COMPANY NUMBER 10385941

Data Protection Policy

September 2024

Headquarters: Moor House Adventure Centre; Rainton Gate, West Rainton, Houghton le Spring, Tyne & Wear. DH4 6QY.

Tel: 01915841703 (Opt. 5) Mob: 07792834117 Email: abworld365@gmail.com Web: www.worlds.org.uk

Contents

Introduction

The Data Protection Policy sets out the Company's approach to handling personal information in all activities and decisions of World Alternative Education (hereinafter referred to as 'World') in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

The GDPR sets out a number of standards and rules and places obligations on those who process personal information while giving rights to those who are the subject of the data. Personal information covers both facts and opinions about the individuals. The rules and procedures cover the collection and use of information; the quality and security of the information; and the rights of individuals regarding the information about themselves.

The policy sets out a framework for understanding the requirements under the legislation. At the same time, it provides an overview of the main obligations for officers and Members in dealing with personal information so they can comply with the Regulations and the six data protection principles.

Statement of Policy

World collects and uses information about people with whom it works to operate and carry out its functions. In some cases, world is required by law to collect and use information to comply with central government requirements.

World is committed through its policy, procedures and guidelines to ensure that it will:
• comply with both the law and good practice
• respect individuals' rights
• be open and honest with individuals whose data is held
• provide training and support for staff who handle personal data, so that they can act confidently and consistently

At the heart of the Regulations is the need to protect personal information otherwise known as personal data and special category personal data. Special categories of personal data include data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union memberships; health; sex life or sexual orientation; genetic or biometric data uniquely identifying a natural person.

What this means is when World collects and uses personal information, it must handle it and deal with it according to the six principles of data protection.

The Six Principles of Data Protection

If World or any individual follows these six principles, they will be acting in accordance with the Regulations. The principles set the framework for the legitimate reasons for which an organisation may process or use personal information. These principles are legally enforceable which means that if you have not processed personal information in accordance with them, you and World can be considered in breach of the GDPR.

The following six principles form the basis of the GDPR:

1) Lawfulness, fairness and transparency Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject

2) Purpose limitation Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes

3) Data minimisation Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4) Accuracy Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5) Storage limitation Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

6) Integrity and confidentiality Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

The principles come with an additional responsibility as World must be able to demonstrate compliance with these principles. World must demonstrate how it is Accountable. It will do this through the policies and procedures it has to meet the Act's principles and requirements. World is required by the Act to demonstrate that it complies with these principles. Generally, this is understood as the responsibility to demonstrate Accountability.

Scope

The policy covers all data that falls within the definition of personal data under the GDPR.

Personal data means data which relate to a living individual who can be identified: a) from those data, or b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The policy applies equally to full time and part time employees on a substantive or fixed- term contract and to associated individuals who work for World including agency staff, contractors and others employed under a contract of service. The policy also applies to Members in their role as a Member of World.

The policy covers all personal information that World holds in either electronic or paper format or file system and applies throughout the life cycle of the information from the time it is created or arrives within World to the time it is either destroyed or preserved permanently.

Roles & Responsibilities

Staff

In line with World's code of conduct, all employees have a responsibility to protect confidential information. The policy applies to all staff.

Management Team (MT)

The Management Team has overall responsibility for ensuring that World, as a data controller under the GDPR, and its staff complies with World's legal obligations regarding the handling of personal information.

By demonstrating World's commitment to accountability and promoting good governance, MT have the lead role in developing a data protection culture within World.

Development of Service and Corporate Procedures

From this policy, additional procedures and guidance notes will be developed. Each service must consider what specific guidance it may need to have in place to meet the data protection principles. The following areas cover the day-to-day work when dealing with personal information under the GDPR:

- How we use personal information
- Privacy notices
- Information Rights
- Data Protection Impact Assessments (DPIA)
- How we store it
- How we keep it confidential
- How we keep it secure
- How we respond to subject access requests
- How we keep it up to date
- How we share it

Please be aware that there will technical areas within the GDPR that are not relevant to the day to day work. If an issue, not covered in the relevant policy or procedure arises please contact the Management Team for advice and assistance.

How to Process or Use Personal Data

The GDPR has a very broad definition of processing data. Almost everything World does with information, such as when it: obtains, holds, files, organises, transmits, retrieves, disseminates, discloses or destroys data, is processing information. Before we begin to use personal information, we have to provide a privacy notice that explains amongst other things what we are going to do with the information and the legal powers to use the information. In addition, we have to explain the legal rights available to the person.

