Dorset Pathways UK GDPR and Data Protection Policy

Dorset Pathways Limited, a registered entity with the ICO, is dedicated to upholding individuals' rights and safeguarding personal privacy in accordance with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). This policy outlines the company's commitment to handling personal information securely, whether it is stored electronically or in paper files, and applies to all individuals who handle or have access to personal data.

Policy Objectives:

The Operations Director, acting as the Data Controller at Dorset Pathways, is responsible for adhering to the obligations set forth in the UK GDPR and DPA. The company is dedicated to being transparent, clear, and succinct in its approach to collecting and using personal information. It ensures that individuals whose data is being processed are well-informed about their rights under the relevant legislation. All staff members are required to have a fundamental understanding of the law and its implications on data handling decisions. Compliance with this policy is mandatory for all staff.

Scope of the Policy:

Personal data encompasses any information linked to an identified or identifiable living individual, either directly or indirectly. This includes various aspects of an individual's identity, such as physical, physiological, genetic, mental, economic, cultural, or social factors. The scope of the UK GDPR also extends to personal identifiers like names, identification numbers, location data, or online identifiers.

Dorset Pathways gathers a substantial amount of personal data annually, which includes learner records, staff records, names and addresses of potential candidates, references, and fee collections. These data types align with Dorset Pathways' education and therapeutic business practices. In certain instances, legal requirements might mandate the collection and use of specific information to fulfil obligations to Local Authorities (LAs), government agencies, and other relevant bodies.

The Principles

The principles set out in the EU GDPR and retained under the UK GDPR must be adhered to when processing personal data:
1. Personal data must be processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation) 3. Personal

data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (data minimisation)
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (accuracy).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (storage limitation)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (integrity and confidentiality).

Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Dorset Pathways.
- Processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the data controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller.
- The data subject has given consent to the processing of his or her data for one or more specific purposes.

Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters. Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent. The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles

and include information about both the purposes of the processing and the lawful basis for it in Dorset Pathways's relevant privacy notice. When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside Dorset Pathways's public tasks) a legitimate interests assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted. Sensitive Personal Information Processing of sensitive personal information (known as 'special categories of personal data') is prohibited unless a lawful special condition for processing is identified. Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on the previous page.
- One of the special conditions for processing sensitive personal information applies:

(a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Centre or the data subject
(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
(d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not for-profit body with a political, philosophical, religious or trade-union aim
(e) the processing relates to personal data which are manifestly made public by the data subject
(f) the processing is necessary for the establishment, exercise or defence of legal claims
(g) the processing is necessary for reasons of substantial public interest
(h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or service
(i) the processing is necessary for reasons of public interest in the area of public health.

Dorset Pathways's privacy notice sets out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies. Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it. Where Dorset Pathways cannot rely on another legal basis of processing, explicit consent is usually required for processing sensitive

personal data. Evidence of consent will need to be captured and recorded so that Dorset Pathways can demonstrate compliance with the UK GDPR.

Data Protection Impact Assessments (DPIA)

All data controllers are required to implement 'Privacy by Design' when processing personal data. This means Dorset Pathways processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles. Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented), consideration to Data Protection Impact must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information.

Privacy Notice

Dorset Pathways will issue privacy notices as required, informing data subjects (or their parents, depending on age of the learner, if about learner information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes. When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the UK GDPR including the identity of the DPO, how and why the Centre will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data). When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. Dorset Pathways will also check that the data was collected by the third party in accordance with the UK GDPR and on a basis which is consistent with the proposed processing of the personal data.

Dorset Pathways will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Dorset Pathways will issue a minimum of two privacy notices, one for learner information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.

Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. Personal data must not be used

for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary. Data minimisation Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role. Dorset Pathways will ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required. This includes requiring third parties to delete such data where applicable. Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Individual Rights

Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed (see the relevant privacy notice)
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request (see Appendix 1 - Procedure for Access to Personal Information)
- To have data corrected if it is inaccurate or incomplete
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where Dorset Pathways no longer needs the personal information, but you require the data to establish, exercise or defend a legal claim
- To restrict the processing of personal information temporarily where you do not think it is accurate (and Dorset Pathways is verifying whether it is accurate), or where you have objected to the processing (and Dorset Pathways are considering whether there are legitimate grounds override your interests)
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format
- To withdraw consent to processing at any time (if applicable)
- To request a copy of an agreement under which personal data is transferred outside of the EEA if applicable.
- To object to decisions based solely on automated processing, including profiling

- To be notified of a data breach which is likely to result in high risk to their rights and obligations
- To make a complaint to the ICO or a Court.

