the risk to them is high.

## 11. Responsibilities, training and review

The Director holds overall accountability; the Compliance Manager handles day-to-day governance, subject access requests and breach management. All staff complete data protection training at induction and annually. Deliberate misuse of personal data is gross misconduct. This policy is reviewed annually.

## 12. Questions and complaints

Questions about this policy or your data: Mathew Vandermotten, 0161 524 1715, info@cucumber-operations.co.uk. You also have the right to complain to the ICO at ico.org.uk or on 0303 123 1113.