As mentioned earlier, officers and Members have to comply with the data protection principles when they use personal information. Even though all the principles are equally important, you need to keep in mind that when you use personal information it is done fairly, lawfully, and transparently. (Principle 1).

This means for personal information it must have at least one condition for processing. For special category data you need at least one condition for processing and must have one from the second schedule. See Appendix 1.

Before we can use someone's personal information we have to give them a privacy notice. Whether we collect the personal information directly or we get it indirectly, another organisation gives it to us, we have to provide the person a privacy notice.

Information Rights

When we use a person's personal information, we have to let them know about their information rights. When they want to exercise those rights, we must have a procedure in place to deal with them. In some cases, the rights are limited by World's responsibilities so they require us to exercise judgments when dealing with them or refusing them.

The information rights are:

The right to be informed in this right, the organisation has to inform the person about what is being collected and how it will be used. This is mainly met through the privacy notice.

The right of access when asked, World has to provide a person with access to their personal information. This is commonly called the subject access request (SAR) process.

The right to rectification Here the person can ask for their personal information to be corrected or changed such as if we have the wrong address. In some cases, this can be quite complex and controversial as there are limits on what can be changed.

The right to erasure This right is also known as the right to be forgotten where a person can ask for some of their personal information to be deleted. However, there are limits to what can be erased as it is limited by World's legal responsibilities.

The right to restrict processing with this right, the person can ask that we stop or restrict processing of their personal information. World has to demonstrate why it needs to continue to process the personal information and the consequences from stopping or restricting the use of the personal information.

The right to data portability in certain circumstances, where we process a person's information under consent or a contract, and we use an automated process where no person is involved, we have to make the information available so they can transfer to another organisation.

The right to object the person has the right to object to any processing we do. It is for World to show why the processing is necessary. Where this is mainly available is when we use personal information based on consent such as marketing or doing a task in the public interest. In the latter situation, we have to justify why we need use the information.

Rights in relation to automated decision making and profiling Like the right to data portability, this is based on automated systems where no person is involved. As such, this right is going to be applied rarely as World does not use automated systems.

Data Protection Impact Assessments

In certain circumstance, especially if we are using a new technology, we have to conduct a data protection impact assessment (DPIA). This is a process to identify and minimise the data protection risks of a project.

The DPIAs are mandatory for process that involves a high risk to individuals' interests such as; a systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences; systematic monitoring of a publicly accessible area on a large scale.

At a minimum, a DPIA must describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks.

When a DPIA is needed, the Data Protection Officer (DPO) has be to consulted and should sign it off because of the high risk both in terms of the likelihood and severity of any impact on individuals.

The Duty of Confidence

Confidentiality applies to a much wider range of information than Data Protection. There are three elements to be considered for something to be confidential;

- the information itself must have the necessary quality of confidence;
- the information must have been imparted in circumstances that oblige confidence;
- disclosure must harm the party communicating it.

Some of the things that are likely to be confidential, but may well not be subject to Data Protection, include information;

- about the organisation (and its plans or finances, for example);
- about other organisations, since Data Protection only applies to information about individuals;
- which is not recorded, either on paper or electronically

How to Keep Personal Information Secure

Security is more than a Data Protection issue because it covers the wider security of all Company facilities. There are direct linkages with the information security policy within ICT as it relates to all Company facilities and systems.

World is required to take all reasonable measures to ensure the personal information is held securely (Principle 7). To meet the principle, security in some instances may involve encrypted and password protected devices or files. In other instances, it may require paper files to be kept in locked cabinets. As a basic rule of thumb, personal information should not be left on an unattended desk or overnight.

When Members, employees and others acting on behalf of World access or use personal data, they must only have access or use personal data that are necessary to carry out their duties and responsibilities.

Further procedures on keeping personal information secure will be provided on the intranet and staff are reminded to check the ICT information security policy for further information relating to wider information security questions.

What to do about a data breach?

On occasion, personal data may be lost, stolen, or compromised. When this happens, it is important to notify the designated officers as set out in the Data Breach Policy as qualifying breaches have to be reported to the ICO within 72 hours. A qualifying breach is one where there is a high risk to a person or persons about the consequences from the breach. If we can demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, then we don't need to report it.

To put it briefly, World has to show the reasons for not reporting a data breach.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay.

When we have to notify the ICO of a breach, we have to tell them the following:

• describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; • communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; • describe the likely consequences of the personal data breach; • describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The Policy will state the procedure to be followed in order to:

• find out what data has been lost;
• mitigate the loss;
• contact the people whose data was lost;
• if serious, notify the Information Commissioner's Office.