Individual Responsibilities

During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. Dorset Pathways expects staff to help meet its data protection obligations to those individuals. If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not Dorset Pathways staff to access personal information if you have specific authority to do so
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with Dorset Pathways policies).

Information Security

Dorset Pathways will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. All staff are responsible for keeping information secure in accordance with the legislation. Dorset Pathways will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks. Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure. Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested. Staff must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows: Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it. Integrity means that personal data is accurate and suitable for the purpose for which it is processed. Availability means that authorised users can access the personal data when they need it for authorised purposes. Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards Dorset Pathways has implemented and maintains in accordance with the UK GDPR and DPA. Where Dorset Pathways uses external organisations to process personal information on its behalf, additional

security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information.

Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of Dorset Pathways
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of Dorset Pathways and under a written Agreement for Services.
- the organisation will assist Dorset Pathways in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to Dorset Pathways as requested at the end of the contract
- the organisation will provide Dorset Pathways with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell Dorset Pathways immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from The Business Finance and Compliance Director.

Storage and retention of personal information

Personal data will be kept securely in accordance with Dorset Pathways's data protection obligations. Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Personal information that is no longer required will be deleted.

Data breaches

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams

- Blagging offences where information is obtained by deceiving the organisation which holds it.

Dorset Pathways must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. Dorset Pathways must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms. Staff should ensure they inform The Business Compliance and Finance Director immediately that a data breach is discovered and make all reasonable efforts to recover the information.

Consequences of a failure to comply

Dorset Pathways takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and Dorset Pathways and may in some circumstances amount to a criminal offence by the individual. Any failure to comply with any part of this policy may lead to disciplinary action under Dorset Pathways procedures and this action may result in dismissal for gross misconduct. If a nonemployee breaches this policy, they may have their contract terminated with immediate effect. If you have any questions or concerns about this policy, you should contact The Business Compliance and Finance Director or the Operations Director.

Review of Policy

This policy will be updated as necessary to reflect best practice or amendments made to the UK GDPR or DPA. The Supervisory Authority in the UK The ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

Appendix 1 – Dorset Pathways Procedure for Access to Personal Information
Right of access to information

There are two distinct rights of access to personal information held by Dorset Pathways. Under the UK GDPR and the Data Protection Act 2018 an individual (e.g. learner, parent or member of staff) has a right to request access to their own personal information. In certain circumstances requests may be made by a parent on behalf of their child (see explanation below). The Education (Pupil Information) (England) Regulations 2005 gives parents the right of access to curricular and educational records relating to their child.
Processing a request
Requests for personal information must be made in writing and addressed to the Business Compliance and Finance Director – Robert Halfhide. If the initial request does not clearly identify the information required, then clarification should be sought. The identity of the requestor must be

verified before the disclosure of any personal information, and checks should also be carried out regarding proof of relationship to the child.
Evidence of identity can be established by requesting production of the following (this list is not exhaustive):
passport / driving licence / utility bills with the current address / Birth or Marriage certificate / P45/P60 / Credit Card or Mortgage statement

Individuals are entitled to be told if we are processing their personal information, obtain a copy of that information and other supplementary information – see below.

In addition to a copy of their personal data, you also have to provide individuals with the following information:

- the purposes for processing their data;
- the categories of personal data concerned;
- the recipients or categories of recipient you disclose the personal data to;
- your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards you provide if you transfer personal data to a third country or international organisation.

Information can be viewed at Dorset Pathways with a member of staff on hand to help and explain matters if requested or provide a face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If the applicant has asked for the information to be posted then special next day delivery or recorded delivery postal service must be used.

Information relating to children

Children possess equivalent rights to access their personal information as adults, including the right to privacy. Although English law doesn't stipulate a specific minimum age, prevailing practice acknowledges that a child who is mature enough to comprehend their rights, particularly those aged 13 and above, is deemed capable of giving consent. However, the absence of a specific age threshold doesn't preclude a valid request from a younger child; each request should be evaluated on an individual basis.

