

Responsibility:	Managing Director	Date doc. created:	12th Dec 2022
Print name sign off:	Simon Little, Managing Director	Last review date of doc:	March 2025
Signature:	Simon Little	Next review date:	April 2026

Owner and version control

This document must be approved annually.

Data Protection Policy

Best Practice Network acknowledges its legal obligation to comply with the **General Data Protection Regulation (GDPR) (EU) 2016**. The GDPR applies to all personal data—defined as any information relating to an identifiable individual—regardless of format (digital, physical, or otherwise).

Processing refers to any operation performed on personal data, including **collecting, recording, storing, using, sharing, or deleting** it. All personnel must maintain the confidentiality of such data and adhere strictly to GDPR principles.

The EU GDPR supersedes the **Data Protection Directive 95/46/EC**, harmonising data privacy laws across Europe. It safeguards individuals' rights and imposes rigorous standards for organisational accountability.

Transparency & Data Subject Rights

Best Practice Network provides **Data Subjects** (individuals whose data we process) with a **Privacy Notice** at the point of data collection. This notice outlines:

- The purpose and legal basis for processing.
- How long data will be retained.
- Their rights (e.g., access, rectification, erasure).

Key Definitions & GDPR Applicability

The GDPR applies to all **personal data** (any information relating to an identifiable individual) processed by Best Practice Network, whether as a **Data Controller** or **Data Processor**.

Roles & Responsibilities

1. Data Controller

Determines the *purposes* and *means* of processing personal data.

Best Practice Network's Designation:

- The **Managing Director (MD)** acts as the organisation's **Data Protection Controller**, with accountability delegated through the **Senior Leadership Team** and **Line Management** to relevant staff.
- **Enquiries:** Contact the **Operations Director, Joanne Hawkins**-
joannahawkins@bestpracticenet.co.uk initially for issues regarding personal data.

2. Data Processor

- Processes data *on behalf of* the Controller (e.g., IT, finance, or marketing providers).
- **Best Practice Network's Requirements:**
 - All third-party processors (e.g., advisers, agencies, sponsors) must:
 - Maintain a **GDPR-compliant Data Protection Policy**.
 - Accept our policy terms within contractual agreements.

3. Data Protection Officer (DPO)

- **Role:** Monitors compliance, advises on GDPR obligations, conducts **Data Protection Impact Assessments (DPIAs)**, and liaises with data subjects and regulators.
- **Appointment:** Best Practice Network has appointed **Judicium** as its DPO.
 - **Contact:** dataservices@judicium.com

Data protection principles

Best Practice Network retains necessary information about employees, clients, and suppliers to fulfil financial, commercial, legal, and health and safety obligations. All personal data must be:

- **Collected and used lawfully.**
- **Stored securely.**
- **Disclosed only to authorised individuals with a legitimate need.**

In alignment with the **General Data Protection Regulation (GDPR) 2016**, we adhere to the following principles. Personal data must be:

1. Processed Lawfully, Fairly, and Transparently

- Collected only where a valid legal basis exists (e.g., consent, contract, legal obligation).
- Data subjects must be informed of:
 - The identity of the **Data Controller** (Best Practice Network).
 - The purpose(s) of processing.
 - Retention periods.
 - Any third-party disclosures.

2. Collected for Specified, Legitimate Purposes

- Not reused in ways incompatible with the original purpose.

3. Adequate, Relevant, and Limited

- Only the minimum necessary data for the intended purpose is collected.

4. Accurate and Up to Date

- Inaccurate data must be corrected or erased without delay.

5. Retained Only as Long as Necessary

- Defined retention periods apply, after which data is securely deleted.

6. Processed in Line with Data Subjects' Rights

- Includes rights to access, rectification, erasure, and objection.

7. Protected by Robust Security Measures

- Technical and organisational safeguards (e.g., encryption, access controls) prevent unauthorised access, loss, or damage.

8. Not Transferred Outside the EEA Without Safeguards

- Transfers require adequacy decisions (e.g., UK GDPR) or approved mechanisms (e.g., Standard Contractual Clauses).

All employees must comply with these principles when handling personal data.