A data breach is any incident involving the loss of personal information that could lead to identity fraud or have other serious significant impact on individuals. A data breach includes both electronic media and paper records; it can also mean inappropriate access to information.

What to do if Someone Requests Their Personal Information
- Subject Access Request (SAR)

One of the main data protection rights is for an individual to be able to obtain a copy of any of their personal information held by an organisation. When someone requests his or her own information, this is called a Subject Access Request (SAR). World has to provide the information within 30 calendar days. Although there are some exceptions to this right, it is rare that these exceptions are used.

When a request is made formally to World for personal information it is usually done through the online form on the 'Accessing your personal data' page or within one of the service specific requests for access to care records. Both the Children and Young Peoples' Service and Adults and Health Service have specific processes by which people in care may request their personal information. However, a person may request their personal information in the normal course of business so officers need to be alert to these types of requests.

If you are in doubt, please contact the Management Team who can advise you on the appropriate response.

Data Quality

What we do to keep personal information accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. As a company we recognise the importance of having good quality data and the same applies for personal data.

A Data Quality Policy has been developed and approved. The policy defines data quality in terms of accuracy, validity, reliability, timeliness, relevance and completeness. When we collect and use personal data we should strive for the same principles.

- Accuracy means that performance data is presented in an accurate, clear, consistent and unbiased manner.

- Validity ensures data is recorded and used in compliance with relevant requirements i.e. the protection of information from unauthorised access or revision to ensure that the information is not compromised through corruption or falsification.

- Reliability means the data must be in an agreed format which conforms to recognised national standards.

- Timeliness ensures that data is available when it is needed as the collection of up to date information is essential to the effective and efficient operation of our processes.

- Relevance means that every effort should be made to ensure that recorded data is appropriate for the purposes for which it is used.

- Completeness ensures that data requirements meet the needs of the organisation and that the data collection processes match these requirements.

