Responsibility:	**Managing Director**	**Date doc. created:**	**12th Dec 2022**
Print name sign off:	Simon Little, Managing Director	**Last review date of doc:**	April 2026
Signature:	Simon Little	**Next review date:**	April 2027

Owner and version control

This document must be approved annually.

Data Protection Policy

1. Purpose

This policy sets out how Best Practice Network Ltd ("BPN") protects personal data, assigns responsibilities, and ensures compliance with applicable data protection legislation.

BPN is committed to processing personal data lawfully, fairly, and transparently, and to safeguarding the rights and freedoms of individuals.

---

2. Legal Framework

BPN processes personal data in accordance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Other applicable data protection and privacy legislation

Where processing involves individuals located in the European Economic Area (EEA), the EU GDPR may also apply.

---

3. Scope

This policy applies to:

- All employees, associates, consultants, and contractors
- All personal data processed by BPN
- All systems, devices, and records used to process personal data

---

4. Definitions

Personal Data – Any information relating to an identifiable individual.
Special Category Data – Sensitive data (e.g. health, ethnicity, religion).
Processing – Any operation performed on personal data.
Data Subject – The individual to whom the data relates.

Data Controller – The organisation determining how and why data is processed.
Data Processor – A party processing data on behalf of the controller.
Personal Data Breach – A security incident leading to accidental or unlawful destruction, loss, alteration, or disclosure of personal data.

---

5. Roles and Responsibilities

5.1 Data Controller

Best Practice Network Ltd is the Data Controller for all personal data it processes.

5.2 Managing Director

The Managing Director has overall accountability for data protection compliance.

5.3 Operations Director

The Operations Director is responsible for operational oversight of data protection and acts as the primary internal contact for data protection matters.

5.4 Data Protection Officer (DPO)

BPN has appointed Judicium as its external Data Protection Officer.

Contact: dataservices@judicium.com

The DPO is responsible for:

- Monitoring compliance
- Providing advice on data protection obligations
- Supporting DPIAs
- Acting as contact for regulators and data subjects

5.5 Employees and Associates

All staff and associates are responsible for:

- Complying with this policy
- Protecting personal data
- Reporting incidents immediately

---

6. Data Protection Principles

BPN adheres to the following principles:

1. **Lawfulness, fairness, and transparency**
2. **Purpose limitation**
3. **Data minimisation**
4. **Accuracy**

5. **Storage limitation**
6. **Integrity and confidentiality (security)**
7. **Accountability**

All personal data must be handled in accordance with these principles.

---

7. Lawful Basis for Processing

BPN will ensure that all processing activities have a valid lawful basis under Article 6 UK GDPR, such as:

- Consent
- Contract
- Legal obligation
- Legitimate interests
- Public task

Where special category data is processed, an Article 9 condition will also be identified.

All processing activities and their lawful bases are recorded in BPN's Record of Processing Activities (RoPA).

---

8. Transparency and Privacy Information

BPN provides clear privacy information to individuals at the point of data collection.

Separate privacy notices are maintained for:

- Staff and associates
- Programme participants
- Website users
- Other stakeholders

These notices explain how personal data is used, retained, and shared.

---

9. Categories of Personal Data

BPN may collect and process the following categories of personal data depending on the individual's relationship with the organisation:

- **Contact Data:** Name, address, email, telephone number
- **Socio-Demographic Data:** Age, gender, education level, job role
- **Financial Data:** Bank details, payroll information, payment records
- **Contractual and HR Data:** Employment records, contracts, performance data
- **Documentary Data:** CVs, identification documents, qualification certificates

- **Identification Numbers:** National Insurance number, professional reference numbers
- **Special Category Data:** Health information, equality data (processed only where lawful)
- **Marketing Preferences:** Communication preferences and consent records
- **Programme Data:** Assessment results, feedback, progression data
- **Technical Data:** IP addresses, browser data, usage analytics

Safeguards for Special Category Data

Special category data is processed only where:

- Explicit consent has been obtained; or
- A legal obligation applies; or
- Another lawful condition under Article 9 UK GDPR is met

Additional safeguards include restricted access and enhanced security controls.

---

10. Information We Collect, Use, and Share

The personal data collected and shared varies depending on the relationship with BPN:

Relationship	Data Collected	Purpose	Lawful Basis	Third Parties
Staff / Directors	Contact, financial, HR data	Employment management, payroll, compliance	Contract, Legal obligation	Payroll providers, pension providers, HMRC, auditors
Associates	Contact, qualifications, bank details	Service delivery, payment, quality assurance	Contract	Payment processors, programme partners
Suppliers / Partners	Contact and financial data	Contract management and payments	Contract, Legal obligation	Financial systems, auditors
Programme Participants	Contact, education, assessment data	Programme delivery and support	Contract, Public task	Facilitators, assessors, awarding bodies, DfE, ESFA, Ofsted
Marketing Contacts	Email and preferences	Communications and insights	Consent / Legitimate interests	Email platforms, CRM systems
Website Users	Technical and cookie data	Website performance and analytics	Legitimate interests / Consent	Analytics providers (e.g. Google), advertising platforms

External Third Parties

BPN may share personal data with the following categories of external recipients where necessary:

- **Government and Regulatory Bodies:** Department for Education (DfE), ESFA, Ofsted, HMRC

- **Programme Delivery Partners:** Facilitators, assessors, quality assurance organisations
- **Service Providers (Data Processors):** IT providers, cloud hosting services, CRM systems, payment processors, marketing platforms
- **Professional Advisers:** Auditors, legal advisers, consultants

All third parties are subject to appropriate contractual controls, including Data Processing Agreements (DPAs), and are required to implement appropriate security measures.

