


Data Protection Policy

Owner and version control

Responsibility:	Joanne Hawkins Development Director	Date doc. created:	12 th Dec 2022
Print name sign off:	Simon Little, Managing Director	Last review date of doc:	12 th Dec 2022
Signature:		Next review date:	December 2023

This document must be approved annually by Senior Leadership Team and presented to the Board.

Best Practice Network recognises its legal requirement to comply with the General Data Protection Regulation (GDPR; EU) 2016. The GDPR covers information that is in any form - it is equally applicable whether the data is computerised, manual or in any other format. All Best Practice Network personnel are required to maintain the confidentiality of any personal data held by the company in whatever form. The EU GDPR replaces the Data Protection Directive 95/46/EC and is designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.

Best Practice Network understands that it must provide those about whom we process data (the Data Subjects) with information about how their data will be processed and used, this will be done through a **Privacy Notice** at the time we obtain their data.

Key definitions

Who does the GDPR apply to?

Data controller: determines the purposes and means of processing personal data.

To ensure the implementation of this policy the company has designated the Managing Director as the company's data protection controller. The MD delegates accountability and authority through the Senior Leadership team and Line Management structure to the staff members responsible for each area of activity. All enquiries relating to the holding of personal data should be referred to the Operations Manager in the first instance.

Data processor: responsible for processing personal data on behalf of a controller.

Best Practice Network employs a number of data processors who work with us to provide IT, finance, marketing and other services.

We require any third party service providers, including our professional advisers, marketing agencies and sponsors, to have in place their own GDPR compliant Data Protection and Information Security Policy's and to confirm acceptance of ours within our standard contract documents.

Data Protection Officer: DPOs assist BPN to monitor internal compliance, inform and advise on our data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

Best Practice Network has appointed the Operations Manager as our DPO.

What information does the GDPR apply to?

Personal data: any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Sensitive personal data: The GDPR refers to sensitive personal data as “special categories of personal data” (see Article 9). The special categories specifically include, but are not limited to, racial or ethnic origin, religious or philosophical beliefs and sexual orientation where processed to uniquely identify an individual.

Data protection principles

The company needs to keep certain information about its employees, clients, and suppliers for financial and commercial reasons and to enable us to monitor performance, to ensure legal compliance and for health and safety purposes. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. In practice, this means that only those who have a necessary and lawful need to access the data will be able to do so.

Best Practice Network abides by the Data Protection Principles set out in the General Data Protection Regulation (2016). These principles require that personal data must be:

- obtained fairly and lawfully and shall not be processed unless certain conditions are met - including informing data subjects of the identity of the data controller, processing purpose(s), an indication of the period for which the data will be kept and, if appropriate, any third party disclosures which are envisaged
- obtained for specified and lawful purposes and not further processed in a manner incompatible with that purpose
- adequate, relevant and not excessive
- accurate and up to date
- kept for no longer than necessary
- processed in accordance with data subjects' rights
- protected by appropriate security
- not transferred to a country outside the European Economic Area without adequate protection

In processing or using any personal data all Best Practice Network personnel must ensure that they follow these principles at all times.

Training

Staff will be trained annually on data protection and information security to ensure continuing compliance with the GDPR (2016) and brief them on any updates to BPN policies regarding data protection.

Data protection and information security will be a standard item on facilitator and associate training days.

Individual responsibility

As an employee you have a responsibility to:

- check that any information that you provide in connection with your employment is accurate and up-to-date

- notify the Company of any changes to information you have provided, for example changes of address
- ensure that you are familiar with and follow the Data Protection and Information Security Policy's

Remember, you will be accountable for all terminal activity and transactions entered through your User ID whether or not you were present at the time.

Any breach of the Data Protection Policy, either deliberate or through negligence, may lead to disciplinary action being taken and could in some cases result in a criminal prosecution.

As an associate/consultant with Best Practice Network, any personal data you process will be handled in accordance with the DPP.

