



## TRIPLE P UK LIMITED

### Information Governance & Data Security and Protection Policies

**Version No: 1**

The purpose of the Triple P UK Information Governance and Data Security and Protection Policies document is to clearly set out in one place, Triple P UK’s policies for Information Governance and Data Protection, clearly setting out all Triple P UK employee responsibilities and the possible consequences of not following the policies and associated guidance.

<b>Document type</b>	Information Governance & Data Security and Protection Policies
<b>Date approved</b>	20/02/2020
<b>Date implemented</b>	20/02/2020
<b>Next review date</b>	<b>July 2021</b> or sooner should legislative change require.
<b>Policy author</b>	TPG Information Governance (IG) Team
<b>Applies to</b>	All Triple P UK Personnel  <b>Please Note:</b> This Policy also applies to all TPI Personnel who process personal data/information on Triple P UK’s behalf, as a result of Triple P UK outsourcing various business functions and tasks to the TPG head office. In those circumstances, references in this document to Triple P UK should be taken to be references to TPI.

**NB Personal Data has been redacted in this version.**

The local version of this document is the only version that is maintained. Any printed copies should therefore be viewed as “uncontrolled”, as they may not contain the latest updates and amendments. For the avoidance of doubt please see Triple P UKs Information Governance Lead.

## 1. GLOSSARY OF TERMS

Term	Acronym	Meaning
Anonymisation	-	The process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.
Data Controller	-	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	-	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Act 1998	DPA 1998	An Act for the regulation of the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information
Data Protection Act 2018	DPA18	Act replaced DPA 1998 above
Data Protection Impact Assessment	DPIA	A method of identifying and addressing privacy risks in compliance with GDPR requirements.
Data Protection Officer	DPO	A role with responsibility for enabling compliance with data protection legislation and playing a key role in fostering a data protection culture and helps implement essential elements of data protection legislation
Data Security and Protection Toolkit	DSP Toolkit	From April 2018, the DSP Toolkit will replace the Information Governance (IG) Toolkit as the standard for cyber and data security for healthcare organisations
Freedom of Information Act 2000	FOIA	The Freedom of Information Act 2000 provides public access to information held by public authorities
General Data Protection Regulation	GDPR	The General Data Protection Regulation (EU) 2016/679

Information Commissioner's Office	ICO	The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Personal Data	-	Means information that relates to an individual who can be identified either directly or indirectly
Pseudonymisation	-	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Subject Access Request	SAR	A subject access request (SAR) is a written request made by or on behalf of an individual for the information which he or she is entitled to ask for under the Data Protection Act.
Triple P Group	TPG	Means the group of companies comprising TPI and its related bodies corporate, including Triple P UK.
Triple P International Pty Ltd	TPI	Means the Australian company, Triple P International Pty Ltd, (ABN 17 079 825 817)) and whose registered office is at Level 1, 22 Wandoo Street, Fortitude Valley, Qld 4006 but who carries on business at 11 Market Street North, Indooroopilly, Queensland, 4068, Australia.
Triple P UK Limited	Triple P UK	Means the British company, Triple P UK Limited, company number SC222936 and whose registered office is at 6 St Colme Street, Edinburgh EH3 6AD, United Kingdom.

## 2. Table of Contents

Information Governance Policy .....	4
Data Protection Policy.....	14
Data Quality Policy .....	18
Records Management Policy.....	21
Access to Information Policy (Subject Access Requests - SAR).....	29
Freedom of Information (FOI) Policy .....	33
Network and IT Security Policies .....	36
Data Security Policy.....	46
Sharing Data with Third Parties Policy.....	51



## TRIPLE P UK LIMITED

### Information Governance Policy

**Version No: 1**

The purpose of the Triple P UK Information Governance Policy is to provide an overview of Triple P UK’s approach to information governance, including data protection and other related matters. This policy details the various roles and responsibilities within Triple P UK and the wider Triple P Group, with respect to data security and data protection. It aims to ensure that all Triple P UK employees understand how to take care of the information they need to do their jobs, and to protect this information on behalf of the data subjects.