Training and awareness

To uphold compliance with the **General Data Protection Regulation (GDPR) 2016** and Best Practice Network's policies:

1. Mandatory Annual Training

- All staff complete **data protection and information security training** annually.
- Covers:
 - GDPR principles and legal obligations.
 - Updates to BPN's policies and procedures.
 - Practical safeguards (e.g., secure data handling, breach reporting).

2. Role-Specific Integration

- Data protection is a **standard agenda item** for:
 - **Facilitator training days.**
 - **Associate induction and refresher sessions.**
- Tailored guidance for roles with higher data access (e.g., HR, IT).

3. Accountability

- Training attendance is **recorded** and monitored.
- Non-compliance may result in disciplinary action.

Individual responsibility

As an employee, associate, or consultant of Best Practice Network, you are responsible for:

1. Data Accuracy & Updates

- Ensuring all information provided (e.g., contact details, qualifications) is **accurate and up to date.**
- Promptly notifying the Company of changes (e.g., address, bank details).

2. Policy Compliance

- Adhering to the **Data Protection and Information Security Policy** at all times.
- Completing mandatory training and staying informed of updates.

3. Accountability for Access

- You are **personally accountable** for all system activity under your login credentials (User ID), whether authorised by you or not.
- Never share passwords or leave devices unlocked/unattended.

4. Consequences of Non-Compliance

- Breaches (deliberate or negligent) may result in:
 - Disciplinary action, up to and including termination.
 - Criminal prosecution in severe cases (e.g., unlawful data disclosure).

5. Associates/Consultants

- All personal data processed on behalf of BPN must comply with this policy.

Refer to **Appendix 1** for detailed Data Security Rules.

Lawful basis for processing personal data

Best Practice Network acknowledges its obligation to identify and document a valid lawful basis for all personal data processing activities, as required by the **General Data Protection Regulation (GDPR) 2016**.

Our Approach

To ensure compliance, we:

1. **Purpose Assessment**
 - Review each processing activity and select the **most appropriate lawful basis** (e.g., consent, contractual necessity, legal obligation, legitimate interest).
2. **Necessity Evaluation**
 - Confirm processing is **strictly necessary** for its intended purpose, with no reasonable alternative.
3. **Documentation & Transparency**
 - Record the lawful basis for each activity in our **GDPR Action Log** to demonstrate compliance.
 - Clearly communicate both the **purpose** and **lawful basis** in our **Privacy Notice**.

Accessing Lawful Basis Information

The lawful basis for specific processing activities is documented in:

- Our **Privacy Notice** (for external transparency).
- The **GDPR Action Log** (internal compliance record).

Rights of data subjects

Best Practice Network fully recognises and upholds the rights of data subjects under the **General Data Protection Regulation (GDPR) 2016**.

Right to Information & Access

Data subjects have the right to know:

- **What personal data** we hold about them and **why** it is processed.
- **How to access** their data (via a Subject Access Request).
- **How we maintain accuracy** and update their information.
- **Details of any automated decision-making** that significantly affects them (including profiling).
- **Our compliance measures** under GDPR.

Right to Restrict Processing

Data subjects may request limitations on processing where:

- It risks causing **damage or distress** or is **unlawful**.

- Used for **direct marketing purposes**.
- Results in **fully automated decisions** with significant effects.
- Data is **inaccurate** or **no longer necessary** for its original purpose.

Right to Data Portability

- Individuals may **request their data** in a structured, commonly used, and machine-readable format.
- They have the right to **transfer this data** securely between service providers without obstruction.

Exercising These Rights

For guidance on:

- Responding to data subject requests
- Reporting personal data breaches
- Implementing the right to data portability

Refer to *Appendix 3* for detailed procedures.

Retention policy

Best Practice Network is legally required to retain records of candidates, associates, and staff for specified periods after their contractual relationship ends.

Retention Periods by Data Subject Category

Relationship with BPN	Retention Period	Responsible Departments
Staff and Directors	7 years	HR, Finance
Associates	7 years	HR, Finance
Suppliers/Partner Hubs	7 years	Operations, Finance
Programme Candidates	7 years	Operations, Assessments, HR, Finance
Newsletter Members	Until consent withdrawal	Marketing

Key Responsibilities

1. **Departmental Accountability:**
 - Each department must ensure **only necessary data** is retained post-contract.
 - Regular audits will verify compliance with retention schedules.
2. **Early Deletion Requests:**
 - Data Subjects may request **early deletion** of their data, subject to legal exceptions.
 - For procedures, refer to *Appendix 3: Responding to Data Subject Access Requests*.