Please see [Appendix 1](#) for a list of data security rules we expect all BPN staff and associates to adhere to.

Lawful basis for processing personal data

Best Practice Network recognises that we must have a lawful basis in order to process personal data. In line with this the Company:

- reviews the purposes of our processing activities, and selects the most appropriate lawful basis (or bases) for each activity.
- checks that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.
- documents our decision on which lawful basis applies to help us demonstrate compliance.
- includes information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.

The lawful basis for each of our personal data processing activities can be found either within our [Privacy notice](#) or GDPR Action Log.

Rights of data subjects

Best Practice Network recognises the rights of its data subjects. All data subjects are entitled to know:

- what personal information the company holds about them and the purpose for which it is used
- how to gain access to it
- how it is kept up to date
- the mechanics of any automated decision making process that will significantly affect them
- what the company is doing to comply with its obligations under the 2016 Regulation

Data subjects have the right to prevent:

- processing that is likely to cause damage or distress or is unlawful
- processing for direct marketing purposes
- processing which would result in significant decisions being taken about them by an entirely automated process
- storage of data which is inaccurate or where there is no compelling reason for its continued processing.

Data subjects now have the right to data portability, which allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer

personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

For information on 'How to respond to a request by data subject', 'How to report a personal data breach' and 'How to action the 'Right to data portability'' see [Appendix 3](#).

Retention policy

Best Practice Network is legally obliged to keep records of its candidates, associates and staff after they have concluded their contract with us.

Please see below for information on how long we are required to keep each Data Subjects personal data:

Relationship with BPN	Retention period	Associated departments
Staff and Directors	7 years	<ul style="list-style-type: none">• HR• Finance
Associates	7 years	<ul style="list-style-type: none">• HR• Finance
Suppliers/Partner Hubs	7 years	<ul style="list-style-type: none">• Operations• Finance
Candidates on one of our programmes	7 years	<ul style="list-style-type: none">• Operations• Assessments• HR• Finance
Newsletter members	Can keep details until Data Subject withdraws consent	<ul style="list-style-type: none">• Marketing

It is the responsibility of each associated department to ensure that only necessary personal data is retained after the conclusion of a contract. For information on retention policy processes specifically related to candidates and the Operations team, see [Appendix 3](#).

Data Subjects may request for their data to be removed from our systems before we are contractually obliged. See 'how to respond to a data subject' in [Appendix 3](#) to deal with a request of this sort.

Removable media

Removable media refers to all types of computer storage which are not physically fixed inside a Company computer and includes, but is not limited to, company laptops, memory cards, USB sticks and mobile devices.

The use of removable media is not prohibited within BPN; it is in fact an essential part of everyday business. The use of removable media to transport non-sensitive data can be done on standard devices. However, shall only be used by staff who have an identified and business need for them.

Regularly updated Antivirus software (maintained by Helpdesk) is present on all Company-owned machines from which the data is taken, and Company-owned machines on which the data is to be loaded.

When removable media is used to transport sensitive data, the data on the device must be encrypted data and should not be removed from the office without prior agreement from Helpdesk.

It is the responsibility of all BPN employees using removable media to ensure encryption of data to the highest standard if they are going to be used to hold sensitive or highly sensitive Company data and to physically protect it against loss, damage, abuse or misuse when in use, storage and transit.

Data stored on removable media is the responsibility of the individual who operates the devices Mobile devices and/or removable media that have become damaged should be handed back to Helpdesk to ensure it is disposed of securely to avoid data leakage.

If a member of staff who used a mobile device and removable media was to leave, they should return the devices to Helpdesk for secure destruction and/or redistribution.

When the business purpose has been satisfied the contents of the removable media should be removed from the media through a destruction method that makes recovery of the data impossible. Alternatively the removable media and its data should be destroyed and disposed of beyond its potential reuse.