<b>Document type</b>	Information Governance Policy
<b>Date approved</b>	20/02/2020
<b>Date implemented</b>	20/02/2020
<b>Next review date</b>	<b>July 2021</b> or sooner should legislative change require.
<b>Policy author</b>	TPG Information Governance (IG) Team
<b>Applies to</b>	All Triple P UK Personnel  <b>Please Note:</b> This Policy also applies to all TPI Personnel who process personal data/information on Triple P UK’s behalf, as a result of Triple P UK outsourcing various business functions and tasks to the TPG head office. In those circumstances, references in this document to Triple P UK should be taken to be references to TPI.

The local version of this document is the only version that is maintained. Any printed copies should therefore be viewed as “uncontrolled”, as they may not contain the latest updates and amendments. For the avoidance of doubt please see Triple P UKs Information Governance Lead.

## **1. INTRODUCTION**

Triple P UK recognises that information is an important asset to its business and as such, there is a need to have robust arrangements in place for Information Governance (IG). Triple P UK also recognises the importance of the IG arrangements being regularly reviewed. It notes the importance of ensuring that information is effectively managed, including through having appropriate policies and procedures in place and clearly identifying management accountability and structures in order to provide a robust governance framework for the entire group. The policies and procedures will assist Triple P UK employees to deal with personal information efficiently, securely and in compliance with relevant data protection laws. This in turn, will enable Triple P UK to provide the best service to the practitioners, organisations and families it works with, by ensuring their personal information is handled appropriately.

The Triple P Group's Executive Team have endorsed the organisation's commitment to data protection and privacy and to handling information in accordance with an identified framework. This commitment is demonstrated through relevant policies, procedures, guidance and training offered to its staff and information offered to its clients and the public.

## **2. THE PRINCIPLES OF DATA PROCESSING (GDPR/ DPA18)**

The GDPR and the DPA18 form the legislative framework for data protection in the UK. They are underpinned by a set of data protection principles.

### **2.1. Lawful, fair and transparent processing**

*Personal Data shall be processed lawfully, fairly and in a transparent manner.*

Triple P UK must be transparent about its collection and use of the personal data of individuals (data subjects). When Triple P UK collects personal data, it must provide the data subject with clear information including why their personal data is collected and how Triple P UK will use the data. Triple P UK provides general information in its Privacy Policy which is published on its website. It also provides data subjects with specific information through Privacy Notices. Triple P UK must also, when requested, provide data subjects with information regarding the processing of their data.

### **2.2. Purpose limitation**

*Personal Data shall be collected for specified, explicit and legitimate purposes (reasons) and not further processed in a manner that is incompatible with those purposes.*

Triple P UK must have a lawful and legitimate purpose for processing people's personal information. It may only collect and use that data for the specified purpose.

### **2.3. Data minimisation**

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

Triple P UK is permitted to collect and use the minimum amount of personal data that is required for the purpose(s) for which it is collected. That is, it may collect personal data that is adequate, relevant and not excessive. Triple P UK cannot collect more information than it needs to meet the processing requirements.

### **2.4. Accurate and up-to-date**

*Personal Data shall be accurate and, where necessary, kept up to date.*

Triple P UK must have process and policies in place to address how they will maintain the data they are processing and storing. Further, Triple P UK is obliged to take every reasonable step to ensure that any inaccurate personal data that it holds, having regard to the purposes for which that data is processed, are erased or rectified without delay.

## **2.5. Kept for no longer than necessary**

*Personal Data shall be kept in a form which permits identification for no longer than is necessary.*

This principle discourages Triple P UK from keeping unnecessary data (i.e. data that is redundant or a replication of data stored elsewhere). To comply with this principle, Triple P UK must control the storage, movement and retention of the data. Triple P UK demonstrates compliance by implementing and enforcing data retention policies. Further, Triple P UK must consider where data is stored in multiple places. Unless this is necessary for an identified purpose, the replication of the data should be removed.

## **2.6. Appropriate security measures**

*Personal Data shall be processed in a manner that ensures appropriate security of the personal data.*

Triple P UK uses appropriate security measures to protect the integrity and privacy (confidentiality) of the personal data that it holds. Triple P UK considers that the security measures it has implemented are proportionate to risks and rights of individual data subjects. Triple P UK has implemented security measures with respect to hard copy data (paper records), electronic data stored in Triple P UK's IT Systems and also physical security measures with respect to Triple P UK's office and equipment.