Upon receiving a subject access request from a child, an assessment is necessary to determine if the child comprehends the implications of their request and the subsequent information provided. If the child demonstrates understanding, their request will be processed akin to an adult's. Alternatively, if a parent or legal guardian submits a request on behalf of a child aged 13 and above, compliance will occur only after verifying that the child has authorized the request and that their consent was not coerced or based on misleading information. In cases where a child lacks understanding, a parent or legal guardian's request for the child's information will be honored only if assurances are provided that the request aligns with the child's best interests.

Response time UK GDPR & DPA

The timeframe for addressing a subject access request is 30 days from the date of receipt. This period commences once Dorset Pathways has obtained all essential information required to fulfil the request, such as proof of identity. In situations involving intricate or numerous requests, an extension of up to two additional months might apply. In such cases, it is obligatory to notify the individual of the extension within the initial 30-day timeframe and provide a clear rationale for the necessity of the extension.

Under the Education Regulations, requests from parents for access to information categorized as part of the education record must receive a response within 15 operational days of Dorset Pathways.

Charges

Under UK GDPR & DPA should the information requested be personal information that does not include any information contained within educational records, Dorset Pathways cannot make a charge, unless the request is manifestly unfounded or excessive. You may charge a “reasonable fee” for the administrative costs of complying with the request. Dorset Pathways can also charge a reasonable fee if an individual requests further copies of their data following a request. You must base the fee on the administrative costs of providing further copies. Under the Education Regulations Dorset Pathways may make a charge if the information requested relates to the educational record, the amount charged will depend upon the number of pages provided.
The fees work on a sliding scale basis as below.

Number of pages / Maximum fee

1-19 £1
20-29 £2
30-39 £3
40-49 £4
50-59 £5

60-69 £6
70-79 £7
80-89 £8
90-99 £9
100-149 £10
150-199 £15
200-249 £20
250-299 £25
300-349 £30
350-399 £35
400-449 £40
450-499 £45
500+ £50

Exemptions

There are specific exceptions to the right of subject access that apply under certain circumstances or to particular types of personal data. This necessitates a comprehensive review of all information before disclosure. Here are some of the exemptions that are applicable to Dorset Pathways, although this list is not exhaustive:

Third-Party Information:
When information reveals the identities of others, it may be necessary to edit or remove such details to protect the privacy of third parties. Consent from these individuals should be sought before disclosure, unless they have agreed to it. Reasonable efforts must be made to obtain third-party consent. In cases where consent cannot be obtained, disclosure might still be warranted if the information is crucial to the data subject. Dorset Pathways must still adhere to the one-month statutory timeframe. In cases of redaction, a complete copy of the provided information should be retained to explain redactions if needed. Any codes or technical terms should be clarified, and unclear or illegible information should be re-typed.

Information Likely to Cause Harm:
Information that could cause serious harm to the physical, mental, or emotional well-being of a student or another individual should not be disclosed. Similarly, information indicating that a child is at risk of abuse or related to court proceedings should also be withheld.

Crime and Disorder:
Information that, if disclosed, might impede the prevention, detection, or prosecution of a crime, or the assessment or collection of taxes or duties, should not be disclosed.

Legal Professional Privilege:

Information involving general legal advice or advice linked to anticipated or ongoing legal proceedings is protected under 'legal professional privilege.' Disclosure of any communication between a legal advisor and another person, including the data subject, should not occur without consultation with the relevant legal advisor.

References:
The right of access does not extend to confidential references given or to be given.

Absence of Valid Consent:
If the data subject lacks the capacity to comprehend the nature and implications of the access request, or if there are suspicions of duress, misleading information, or invalid consent obtained by a representative, access should be denied.

Complaints:

Complaints concerning the outlined procedures can be directed to the Data Protection Officer (DPO), Robert Halfhide. The DPO will assess whether the complaint should follow Dorset Pathway's Complaints Procedure. Matters not suitable for the Complaints Procedure can be addressed by the Information Commissioner. Contact details for both will be provided alongside the disclosure information.

Contacts
Further advice and information can be obtained from the Information Commissioner's Office: www.ico.gov.uk

Dorset Pathways's Data Protection Officer is Mr Rob Halfhide and he can be contacted on office@dorsetpathways.co.uk

Authored by Directors Last Reviewed : August 2023 Next Review : August 2024