Marketing

We may contact Data subjects to ask their opinion, offer insight and research into the education sector and tell them about policy, funding and programmes we think are relevant to them. This is what we mean when we talk about 'marketing'.

We ensure that any marketing which the company sends out is directed only at data subjects which have given their direct consent. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build customer trust and engagement, and enhance our reputation.

Our consent request is prominent, concise, separate from other terms and conditions, and easy to understand.

It Includes:

- the name of our organisation;
- the name of any third party controllers who will rely on the consent;
- why **we** want the data and what **we** will do with it;
- that individuals can withdraw consent at any time.

We must ask people to actively opt in and not rely on any pre-ticked boxes. Records are kept to evidence consent – who consented, when, how, and what they were told.

It is easy for people to withdraw consent at any time they choose. Consents are kept under review and are refreshed if anything changes.

Appendix

Appendix 1: Data security rules for staff and associates

- Ensure any computer or mobile device is locked when not in use even if temporarily.
- Log out of any BPN secure system or software (CCMS, SAGE, Outlook, BPN network) when not in use.
- Never share your password to any BPN secure system.
- Personal data should always be stored in a password protected location such as any of the BPN secure systems.
- Personal data should not be stored on the hard-drive of an individual PC or laptop unless it is temporary, essential and password protected.
- When removable media is used to transport personal data, the data on the device must be encrypted.
- Personal data should not be disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.
- Telephone conversations where personal data is disclosed should be conducted in a way or place that avoids third party disclosure.
- Do not disclose special category data to any third party without direct consent by data subject
- If it is essential to send personal data via email, the document must be password protected and the password sent in a separate communication.
- Items that are marked 'personal' or 'private and confidential', or which appear to be of a personal nature, are opened by the addressee only.
- Do not open attachment unless you are sure of the sender.
- Where appropriate, delete data subject details from personal emails once information has been documented in a secure system.
- Any hard-copy personal data should only be kept where essential and should be kept inside a locked pedestal or filing cabinet when not in use.
- All waste paper, which has any personal or confidential information or data on, must be placed in the confidential waster sacks located in each office. Under no circumstances should this type of waste paper be thrown away with normal rubbish in the waste paper bins.
- You should not use the company's contact details for matters that are not work-related.

- Report any breach in data protection either through the loss of device containing personal data or the incorrect processing, storing or sharing of personal data to the data controller, operations manager and IT systems.

Appendix 2: Privacy Notice

Best Practice Network and Outstanding Leaders Partnership provide professional development programmes for individuals working in the education sector in partnership with Schools, Early Years providers, Universities and Colleges. This privacy notice explains how we use any personal data we collect about you, the choices you have about what marketing you want us to send you, and your privacy rights and how the law protects you.

Data protection changed on 25 May 2018

On the 25 May 2018 the General Data Protection Regulation (2016) came into effect, giving you more control over how your data is used and how you're contacted. This notice sets out most of your rights under the new laws. We will update this if any changes to our policies occur.

Our privacy promise

The company needs to keep certain information about its employees, clients, and suppliers for financial and commercial reasons and to enable us to monitor performance, to ensure legal compliance and for health and safety purposes. To comply with the law, your personal data must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. In practice, this means that only those who have a necessary and lawful need to access your data will be able to do so.

Data protection controller

For the purposes of the Data Protection Act (2018) we confirm that the data controller is Best Practice Network Limited, a limited liability company based in England, with its registered office address at Newminster House, 27-29 Baldwin Street, Bristol, BS1 1LT.

We also contract a number of 'data processors' who process or store personal data on behalf of Best Practice Network for example suppliers of IT and other systems. We ensure that our contracts with these processors are compliant with the Data Protection Act (2018) and that your data is kept safe by these companies.

How the law protects you

Best Practice Network understands that we must have a lawful basis in order to process your personal data, as outlined in Article 6 of the GDPR (2016). At least one of these must apply whenever we process your personal data:

- Consent: you have given clear consent for us to process your personal data for a specific purpose.

