

Bedlinog Community Primary School

AND

THE PLACE2Be

DATA DISCLOSURE AGREEMENT TO ENABLE PLACE2Be TO PROVIDE A COUNSELLING SERVICE TO THE PUPILS OF THE SCHOOL

Contents

Contents

Clause:	Page:
	Error!
	Boo
	km
	ark
1. Party to the Agreement	not
	defi
	ned
	.
	Error!
	Boo
	km
	ark
2. Introduction	not
	defi
	ned
	.
	Error!
	Boo
	km
	ark
3. Purpose of Disclosure	not
	defi
	ned

4.	Lawful Basis	3	.
			Error!
			Boo
			km
5.	Data to be Disclosed		ark
			not
			defi
			ned
			.
6.	Information Security	4	
7.	Detail of Disclosure	5	
8.	Data Subjects Rights	5	
9.	Review	6	
10.	Agreement Signature	7	
11.	Glossary of Terms	8	

1. PARTIES TO THE AGREEMENT

1.1 The personal data is disclosed by:

Bedlinog Community Primary School, of Hylton Terrace, Bedlinog, Treharris, CF46 6RE, with Data Protection Registration Number Z7332104 (the School)

The personal data is disclosed to:

The Place2Be, of 175 St. John Street, Clerkenwell, London, EC1V 4LW, with Data Protection Registration Number Z5326927 (the Company)

Together known as the Parties.

- 1.2 Parties to this agreement understand that they are each responsible for compliance with the Data Protection Legislation. The Receiving Party will be responsible for the Relevant Data transferred under the terms of this Agreement.
- 1.3 In line with the requirements of Data Protection Legislation, the Parties will ensure data subjects are informed of how their personal data will be used. All Parties will ensure that a privacy notice is available to the pupils and their parents and is shared with them as soon as possible.
- 1.4 The Parties will regularly monitor and review the use of this Data Disclosure Agreement (DDA) to ensure data is disclosed effectively and appropriately.

2. INTRODUCTION

- 2.1 The purpose of this disclosure is to ensure the Relevant Data relating to the pupils who will be receiving the Services provided by the Company, is supplied by the School in a safe and lawful format, prior the commencement of the Services.
- 2.2 This DDA has been written in accordance with the principles contained within the General Data Protection Regulation and provisions of the Data Protection Act 2018.
- 2.3 This DDA is intended to help the Parties understand what data can be disclosed for the stated purpose. It also provides assurance that the Parties have considered the requirements of the Data Protection Legislation.
- 2.4 The Parties understand that they will each be data controllers and the Receiving Party will assume all responsibility of the Relevant Data disclosed under the terms of this DDA.

3. PURPOSE OF DISCLOSURE

- 2.2 This DDA has been set up to facilitate the sharing of the pupils personal data.
- 2.3 The Company is responsible for providing a mental health support service to the School. The School will obtain the consent of the parents before the children referred to the Companies Mental Health

Professional. Disclosure of the Relevant Data will enable to Company to register the pupil into the service.

- 2.4 The Relevant Data will be used in order to put in place appropriate safeguards before the commencement of the service.

4. LAWFUL BASIS

- 4.1 For the purpose of the Data Disclosure Agreement, the lawful bases for processing are as follows:

GENERAL PROCESSING (as defined by the General Data Protection Regulation and the Data Protection Act 2018)
Article 6 (1)(a) – the School will obtain parental consent prior to the pupil being referred into the Service.
If processing involves special categories of data, Article 9(2)(a) will be relied upon. The School will obtain the explicit consent from parents.

5. DATA TO BE DISCLOSED

- 5.1 Details of the categories of personal data that will be disclosed:

- a. Personal descriptors:
Which includes title, name including middle, last and previous names, other names such as nicknames or alias', address, contact telephone numbers, email address, age, date of birth, gender.
- b. Identification numbers:
Including project reference numbers.
- c. Education details:
This includes education status, the form of education (which includes home schooled, mainstream school), additional learning needs (ALN) information.
- d. Lifestyle data:
This information relates specifically to the children's character, personal characteristics, and cultural information. This also includes home and family information for example if they are receiving support from social services.
- e. Health data:
This relates to the physical or mental health of an individual. This includes disabilities, family or individual health history, dental and medical health records, blood type, prescriptions, assessments of needs, hospital admissions including the length of your stay. Care needs including whether an individual is receiving care, they type of care or if they are a registered carer.

5.2 The School will not be responsible for any data that is collected by the Company. The Company will be required to ensure they have satisfied all of the appropriate GDPR provisions for the processing of that personal data.

5.3 Parties to this agreement will ensure that all data disclosed or collected is adequate, relevant, accurate, and up to date and limited to what is necessary to meet the stated purpose.

6. INFORMATION SECURITY

6.1 Parties to this agreement will ensure that individual access to the data is limited to those who have a legitimate purpose to view, use or otherwise access it. Appropriate measures will be taken to ensure that the confidentiality of the data is maintained at all times.

6.2 Parties to this agreement must have an appropriate and adequate security framework.

6.3 The Parties shall comply at all times with the requirements of the Data Protection Legislation and shall perform its obligations under this Agreement in such a way as to ensure that the disclosing Party does not or is not likely to breach any of its obligations under the Data Protection Legislation.