Compliance Measures

- **Secure Deletion:** Data is permanently erased using approved methods (e.g., encryption shredding) upon expiry.
- **Documentation:** All deletions are logged for audit purposes.

Removable media policy

Definition & Scope

Removable media includes any portable storage device not permanently fixed to company systems (e.g., USB drives, memory cards, external hard drives, and company-issued laptops/mobile devices).

General Use Guidelines

1. **Permitted Use:**
 - Allowed for **non-sensitive data** transport when there is a **valid business need**.
 - Restricted to authorised staff only.
2. **Security Measures:**
 - All company machines (source/destination) must have **up-to-date antivirus software** (managed by Kocho).

Handling Sensitive Data

- **Encryption Required:** Sensitive data must be encrypted to **AES-256 standard** or equivalent.
- **Off-Site Use:** Prior approval from Kocho is mandatory before removing encrypted media from office premises.

User Responsibilities

- **Protection:** Physically secure devices against loss, theft, or damage during transit/storage.
- **Return/Destruction:**
 - Report **damaged devices** to Kocho for secure disposal.
 - Return devices upon **employment termination** for destruction or reissue.
- **Data Disposal:**
 - Use **irrecoverable deletion methods** (e.g., cryptographic erasure) after use.
 - Alternatively, **physically destroy media** if reuse is unintended.

Compliance Enforcement

- **Breach Reporting:** Immediately notify Kocho of **lost/stolen devices**.

Marketing and communications policy

Purpose of Marketing

Best Practice Network may contact data subjects to:

- Seek opinions or offer insights.
- Share research on education sector developments.
- Inform about relevant policies, funding opportunities, or programmes.

Consent-Based Approach

1. Standards for Consent

- Marketing communications are sent **only to individuals who have given explicit, informed consent**.
- Consent must:
 - Provide genuine choice and control.
 - Be separate from other terms and conditions.
 - Be easy to understand and withdraw.

2. Consent Request Requirements

Requests clearly state:

- **Our identity:** "Best Practice Network" (and any third parties relying on consent).
- **Purpose:** Why data is collected and how it will be used.
- **Withdrawal right:** Individuals may opt out anytime.

3. Active Opt-In

- **No pre-ticked boxes** – consent must be a positive action (e.g., ticking an empty box).
- **Records maintained:** Includes who consented, when, how, and what they were told.

Managing Consent

- **Easy Withdrawal:** Clear "unsubscribe" options in all communications.
- **Regular Reviews:** Consent is refreshed if processing purposes change.

Appendices

Appendix 1: Data security rules for staff and associates

Device & Access Security

1. **Lock screens** when leaving devices unattended (even briefly).
2. **Log out** of all BPN systems (CCMS, SAGE, Outlook, BPN network) after use.
3. **Never share passwords** or credentials for any BPN systems.

Data Storage & Handling

4. **Store personal data** only in:
 - Password-protected BPN secure systems (e.g., SharePoint, encrypted drives).
 - **Temporary local storage** (e.g., laptop hard drives) only if essential, and always encrypted.
5. **Removable media:**
 - Must use **encryption** (e.g., BitLocker, AES-256) for personal data.
6. **Hard copies:**
 - Keep in **locked cabinets**; shred via **confidential waste sacks** (never general bins).

Communication Protocols

7. **Verbal/written disclosures:**
 - Avoid sharing with **unauthorised parties** (even accidentally).
 - Conduct sensitive calls **in private spaces**.
8. **Special category data:**
 - Requires **explicit consent** before third-party sharing.
9. **Emails:**
 - **Password-protect attachments**; send passwords separately.
 - Open only **trusted sender** attachments.
 - Delete personal data from emails once logged in secure systems.

Incident Reporting

10. **Report breaches immediately** to:
 - Data Controller
 - Operations Director
 - IT Systems*(Include: lost devices, incorrect processing/sharing, or suspicious activity.)*

Prohibited Actions

11. **Do not:**
 - Use BPN contact details for **non-work purposes**.
 - Leave sensitive documents **unsecured** (e.g., on desks, printers).