- Contract: the processing is necessary for a contract we have with you.
- Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).
- Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
- Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party.

What information we collect about you

Depending on our relationship with you, we may use your personal data in a number of ways:

Relationship with BPN	What data we collect about you	What we use your data for	Lawful basis
Staff and Directors	Contact Socio-demographic Financial Contractual and HR Documentary Data Identification number Consents	To manage our relationship with you To ensure we fulfil our obligations as part of our contract with you	Contract Legal basis
Associate	Contact Socio-demographic Financial Contractual and HR Documentary Data Identification number Consents	To manage our relationship with you To contract you for work To ensure we fulfil our obligations as part of our contract with you	Contract Legal basis Consent
Supplier/ Partner Hub	Contact Financial Contractual and HR	To manage our relationship with you	Contract Legal basis
Candidate on one of our programmes	Contact Socio-demographic Financial Identification number Equal opportunities information Consents Programme assessment and evaluation Documentary data	To manage our relationship with you and deliver our services To ensure you receive information about your course To provide you with support and guidance To respond to complaints and queries and aim to effectuate these To collect money for services	Contract Legal basis Consent
Newsletter	Contact	To provide you with insight and information on the education	Consent

Relationship with BPN	What data we collect about you	What we use your data for	Lawful basis
member	Marketing preferences Consents	sector To manage our relationship with you and deliver our services To promote our products and services where applicable	
Website visitor	Technical information	To provide a better user experience To remarket information you may be interested in from our website	Legitimate interest

Categories of personal data

We may collect a number of different categories of personal data from you, which are explained in more detail below:

Types of personal information	Details
Contact	Your contact details and where you live
Socio-demographic	Information about your age, gender, education level, work, type of client and nationality
Financial	Your bank details or payroll and invoicing information
Contractual and HR	Information on your contract with BPN and HR information
Documentary data	Details about you which are stored in a separate format such as CVs, copies of passports and driving licences
Identification number	A number provided to you by the government to identify who you are or a qualification you have obtained such as national insurance number or teacher reference number
Special categories of personal data	Racial or ethnic origin, religious or philosophical beliefs, disability and sexual orientation
Marketing preferences	Details about the products and services you would like to receive from us
Consents	Any agreement to use and process your data, usually in regards to marketing
Programme assessment and evaluation	Work completed as part of your qualification and details of marking, feedback and outcome
Technical information	Information we automatically collect from you when you visit our website which includes traffic data, location data and other communication data

We will only process special categories of personal data where we have sufficient a lawful basis to do so e.g., where the data subject has given explicit consent to the processing of those personal data for one or more specified purposes as outlined in Article 9 of the GDPR (2016).

Who we share your personal information with

We may share your data internally within Best Practice Network and Supporting Education Group where it is necessary for a specific purpose i.e., administrating employment.

There may be some instances where we share your data with third parties such as programme facilitators and assessors, funding or government bodies such as the Department for Education, the Education & Skills Funding Agency and Ofsted, our Data processors and any third parties which require us to share your personal data to fulfil our legal obligations such as auditors.

Please note that if a participant moves schools and continues their training programme, then under DfE requirements we may need to share their name and contact details, participation and progress data with the new school or provider.

Marketing

We may contact you to ask your opinion, offer insight and research into the education sector and tell you about policy, funding and programmes we think are relevant to you. This is what we mean when we talk about 'marketing'.

The personal information we have for you is made up of what you tell us, data we collect when you use our services, or from third parties we work with. We use this information to decide what may be relevant and of interest to you.

We can only use your personal information to send you marketing messages if we have either your consent or a 'legitimate interest'. That is when we have a business or commercial reason to use your information. It must not unfairly go against what is right and best for you.

Whatever you choose, you'll still receive information relating to your existing programmes and services.