6.4 The receiving Party shall ensure that the Relevant Data is kept secure and shall comply with the Security Measures and use all reasonable security practices and systems applicable to prevent, and take prompt and proper remedial action against, unauthorised access, copying, modification, storage, reproduction, display or distribution of the Relevant Data.

6.5 Practitioners carrying out the functions outlined in this DDA should make themselves aware of, and adhere to, their organisation's data protection, confidentiality and information security policies and procedures.

6.6 All Parties must ensure that adequate and appropriate training on the subjects of data protection, confidentiality and information security is provided to all staff with access to personal data.

6.7 If for any reason, the receiving Party uses the Relevant Data for any purpose other than the purpose stated in Clause 3 they must ensure that all provisions of the Data Protection Legislation are considered. The disclosing Party will not be responsible for any non-compliance of the Data Protection Legislation by the receiving Party.

7. DETAIL OF DISCLOSURE

Description	Detail
Source of Data	Data will be obtained from parents of the children participating in the residential and from the School's internal IT systems such as SIM's.
Methods of Transfer	The data will be transferred to the company using secure email or via a recorded delivery service.
Destination of Data	The data will be provided to the Company which is based in South Wales.
Frequency	The data will be sent by the time agreed by the Parties.

Retention period	The Parties will ensure the data is retained in accordance with their retention schedules which will vary depending on the purpose of the data collected.
------------------	---

8. DATA SUBJECTS RIGHTS

- 8.1 Data protection legislation provides various individual rights for data subjects. Advice on how these rights should be met should be sought from each organisation's Information Governance representative, Data Protection Officer or equivalent. Specific guidance on these rights is available on the Information Commissioner's website; www.ico.org.uk
- 8.2 Parties should ensure that data subjects are informed how and why their personal information will be processed and who it is shared with (the Right to be Informed).
- 8.3 Parties will ensure that all information is clear and particular care taken where working with young people, as there are additional requirements to consider.
- 8.4 All Parties will have in place the appropriate policies and procedures to uphold the confidentiality, integrity and availability of personal information with specific reference to the retention, storage and disposal of records.
- 8.5 Parties will deal with requests for the information referenced in this DDA in accordance with each organisation's relevant policies and procedures.
- 8.6 Each Party will put in place a formal procedure through which data subjects, Party organisations and practitioners can direct any complaints regarding the data disclosed documented in this DDA.
- 8.7 There is an expectation that the organisations involved in this DDA will work together to keep each other informed of any complaints or requests for information received from data subjects or third parties. The organisations will also keep each other informed of any problems, amendments or requests for erasure associated documented in this DDA and there is an expectation that they will collaborate to develop and improve these practices.


9. REVIEW

- 9.1 Where applicable this agreement will be reviewed annually or sooner, if appropriate.

10. AGREEMENT SIGNATURE

SIGNATURES TO THE DATA DISCLOSURE AGREEMENT

SCHOOL - AUTHORISED SIGNATORY

Name Lisa Richards
Designation Data Protection Officer
Signed 
Dated 22nd July 2020

COMPANY - AUTHORISED SIGNATORY

Name
Designation
Signed
Dated

11. GLOSSARY OF TERMS

Term	Definition
Data Protection Act 2018	The UK's third generation of data protection law replaces the previous Data Protection Act 1998. The 2018 Act accepts the standards and obligations set by GDPR and, where GDPR allows, makes specific provisions relevant to the UK.
Data Protection Legislation	<p>The General Data Protection Regulation ((EU) 2016/679) (GDPR) unless or until it is no longer directly applicable in the UK.</p> <p>The Data Protection Act 2018</p> <p>The applied GDPR and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then any successor legislation to the GDPR or the Data Protection Act 2018.</p> <p>The Regulation of Investigatory Powers Act 2000</p> <p>The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)</p> <p>The Electronic Communications Data Protection Directive (2002/58/EC)</p> <p>The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003)</p> <p>All other applicable laws and regulations relating to the processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner or any other supervisory authority, and the equivalent of any of the foregoing in any relevant jurisdiction.</p>
Data Protection Officer	Certain categories of organisation, including any public body or authority (except courts in their judicial capacity) are required to designate a suitably qualified Data Protection Officer (DPO). The tasks of the DPO are set out in Article 39 of GDPR.
Data subject	A 'data subject' is an identified or identifiable natural person. For the purposes of this Agreement, the Parties have referred to the data subjects as young people or students.
Disclosing Party	The Party that is disclosing personal data to the other Party.
GDPR	The General Data Protection Regulation (GDPR) lays down laws relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

Personal data	Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal identifiers	A set of basic personal details that allow Party organisations to identify a data subject.
Personal information	Includes information falling within the definition of 'personal data'.
Practitioner	An inclusive term that refers to those involved in the care, education, welfare of data subjects; i.e. those who provide the service.
Processing personal data	'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.' (GDPR Art 4(2))
Receiving Party	The Party that has received the personal data from the other Party.
Relevant Data:	The data that is transferred under the terms of this DDA that includes any data or information, in whatever form, which will include the personal data detailed in Clause 5 of this Agreement.
Services:	The services that will be provided to the School by the Company in accordance with the Letter of Agreement.
Special categories of data / sensitive data	Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. (GDPR Art 9(1))
Security Measures	appropriate security, technical and organisational measures which may include pseudonymising and encrypting personal data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to personal data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it.