Appendix 2: Privacy Notice

Who We Are

Best Practice Network Limited (Company No. **04566320**) delivers professional development programmes for educators in partnership with schools, early years providers, universities, and colleges.

Your Data Rights Under GDPR

Since **25 May 2018**, you have the right to:

- Access, correct, or request deletion of your data
- Object to processing or request data portability
- Withdraw consent (where applicable)
- Lodge complaints with the ICO (www.ico.org.uk)

Our Privacy Commitment

We collect only necessary data to:

- Deliver contractual services
- Comply with legal obligations (e.g., safeguarding, HMRC)
- Improve our programmes (based on legitimate interests)

How We Protect Your Data

- **Controller:** Best Practice Network Ltd (Registered Office: Newminster House, 27-29 Baldwin Street, Bristol BS1 1LT)
- **Processors:** All third parties (e.g., IT providers) are GDPR-compliant under strict contracts
- **Security:** Encryption, access controls, and regular audits


Lawful Processing Bases

We process data only when:

- ✓ **Consent:** You opt-in (e.g., marketing)
- ✓ **Contract:** To deliver services you've requested
- ✓ **Legal Duty:** Statutory requirements
- ✓ **Public Task:** Official education functions
- ✓ **Legitimate Interest:** Carefully balanced against your rights

Contact Us

For data requests or concerns:

 **Data Protection Officer:** dataservices@judicium.com

 **Operations Manager:** [Insert Phone]

 **Post:** FAO Data Protection, Newminster House, Bristol BS1 1LT

What information we collect about you

The personal data we collect depends on your relationship with Best Practice Network:

Relationship	Data Collected	Purpose of Processing	Lawful Basis
Staff/Directors	Contact details, ID numbers, financial data, employment records, consents	Employment management, payroll, legal compliance	Contract, Legal obligation
Associates	Contact details, qualifications, bank details, DBS checks, consents	Contracting services, payment processing, quality assurance	Contract, Consent
Suppliers/Partners	Contact details, financial information, contract documents	Managing partnerships, processing payments	Contract, Legal obligation
Programme Candidates	Contact details, educational history, assessment data, equal opportunities	Delivering training programmes, providing support, quality improvement	Contract, Consent, Public task
Newsletter Members	Email address, communication preferences	Sending sector insights, marketing (where consented)	Consent
Website Visitors	IP address, cookies, browsing behaviour	Improving website functionality, personalised marketing (legitimate interests)	Legitimate interests

Key Notes:

1. **Special Category Data:** We only process sensitive data (e.g., equal opportunities information) with explicit consent or where legally required.
2. **Minimisation Principle:** We collect only what is necessary for each purpose.
3. **Transparency:** Full details of processing activities are recorded in our GDPR Register.

Your Control:

- Update preferences via your online account or by contacting dataservices@judicium.com
- Withdraw consent for marketing at any time (unsubscribe link in all emails)

Categories of personal data

Best Practice Network may collect and process the following types of personal data, as required by your relationship with us:

Category	Description	Special Considerations
Contact Data	Full name, address, email, phone number	Stored in encrypted systems; accessible only to authorised personnel
Socio-Demographic Data	Age, gender, education level, job role, nationality	Used only for equality monitoring or programme customisation (with consent)

Financial Data	Bank details, payroll information, invoice records	Protected via PCI-compliant systems; retained for 7 years for HMRC compliance
Contractual & HR Data	Employment contracts, performance reviews, disciplinary records	Access restricted to HR and line managers
Documentary Data	CVs, passport copies, driving licences, qualification certificates	Digitally stored with watermarking; physical copies kept in locked cabinets
Identification Numbers	National Insurance number, Teacher Reference Number (TRN)	Never used as sole identifiers; pseudonymised where possible
Special Category Data	Racial/ethnic origin, religious beliefs, disability status, sexual orientation	Processed only with explicit consent (Article 9 GDPR) or legal obligation (e.g., safeguarding)
Marketing Preferences	Opt-in/out status for newsletters, sector updates	Updated via self-service portal or direct request
Consent Records	Date, method, and scope of consent given	Logged in auditable systems; separate from operational data
Programme Assessment Data	Assignments, feedback, grades, certification outcomes	Retained for 7 years (QAA requirements); anonymised for research where applicable
Technical Data	IP address, browser type, cookie data, website interaction patterns	Collected via cookie banners (legitimate interests); used only for analytics/security