We may ask you to confirm or update your choices if you start any new programmes or use our services in future. We will also ask you to do this if there are changes in the law, regulation, or the structure of our business.

If you change your mind you can update your choices at any time by contacting us.

Cookies

We use cookies to temporarily remember your location and device type so we can provide you with a better user experience when visiting our website.

Cookies helps us to use remarketing to show you adverts across different google platforms based on content you searched during past visits to our website. You can opt out of our remarketing campaign by visiting your web browser's Settings page.

How long we keep your personal data

We will keep your personal information for as long as you are a service user or subscriber with Best Practice Network.

After you stop your contract with BPN, we may keep your data for up to 7 years for one of these reasons:

- To respond to any questions or complaints

- To show that we treated you fairly
- To maintain records according to rules that apply to us
- To provide you with a reference for your work with BPN

You can ask to have your data removed earlier by contacting us.

If you make an 'Expression of Interest' or submit an application but do not engage in a contract with Best Practice Network, we are required to delete your personal data after 18 months.

How to get a copy of your personal information

You can request details about the personal data we hold on you by filling in a data request form and sending it to us at Best Practice Network, Newminster House, 27-29 Baldwin St, Bristol, BS1 1LT.

You will be required to make a written request with sufficient information to enable us to identify who you are; we will then supply you with a copy of the personal data held about you within one month. We may charge a 'reasonable fee' where request is manifestly unfounded or excessive.

Letting us know if your personal information is incorrect

You have the right to query the accuracy of any personal data we have about you that you think is incorrect or incomplete. Please contact us if you want to do this. In the event that your personal data changes, please contact us as soon as possible so we can update our records.

If you do, we will take reasonable steps to check its accuracy and update it.

What if you want us to stop using your personal information?

As a data subject you have the right to object to our use of your personal data, or to ask us to remove or stop processing it if there is no need for us to do so. This is known as the 'right to object' and 'right to erasure', also known as the 'right to be forgotten'.

We may sometimes be able to restrict the use of your data. This means that we are permitted to store your personal data, but not process it any further.

You can ask us to restrict the use of your personal information in the following circumstances:

- Where you contest the accuracy of the personal data, we will restrict the processing until you have verified the accuracy of the personal data
- Where you object to the processing
- When processing is unlawful and you opposes erasure and requests restriction instead
- If we no longer need the personal data but you require the data to establish, exercise or defend a legal claim

Please contact us if you want to object to how we use your data, or ask us to delete it or restrict how we process it.

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.

Future formats for sharing data

Data Privacy laws changed on 25 May 2018. You now have the 'right to data portability'.

This means that you can obtain and reuse your personal data for your own purposes across different services. We must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

This service will be free of charge.

How to contact us

For further information on how your information is used, how we maintain the security of your information, and your rights to access information we hold on you, please contact:

- by email: enquiries@bestpracticenet.co.uk
- by telephone: 0117 920 9200
- or write to us at: Best Practice Network, Newminster House, 27-29 Baldwin St, Bristol, BS1 1LT

You also have the right to complain to the Information Commissioner's Office. Find out on their website how to report a concern- <https://ico.org.uk/concerns/>