Key Controls

- Only the minimum necessary data is shared
- All sharing is based on a valid lawful basis
- Third-party compliance is assessed and monitored
- Data sharing is recorded in the Record of Processing Activities (RoPA)

---

11. Data Retention

BPN retains personal data only for as long as necessary to fulfil its legal, contractual, and operational obligations.

Standard Retention Periods

Category	Retention Period	Responsible Functions
Staff and Directors	7 years after employment ends	HR, Finance
Associates	7 years after engagement ends	HR, Finance
Suppliers / Partners	7 years after relationship ends	Operations, Finance
Programme Participants	7 years after programme completion	Operations, Assessments, HR
Marketing Contacts	Until consent is withdrawn or no longer valid	Marketing
Unsuccessful Applications	Up to 18 months	HR, Operations

Retention Principles

- Data is retained only where necessary for:
    - Legal compliance (e.g. HMRC, regulatory requirements)
    - Contractual obligations
    - Dispute resolution
    - Quality assurance and audit purposes
- Data will be securely deleted or anonymised when no longer required.
- Where individuals request deletion, requests will be considered in line with legal obligations and exemptions.

Secure Disposal

- Electronic data is permanently deleted using approved methods
- Physical records are destroyed via confidential waste processes
- All disposals are recorded where appropriate

BPN maintains a detailed Data Retention Schedule to support implementation.

---

12. Data Subject Rights

BPN upholds all data subject rights, including:

- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object

All requests must be handled in accordance with BPN procedures and responded to within statutory timeframes.

---

13. Data Security

BPN implements appropriate technical and organisational measures to protect personal data, including:

- Access controls
- Encryption
- Secure storage systems
- Staff training
- Regular system monitoring

Personal data must only be accessed by authorised individuals.

---

14. Data Retention

Personal data will only be retained for as long as necessary.

BPN maintains a separate Data Retention Schedule that defines retention periods for different categories of data.

Data is securely deleted or destroyed when no longer required.

---

15. Data Sharing and Processors

BPN may share personal data with:

- Programme partners
- Government bodies
- Service providers
- Professional advisers

All third-party processors must:

- Enter into a Data Processing Agreement (DPA)
- Provide sufficient guarantees of GDPR compliance

Only the minimum necessary data will be shared.

---

16. International Transfers

Personal data will not be transferred outside the UK unless appropriate safeguards are in place, such as:

- Adequacy regulations
- Standard Contractual Clauses (SCCs)

---

17. Personal Data Breaches

All personal data breaches must be reported immediately via internal reporting channels.

BPN will:

- Investigate all incidents
- Notify the ICO where required (within 72 hours)
- Inform affected individuals where there is a high risk

---

18. Training and Awareness

All staff must complete mandatory data protection training annually.

Additional role-specific training is provided where appropriate.

Training records are maintained and monitored.

---

19. Individual Responsibilities

All individuals must:

- Keep personal data accurate and up to date
- Use secure systems only

- Protect passwords and devices
- Follow all data protection procedures

Failure to comply may result in disciplinary action.

---

20. Use of Devices and Removable Media

Use of removable media must be:

- Authorised
- Encrypted where personal data is stored
- Securely handled and disposed of

Sensitive data must not be stored on unencrypted devices.

---

21. Marketing Communications

BPN will only send marketing communications where there is a valid lawful basis, such as:

- Consent
- Legitimate interests (where appropriate and balanced)

Individuals can opt out at any time.

---

22. Monitoring and Compliance

Compliance with this policy will be monitored through:

- Internal audits
- Training records
- Incident reporting

Non-compliance will be addressed appropriately.

---

23. Related Documents

This policy should be read alongside:

- Information Security Policy
- Data Retention Schedule
- Data Breach Procedure
- Subject Access Request Procedure
- Privacy Notices

- Cookie Policy

---

24. Review and Approval

This policy will be reviewed annually or sooner if required due to:

- Legislative changes
- Organisational changes
- Identified risks or incidents

---

25. Controlled Procedures

The following procedures support this policy and are maintained as separate controlled documents:

- Personal Data Breach Procedure
- Data Subject Access Request (DSAR) Procedure
- Data Portability Procedure
- Data Security Rules and Acceptable Use Standard
- Data Protection Training Procedure

Each procedure includes:

- Defined ownership
- Version control
- Approval records
- Detailed operational steps

All staff must follow these procedures in conjunction with this policy.