Key Safeguards for Special Category Data

We process sensitive data **only** when:

- ✓ **Explicit consent** is given (e.g., disability status for reasonable adjustments)
- ✓ **Legal obligation** applies (e.g., safeguarding checks in education)
- ✓ **Vital interests** are at stake (e.g., medical emergencies)

Who we share your personal information with

Internal Sharing

Your data may be accessed by authorised personnel within:

- **Best Practice Network**
- **Supporting Education Group** (our parent company)
Only when strictly necessary for purposes such as:
 - ✓ HR administration
 - ✓ Programme delivery
 - ✓ Financial processing

External Third Parties

We share data with these categories of recipients *only when justified*:

Recipient Type	Examples	Purpose	Legal Basis
Programme Partners	Facilitators, assessors, quality assurance bodies	Delivering and certifying training programmes	Contract, Public task
Government Bodies	DfE, ESFA, Ofsted, HMRC	Compliance with statutory reporting/audits	Legal obligation
Educational Institutions	Schools, colleges, or new training providers	Ensuring continuity of learning (DfE requirements)	Public task
Data Processors	Cloud IT providers, payment processors, marketing platforms	Secure service delivery under strict contracts	Article 28 GDPR compliance
Professional Advisers	Auditors, legal counsel	Regulatory or legal requirements	Legal obligation

Key Safeguards

- **School Transfers:** For participants changing schools, we share only:
 - Name & contact details
 - Programme progress data
(Strictly limited to DfE requirements)
- **Contracts:** All third parties sign GDPR-compliant Data Processing Agreements (DPAs).
- **Minimisation:** We disclose only the **minimum necessary data** for each purpose.

Your Rights

You can:

- Request a list of current data processors
- Object to specific sharing (where no legal basis overrides)

Contact our DPO at dataservices@judicium.com to exercise these rights.

Marketing communications

Purpose of Marketing Communications

Best Practice Network may contact you to:

- Request feedback on education sector developments
- Share relevant research insights and policy updates
- Provide information about programmes, funding opportunities or services aligned with your professional interests

Data Sources for Personalisation

We may use information from:

- Details you provide during programme applications or enquiries
- Your engagement with our services and resources

- Reputable third-party sources in the education sector

Legal Basis for Processing

Marketing communications will only be sent where:

1. **Consent:** You have actively opted in (e.g., newsletter subscriptions)
2. **Legitimate Interest:** Where we have a valid business reason that doesn't override your rights (e.g., informing past participants about programme developments)

Your Communication Preferences

- Essential service communications regarding your current programmes will continue regardless of marketing preferences
- We will periodically reconfirm your preferences:
 - When you enrol in new programmes
 - Following significant regulatory changes
 - During organisational restructuring

Managing Your Preferences

You may update your choices at any time by:

- Emailing: enquiries@bestpracticenetwork.co.uk
- Using the unsubscribe link in all marketing emails
- Calling: 0117 920 9200

Third-Party Communications

We do not sell or share your data for external marketing purposes without your explicit additional consent.

Use of cookies

How We Use Cookies

Best Practice Network uses cookies to:

- Temporarily store your device type and location preferences to optimise your website experience
- Enable remarketing services to display relevant content across Google platforms based on your previous interactions with our site

Your Cookie Controls

- **Opting Out:** You may disable remarketing cookies through your web browser's settings:
 1. Access your browser's preferences or settings menu
 2. Locate the privacy or security section
 3. Adjust your cookie preferences accordingly

- **Full Details:** Our comprehensive Cookie Policy provides complete information about:
 - The specific cookies we use
 - Their individual purposes
 - Their duration periods

Legal Basis

All non-essential cookies are deployed only after obtaining your explicit consent through our cookie banner. Essential operational cookies are used under legitimate interest to maintain basic website functionality.