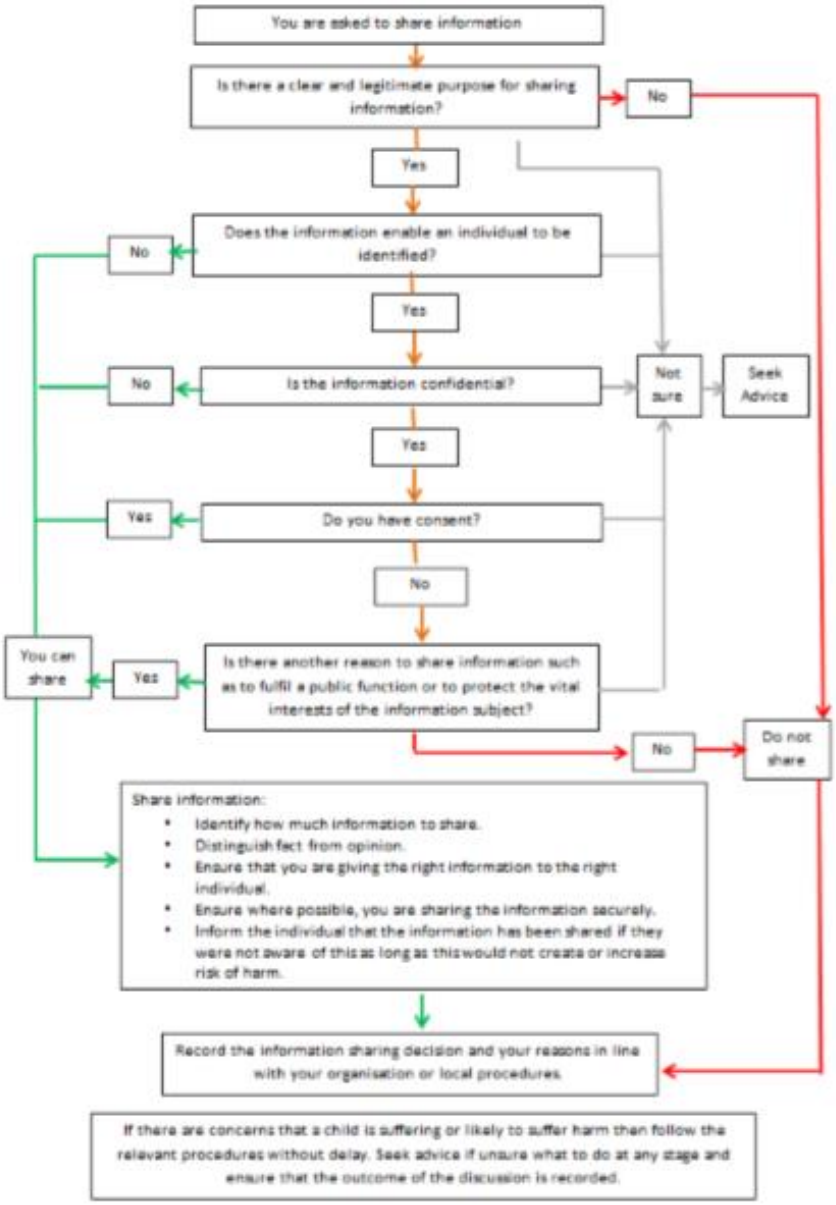
Sharing Personal Information

What to do if you want to share personal information with a partner organisation

Information sharing is key to World's ability to deliver effective and efficient public services that are coordinated around the needs of the individual. It is essential to enable early intervention and preventative work and in some cases for safeguarding, promoting welfare and for wider public protection. This sharing can be with a service level agreement or statutory sharing with other public authorities and agencies.

At the same time, World is aware that the public want to be confident that their personal information is kept safe and secure. Company officers have to maintain a balance between preserving the privacy of the individual and sharing information when appropriate.

The flow chart below provides additional information on how to share data:



S29 and S35 of the Data Protection Act

Sections 29 and 35 of the Data Protection Act enable other organisations, e.g. Police, DWP, HMRC to request information relevant to crime prevention and detection of mental legal proceedings. These requests are processed by the Management Team working with relevant DCC services on the responses.

See the guidance note regarding this type of disclosure at http://intranet.durham.gov.uk/Pages/ThinkPrivacy.aspx

If you are in any doubt whether you can share information or disclose it to a third party, please contact the Management Team.

Training & Awareness

All staff and Company employees will need to be aware of World's Data Protection Policy. To help staff understand the basic principles within this policy an awareness guide is available. For some posts within World, additional training and guidance will be required. Those posts will be identified through their work and any additional training and guidance will need to be discussed with the line manager in the first instance.

Enforcement

Significant intentional breaches of this Policy will be handled under World's disciplinary procedures. If criminal activity is in evidence, then the police will be informed.

The GDPR removes the corporate protection of individual employees or agents from prosecution should they breach the conditions imposed by the Regulations. This means that staff are individually responsible for compliance with the provisions of the Regulations. The unauthorised accessing or processing of personal data is a criminal offence.

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. The company is registered as such. The General Data Protection Regulations require every data controller to notify and renew their notification on an annual basis. Failure to do so is a criminal offence.

Equality & Diversity

The Company is committed to promoting equality of opportunity, valuing diversity and ensuring discrimination, harassment or victimisation is not tolerated. Our policy is to treat people fairly, with respect and dignity. We also comply with legal requirements in relation to age, disability, gender, pregnancy and maternity, marriage and civil partnership, gender reassignment, race, religion or belief and sexual orientation.

Contacts

Further guidance is available on the Intranet at http://intranet.durham.gov.uk/Pages/ThinkPrivacy.aspx
You can contact the Management Team: Email: abworld365@gmail.com and Telephone: 07792834117

References

- Data Protection Act 2018
- General Data Protection Regulations
- Personal Information Security Policy
- Data Protection Policy Breach Procedure
- Subject Access Request procedure
- Your Information, Your rights
- Guidance on S29 and S35
- Secure Handling and Transit Guidance
- Multi Agency Information Sharing Protocol County Durham, Tees Valley and North Yorkshire
- Secure Handling and Transit Guidance
- Retention and Destruction Policy
- Corporate Records Management Policy

Appendix 1 Lawful basis for processing data

Lawful Basis (Article 6) a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; c) processing is necessary for compliance with a legal obligation to which the controller is subject; d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such

interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Special Category Data

When we use special category data we must have at least one of the conditions set out below. If we don't have one, we cannot use the special category data. We must stop using the data and delete it. Special category data is any personal information that is one or more of these eight categories.

a) Racial or ethnic origin
b) Political opinions
c) Religious or philosophical beliefs
d) Trade union membership
e) Genetic data (new)
f) Biometric data (new)
g) Health Data

Policy Review

This policy will be reviewed annually or in light of any changes in legislation and/or guidance.

This policy document will be reviewed in September 2025.

Signed by:

Martin Coy (General Manager)

MCoy