## **2.7. Accountability**

*Data Controllers must demonstrate compliance with the data processing principles.*

This principle ensures that Triple P UK can demonstrate its compliance with the other data processing principles. This requires that Triple P UK clearly document relevant policies and procedures and maintain accurate records and evidence of compliance (for example maintaining evidence of consent given to process data). It's compliance with the requirements of the GDPR must be auditable, and demonstrate that Triple P UK has taken appropriate action, where necessary.

## **3. CALDICOTT PRINCIPLES**

In 1997, the Caldicott Committee produced a report on its review of patient-identifiable information which identified issues regarding compliance with confidentiality and security arrangements across the NHS. The report identified six good practice principles for the health service when handling patient information. The principles were subsequently updated in March 2013. Although Triple P UK does not deal with patient records/information, as it undertakes projects with NHS organisations, it recognises and aims to comply with these principles.

### **1. Justify the purpose(s).**

Triple P UK recognises that when it processes personal data, it must ensure that it has a valid purpose for the processing activity. The purpose must be clearly defined and documented and reviewed on an ongoing basis.

### **2. Don't use personal confidential data unless it is absolutely necessary.**

Triple P UK recognises that it must only use people's personal data where it is necessary for the defined purpose. Where the data does not need to be identifiable, Triple P UK aims to use anonymised data. Triple P UK is particularly cautious of using personal data where the data is sensitive in nature (for example financial information or information categorised as "special category personal data" by the GDPR). Triple P UK recognises the need to review its use of identifiable personal data on an ongoing basis.

### **3. Use the minimum necessary personal confidential data.**

Triple P UK recognises that it must only use minimum personal data that is necessary to achieve the defined purpose for processing the data. Triple P UK recognises the need for this to be reviewed on an ongoing basis.

### **4. Access to personal confidential data should be on a strict need-to-know basis.**

Triple P UK's employees and independent contractors (e.g. independent Contract Trainers who run

Triple P Training/Accreditation sessions) or independent Implementation Consultants are only authorised to access and use people's personal data if that data is necessary for their performance of their role. Where Triple P UK uses sensitive personal data, such as financial information, it stores this information in databases with access controls in place. Where sensitive personal data is contained in emails, Triple P UK should save the emails to the appropriate database and delete the email from the email network. All Triple P UK's employees and independent contractors with @triplep.net email addresses are instructed to create robust passwords for the email account and to never share the password with anyone.

5. Everyone with access to personal confidential data should be aware of their responsibilities.

All Triple P UK employees and independent contract trainers have undertaken training, through an external training organisation, on the GDPR. Further, Triple P UK has begun an ongoing training process, in order to keep data protection considerations front of all Triple P UK employees' minds.

6. Comply with the law.

Triple P UK has regard to the requirements of the GDPR and the DPA18 when designing its data protection policies and procedures. The TPG Data Protection Officer works with Triple P UK regarding compliance with the UK's data protection laws.

7. The duty to share information can be as important as the duty to protect patient confidentiality.

This practice does not apply to Triple P UK, as Triple P UK does not include health and/or social care professionals.

### **3.1. Appointment of Caldicott Guardian**

Although Triple P UK does not handle patient information, Triple P UK have appointed a Caldicott Guardian, who is also Triple P UK's Data Protection Officer. The Caldicott Guardian is the senior person who is responsible for protecting the confidentiality of people's health and care information by Triple P UK (and TPI) and making sure it is used properly, should Triple P UK (or TPI) be provided with that type of information. When making decisions or giving guidance, the Caldicott Guardians will consider the Caldicott principles.

## **4. APPOINTMENT OF DATA PROTECTION OFFICER**

Triple P UK have appointed a Data Protection Officer ("DPO"), who is also the DPO for the entire Triple P Group of companies. The TPG Head of Information Governance (IG Lead) has been designated as Triple P UK's DPO, on the basis of their professional qualities, knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 of the GDPR. The DPO is a key part of Triple P UK's data protection compliance work. Triple P UK is committed to including the DPO in all discussions, working groups and decisions regarding issues which relate to the protection of personal data, including changes to data processing procedures. This includes involvement in the completion of any Data Protection Impact Assessments (DPIA). Triple P UK follows a privacy by design approach that recognises the importance of informing and consulting with the DPO promptly, at the outset of new projects, where data subjects seek to enforce their rights and if a data breach or other incident occurs. Triple P UK recognises that the opinion of the DPO should always be given due weight and in case of disagreement between Triple P UK's management and the DPO, Triple P UK should document the reasons for not following the DPO's advice.