Third-Party Cookies

We utilise Google Analytics and Google Ads cookies for:

- Website performance measurement
- Targeted advertising (where consented)
These services may transfer data to servers outside the UK, protected by Standard Contractual Clauses.

For any questions about our cookie practices, please contact our Data Protection Officer at dataservices@judicium.com

How long we keep your personal data

Active Relationships

We retain your personal data for the **duration** of your:

- Programme participation
- Employment contract
- Service subscription
- Ongoing business relationship

Post-Contract Retention (Up to 7 Years)

After your relationship ends, we may keep data where necessary for:

- ✓ **Legal compliance** (e.g., HMRC, QAA requirements)
- ✓ **Dispute resolution** (questions/complaints)
- ✓ **Quality assurance** (demonstrating fair treatment)
- ✓ **Professional references** (for former staff/associates)

Early Deletion Requests

You may request earlier deletion by contacting:

Email: dataservices@judicium.com

Post: FAO Data Protection Officer, Best Practice Network, Newminster House, 27-29 Baldwin St, Bristol, BS1

1LT

Note: We may retain minimal data if legally required.

Unfulfilled Applications

- **Expression of Interest/Applications:** Deleted after **18 months** if no contract established
- **Withdrawn Applications:** Deleted within **30 days** of withdrawal notification

Exceptions

Certain data may be retained longer for:

- **Archival research** (anonymised where possible)
- **Legal proceedings** (until case resolution)

How to get a copy of your personal information

How to Make a Subject Access Request

You may obtain a copy of your personal data by:

1. Completing our **Data Subject Access Request Form**
2. Sending a written request containing:
 - Your full name and contact details
 - Proof of identity (e.g., copy of passport/driving licence)
 - Specific details of the information requested

Submit to:

Data Protection Officer
Best Practice Network
Newminster House, 27-29 Baldwin Street
Bristol, BS1 1LT
Email: dataservices@judicium.com

Our Process

- **Verification:** We will confirm your identity before processing
- **Response Time:** Within **1 calendar month** of receipt (may extend by 2 months for complex requests)
- **Format:** Electronic copy (default) or paper format by request

Fees

- **Standard Requests:** Free of charge
- **Excessive Requests:** May charge a reasonable fee based on administrative costs
- **Manifestly Unfounded Requests:** Reserve the right to refuse (with explanation)

What We Provide

- Copies of personal data we hold
- Purposes of processing
- Categories of data
- Recipients or recipient categories
- Retention periods
- Your GDPR rights

Exceptions

We may withhold information where it would:

- Affect the rights of others
- Relate to ongoing legal proceedings
- Include legally privileged information

For assistance with your request, contact our DPO at dataservices@judicium.com or 0117 920 9200.

Letting us know if your personal information is incorrect

To update your information:

1. Contact:

- **Email:** dataservices@judicium.com
- **Post:** Data Protection Officer, Best Practice Network, Newminster House, 27-29 Baldwin Street, Bristol, BS1 1LT
- **Phone:** 0117 920 9200

2. Provide:

- Proof of identity (e.g., passport copy)
- Evidence supporting the correction (e.g., utility bill for address change)
- Clear explanation of required changes

Our Process

- **Verification:** We will confirm your identity within **20 working days**
- **Assessment:** Review requested changes against evidence provided
- **Action:**
 - Correct verified inaccuracies within **1 month**
 - Where disputes arise, add a supplementary statement to your record
- **Notification:** We will inform you and any relevant third parties of updates

Ongoing Obligations

Please proactively notify us of changes to:

- Contact details
- Professional qualifications
- Payment/bank details
- Other critical information

Dispute Resolution

If we cannot resolve a disagreement about accuracy:

- You may request restriction of processing
- You may lodge a complaint with the ICO (www.ico.org.uk)

Your Control Over Personal Data Use

You may exercise the following rights regarding your personal data:

1. Right to Object

- Challenge our processing where:
 - Based on legitimate interests
 - Used for direct marketing
 - Involves automated decision-making

2. Right to Erasure ('Right to Be Forgotten')

- Request deletion where:
 - Data is no longer necessary
 - You withdraw consent (where applicable)
 - Processing was unlawful

3. Right to Restriction

- Limit processing while:
 - Accuracy disputes are resolved
 - Processing legality is investigated
 - You need data preserved for legal claims