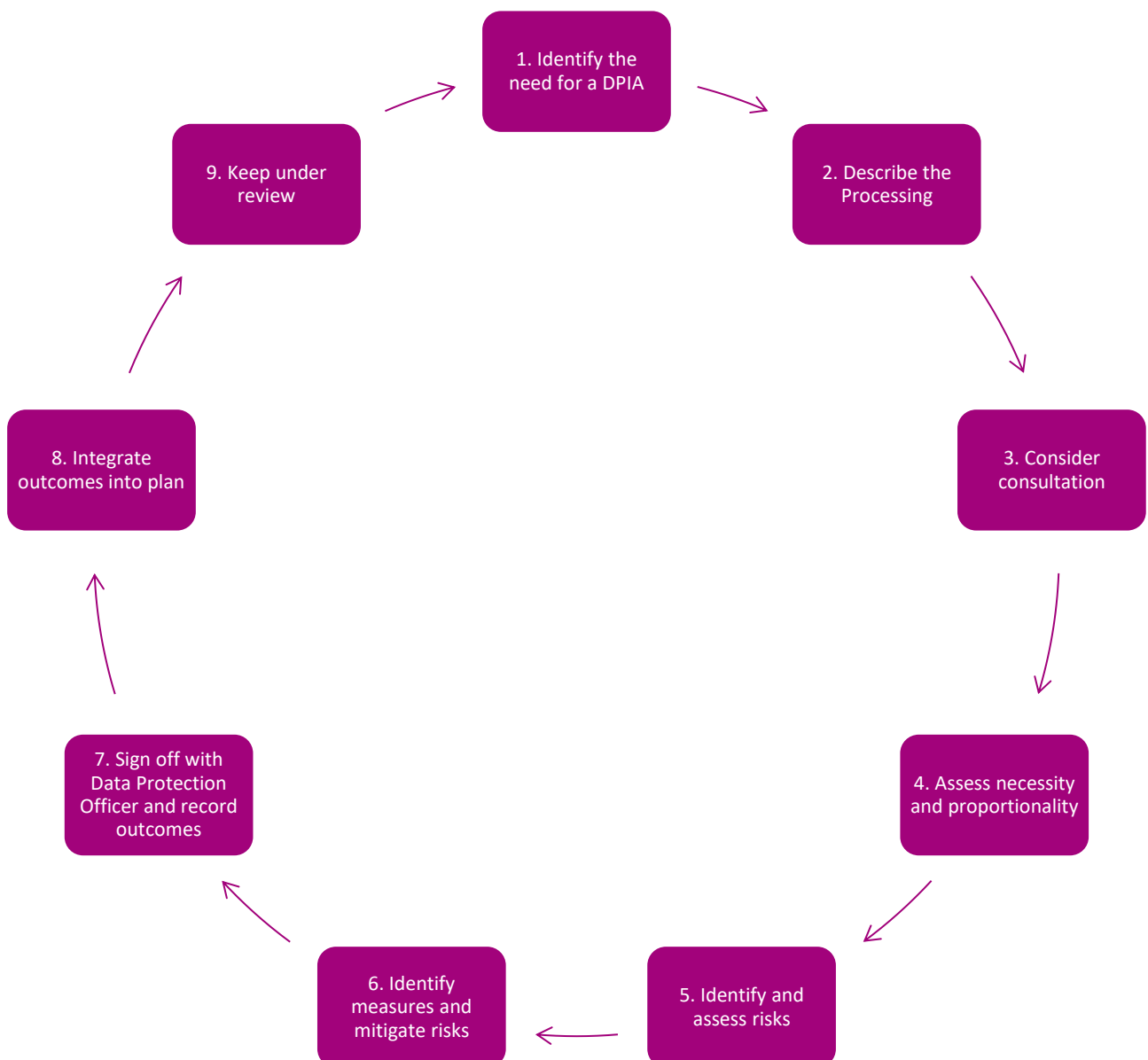
Appendix 3: Personal data processes

Data Protection Impact Assessments (DPIA)

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. An effective DPIA will allow the Company to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