### **4.1. Resources**

Triple P UK recognises that the UK's data protection laws require that it support the DPO function by providing the DPO with the resources necessary to carry out tasks and with access to personal data and processing operations, to maintain their expert knowledge. Triple P UK supports the DPO through active support of the DPO function by Triple P UK's senior management. This includes promoting the importance of Triple P UK employees reviewing all policies, procedures, guidance and training produced by or on behalf of the DPO. The DPO is supported by a team which includes the Group's IT Manager.

## **5. RESPONSIBILITIES:**

### **5.1. Data Protection Officer**

Triple P UK has appointed the Head of Information Governance as the Data Protection Officer (see section above about this role).

### **5.2. Caldicott Guardian**

Triple P UK has appointed the Head of Information Governance as the Caldicott Guardian (see section above about this role).

### **5.3. Chief Executive Officer**

Triple P UK's CEO is responsible for the application of this policy by Triple P UK and all Triple P UK employees. This includes the CEO:

1. Leading and fostering a culture that values, protects and uses people's personal information in appropriate ways and protects their information from misuse;
2. Ensuring the DPO is included in all discussions, working groups and decisions regarding issues which relate to the protection of personal data by Triple P UK;
3. Knowing what personal data Triple P UK collects and holds and understanding how it processes the information, the purpose and the lawful basis for the processing activities;
4. Knowing who has access to the personal data Triple P UK holds;
5. Ensuring Triple P UK employees only access and use the personal data that is necessary for the performance of their job;
6. Monitoring Triple P UK employee's compliance with Triple P UK's policies and procedures;
7. Ensuring Triple P UK employees promptly read all policies, procedures, guidance and other documents distributed to them by or on behalf of the DPO;
8. Ensuring Triple P UK employees promptly watch all training videos distributed to them by or on behalf of the DPO;
9. Ensuring there is a legal basis for processing and for any disclosures of personal information;
10. Ensuring Triple P UK employees immediately notify the DPO in the case of a data breach or suspected data breach;
11. Ensuring Triple P UK employees immediately refer the following to the DPO:
  - a. Requests from data subjects to enforce their rights under the GDPR, including but not limited to subject access requests;
  - b. Complaints or questions from data subjects regarding Triple P UK's use of their personal data or data protection practices;
12. Referring queries from Triple P UK employees, about any of the above, to the DPO.

### **5.4. TPG Head of Information Governance**

The TPG Head of Information Governance is responsible for:

1. Maintaining an awareness of information governance issues within Triple P UK;
2. Reviewing and updating Triple P UK's information governance policy in line with local and national requirements;
3. Reviewing and auditing all procedures relating to this policy where appropriate on an ad-hoc basis; and



4. Ensuring that Triple P UK's CEO and line managers at Triple P UK (and line managers at TPI where TPI employees process personal data on behalf of Triple P UK) are aware of the requirements of this policy.

### **5.5. Senior Information Risk Owner (SIRO)**

Triple P UK's CEO has been appointed as TPG's SIRO. Triple P UK considers that its CEO, as an Executive who is familiar with both the risks the organisation faces and the organisation's response to risk, is the appropriate person for this role. The SIRO is accountable and responsible for information risk across the organisation. The SIRO is responsible for ensuring that TPG treats information risks as a priority. The SIRO does not manage information risk from a technical perspective, rather focusing on information risk from a business perspective.