How to Exercise These Rights

Submit a written request including:

- Your full contact details
- Specific data/content concerned
- Reason for request (e.g., "object to marketing")
- Supporting evidence (for accuracy disputes)

Submit to:

Data Protection Officer
Best Practice Network
Newminster House, 27-29 Baldwin Street
Bristol, BS1 1LT
Email: dataservices@judicium.com

Our Obligations

- **Response Time:** Within 1 month (extendable for complex requests)
- **No Fee:** Unless manifestly unfounded/excessive
- **Verification:** May require ID confirmation

Important Considerations

We may continue processing if:

- Required by law (e.g., safeguarding records)
- Necessary for legal claims
- For public interest tasks

Example: We retain programme assessment records for 7 years per QAA requirements, even if requested for erasure.

Dispute Resolution

If unsatisfied with our response:

1. Internal appeal to our DPO
2. Complaint to ICO (www.ico.org.uk)

How to withdraw your consent

You can withdraw your consent at any time. Please contact us if you want to do so.

This may mean that we cannot provide you with relevant information regarding our products and services. We will notify you if this is the case.

Right to Data Portability

Your Entitlement

Under GDPR (effective 25 May 2018), you may request:

- A copy of your personal data in a **structured, machine-readable format** (e.g., CSV, JSON)
- Direct transmission to another organisation (where technically feasible)

Applicable Data

This right applies to:

- ✓ Data you provided to us
- ✓ Data generated through your use of our services (e.g., programme progress records)
- ✓ Data processed by automated means under:

- Your consent, or
- Performance of a contract

How to Request

Submit a written request including:

1. Your full contact details
2. Specific datasets required
3. Preferred format (if applicable)
4. Destination organisation details (for direct transfers)

Submit to:

Data Protection Officer
Best Practice Network
Newminster House, 27-29 Baldwin Street
Bristol, BS1 1LT
Email: dataservices@judicium.com

Our Process

- **Verification:** Identity confirmation within 5 working days
- **Response:** Provided within 1 month (free of charge)
- **Format Options:**
 - CSV (standard)
 - JSON (API-compatible)
 - PDF (human-readable backup)

Limitations

Does not apply to:

- Data processed under legal obligations
- Data containing others' personal information
- Manual (paper-based) records



Appendix 3: Data Protection Procedures

1. Reporting a Personal Data Breach

Step 1: Immediate Notification

- **Contact:** Judicium (Our Data Protection Officer)
Email: dataservices@judicium.com

Step 2: Provide Key Details

Include in your report:

- Nature of the breach (e.g., accidental email disclosure)
- Number of affected individuals
- Types of data compromised (e.g., names, financial details)
- How the breach was discovered
- Any immediate containment actions taken

Step 3: Follow-Up

- Judicium will:
 - Log the incident and assess risk severity
 - Report to the ICO within 72 hours if high risk
 - Advise on remedial actions

Note: All breaches must be reported within 24 hours of discovery to ensure ICO compliance.

2. Responding to Data Subject Access Requests (DSARs)

Process Overview

1. **Receipt:** Forward all DSARs to:
Joanna Hawkins, Operations Director
Email: joannahawkins@bestpracticenet.co.uk
Phone: +44 (0)117 920 9421
2. **Verification:**
 - Confirm requester's identity (e.g., via secure portal or signed request)
3. **Fulfilment:**
 - Provide data within 1 calendar month
 - Format: PDF (default) or structured format (e.g., CSV) upon request

Exceptions:

- May extend by 2 months for complex requests
- May charge a fee for manifestly unfounded/repetitive requests

3. Implementing Data Portability Requests

Requirements:

- Provide data in machine-readable formats (CSV, JSON, XML)
- Include:
 - Data provided by the subject
 - Observed data (e.g., programme progress)
 - Inferred data (e.g., assessment analytics)

Process:

1. **Direct Requests** to Joanna Hawkins (contact details above)
2. **Validation:** Verify identity and scope
3. **Delivery:** Within 1 month, via:
 - Secure email encryption
 - Password-protected cloud transfer

Limitations:

- Excludes data processed under legal obligations
- Excludes manual/paper records