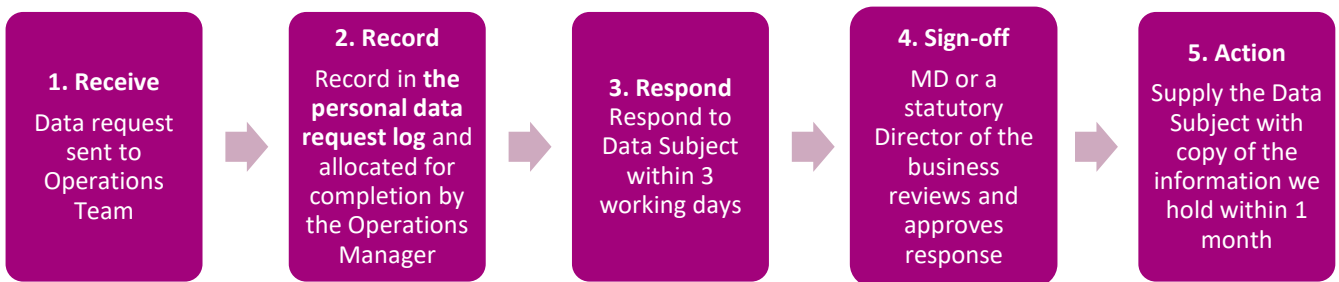
DPIA Framework can be found [here](#), which must be filled out at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process.

How to carry out a DPIA:



For further information visit the [ICO webpage](#) about DPIA.

How to respond to request by Data Subject



When a Data Subject makes a written request with sufficient information to enable the person to be identified, we will supply them with a copy of the information held about them within one month. We may charge a 'reasonable fee' where request is manifestly unfounded or excessive.

Any request by a Data Subject to suppress or object to the processing of personal data or erase personal data should also be documented in the personal data request log and requests dealt with within a month.

Each request will then be dealt with on a case by case basis

How to respond to a personal data breach



If one of our processors detects a personal data breach, the processor must notify us that the breach has taken place and we in turn notify the ICO.

Operations retention policy

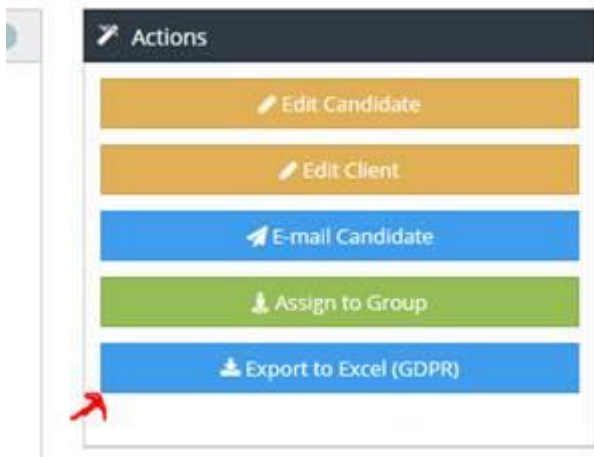
It is imperative that after a candidate completes a programme with us, we retain only the personal data necessary for our legal obligations. In line with this, group administrators must ensure that Canvas profiles and any documents in G drive containing personal data of candidates is removed as per the milestones. Personal data, including documentary data and correspondence, shall only be held on the CCMS.

Where a data subject has made an 'Expression of interest' or submitted an application but not engaged in a contract with Best Practice Network, we are required to delete their personal data after 18 months.

How to action the 'Right to Data Portability'

The 'right to data portability' means that Data Subjects can obtain and reuse their personal data for their own purposes across different services. We must provide the personal data in a structured, commonly used and machine readable form.

An initial export button has been supplied when viewing a candidate (note you have to be logged in as a System Administrator):



This lists their personal details, and then any additional answers given per application (as there could be more than one).

You can then supply the Data Subject with a zip file containing any documentary data and a PDF generated version of their application form and the excel spreadsheet. This must be encrypted and the password provided to the Data Subject via another communication.

Data Protection Registration Certificate

Best Practice Network Ltd

Newminster House
27-29 Baldwin Street
Bristol
BS1 1LT

Registration reference: Z833183X
Date registered: 02 December 2003
Registration expires: 01 December 2023



Issued by: Information Commissioner's Office,
Wycliffe House, Water Lane, Wilmslow, Cheshire
SK9 5AF

Telephone: 0303 123 1113
Website: ico.org.uk