### **5.6. TPG IT Manager**

The TPG IT Manager is responsible for:

1. The formulation and implementation of IT related policies
2. The creation of procedures to support IT related policies and ensuring these are embedded within the IT Team when developing, implementing and managing robust IT security arrangements in line with industry best practice;
3. The effective management and security of the TPG, including Triple P UK, IT resources, for example, infrastructure and equipment;
4. Developing and implementing a robust IT Disaster Recovery Plan;
5. Ensuring that IT security levels required by NHS Toolkit are met (if any);
6. Ensuring the maintenance of all firewalls and secure access servers are in place at all times;
7. Ensuring the IT infrastructure has appropriate security measures in place. The IT infrastructure includes the work computers, work telephones, servers, networks, databases etc;
8. Ensure that where third party service providers are used for IT purposes (for example where external data warehouses are used for data storage) have appropriate security measures in place and have appropriately addressed GDPR compliance; and
9. Maintain a record of Triple P UK employees who have access to work emails on their personal mobiles, provide those employees with assistance/guidance regarding the security of their devices and ensure that access to work emails is removed from personal devices when a person's employment with Triple P UK comes to an end.

### **5.7. TPG Group General Manager**

The TPG IT Manager is responsible for:

1. Leading TPG's Data Protection and Privacy Project;
2. Supporting Triple P UK's CEO and Line Managers in ensuring that these policies and associated procedures are implemented;
3. Leading and fostering a culture that values, protects and uses people's personal information in appropriate ways and protects their information from misuse;
4. Ensuring the DPO is included in all discussions, working groups and decisions regarding issues which relate to the protection of personal data by Triple P UK;
5. Understanding the personal data Triple P UK collects, how it processes that data and the purpose and the lawful basis for the processing activities; and
6. Make or support Country Leads or Department Managers make decisions (where appropriate) involving GDPR compliance and data protection issues, such as data retention periods.

## 5.8. Line Managers

Line managers are responsible for:

1. Ensuring that these policies are implemented within their department or area of responsibility; and
2. Ensuring the employees who work in their department or area of responsibility, read the guidance, policies, procedures etc and watch the training videos released by or on behalf of the DPO.

## 5.9. Triple P UK Employees (Users of Data)

It is the responsibility of each Triple P UK employee to adhere to the information governance, data protection and associated policies and procedures. All Triple P UK employees must make sure they:

1. Use the organisation's IT systems appropriately and in accordance with IT policies, procedures, training and/or guidance; and
2. Only access and use people's personal data where the data is necessary for the performance of their job.

## 5.10. Information Governance Team

The Information Governance Team (otherwise referred to as the Privacy and Data Protection Team) is responsible for:

1. Monitoring and co-ordinating the implementation of these policies;
2. Providing advice and guidance on Information Governance and Privacy and Data Protection issues to all employees;
3. Developing information governance and privacy and data protection policies and procedures;
4. Developing information governance, privacy and data protection awareness and training programmes for employees;
5. Assisting Triple P UK to be compliant with GDPR/DPA18, Information Security and other information related legislation;
6. The creation of documents and processes required for compliance with applicable data protection and privacy laws; and
7. Managing freedom of information and subject access requests.

The Team includes:

1. TPG Head of Information Governance (also the DPO);
2. TPG Group General Manager; and
3. TPG IT Manager.

## 6. INFORMATION GOVERNANCE TRAINING

TPG recognises the GDPR as the global gold standard of data protection laws. As such, all TPG (not just Triple P UK) employees and independent contract trainers who were in place in 2018, were required to undertake training on the requirements of the GDPR/data protection. All new TPG employees and independent contract trainers are required to undertake training on the requirements of the GDPR/data protection within the following timeframes:

Full time employees	2 months of their start date
Part time employees	2 – 3 months of their start date
Independent contract trainers	2 – 3 months from completing Trainer training/accreditation

The training forms part of the induction process and is managed by TPG’s HR Team. If a new employee does not complete the GDPR/data protection training within the above timeframe, the matter is escalated to their Managers who are responsible for ensuring the training is completed ASAP. If a new independent contract trainer does not complete the training in the above timeframe, the Head of Training is notified and the trainer will not receive accreditation as a Triple P Trainer until the course is completed. This process ensures no Triple P Trainers deliver Triple P training or accreditation courses, without having first learnt about the data protection obligations and principles under the GDPR.

TPG further recognises that training must be reinforced. For subsequent information governance training, TPG employees and contract trainers will undertake refresher training on the GDPR and additional training on TPG’s data protection/information governance policies, procedures and guidance. This training is delivered by training videos which are prepared and released on behalf of the Data Protection Officer

## 7. DATA SECURITY AND PROTECTION TOOLKIT

The NHS have a Data Security and Protection Toolkit (DSP Toolkit) which forms part of their new framework for the NHS to assure itself that organisations are implementing the ten data security standards and meeting their statutory obligations on data protection and data security recommended in the UK government’s response to the National Data Guardian for Health and Care’s Review of Data Security, Consent and Opt-Outs and the Care Quality Commission’s Review ‘Safe Data, Safe Care’.

The NHS identifies that the ten data security standards apply to all health and care organisations. Whilst Triple P UK is not a health or care organisation, and does not process patient records or other NHS patient data, Triple P UK does work with NHS organisations, such as CCGs. As such Triple P UK is required by the NHS to complete at least the entry level requirements of the DSP Toolkit.

### 7.1.NHS’s Data Security and Protection Requirements Organisations

The NHS identifies the following Data Security and Protection Requirements for NHS Organisations. Triple P UK has considered where these requirements apply, given Triple P UK doesn’t deal with NHS patient information and will adhere to the following:

<b>Leadership Obligation 1</b>
<b>People:</b>
Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles
<ul style="list-style-type: none"> <li>• All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful and appropriate purposes</li> <li>• All staff understand their responsibilities with respect to data protection, including their obligation to handle information responsibly and only access and use people’s personal data where it is necessary for the performance of their job.</li> <li>• All staff complete appropriate data security training and are required to undertake refresher training (provide via in-house training programmes)</li> </ul>

<b>Leadership Obligation 2</b>
<b>Process:</b>
Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses
<ul style="list-style-type: none"> <li>• Triple P UK only permits its employees and independent contractors to access and use personal data that is necessary for them to perform their current role. All access to personal confidential data on IT systems can be attributed to individuals. Once accessed however, TPG’s IT Systems cannot control how the data is shared.</li> <li>• Triple P UK commits to review processes annually (and at the point of any infrastructure change) to identify and improve processes which have caused breaches or near misses, or which force employees or contractors to use workarounds which compromise data security</li> <li>• Cyber-attacks against Triple P UK (or TPG) are identified and resisted. Action is taken immediately following a data breach or a near miss, with a report made to management immediately and a report to the DPO within 30 minutes. Where the suspected breach involves the server being down and/or a possible cyber-attack, a report must also be immediately made to the IT Manager.</li> <li>• A disaster recovery plan is in place to enable Triple P UK to rebuild our IT infrastructure and restore data, in the event of a disaster.</li> <li>• A Data Breach Response Plan is in place to record and respond to data breaches or near misses, and it is scheduled to be reviewed annually.</li> </ul>

<b>Leadership Obligation 3</b>
<b>Technology:</b>
Ensure technology is secure and up-to-date.
<ul style="list-style-type: none"> <li>• No unsupported operating systems, software or internet browsers are used within the IT estate.</li> <li>• A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually</li> </ul>

## 7.2. Supporting Policies and Procedures

Supporting policies and procedures are needed to enable Triple P UK (and TPG’s) information governance, data security and protection obligations/responsibilities. These policies provide a framework that brings together the requirements, standards and best practice that apply to the handling of confidential, business sensitive and personal information. They include policies on Data Protection, Data Quality, Records Management, Access to Information, Freedom of Information and IT/Network Security.

## 8. NOT REQUIRED TO HAVE REGISTRATION AUTHORITY POLICY

As Triple P UK works with NHS bodies on projects, it has considered whether it required a Registration Authority Policy, which is associated with the entry level items for the NHS Toolkit. The NHS website (<https://digital.nhs.uk/services/registration-authorities-and-smartcards#registration-authorities>) defines registration authorities as follows

*“A registration authority is a function, usually within a NHS organisation, that carries out the identity checks of prospective smartcard users and assigns an appropriate access profile to the health professional's role as approved by the employing organisation.*

*Smartcards are required to access NHS Spine information systems and registration authorities roles and responsibilities are defined by NHS policy.”*

This does not apply to Triple P UK as we do not employ healthcare professionals, do not have access to NHS Spine information systems and do not hold or process NHS patient information. Accordingly, TPUK will not be creating a Policy re Registration Authority when completing the other entry level items for the NHS Toolkit.



## TRIPLE P UK LIMITED

### Data Protection Policy

**Version No: 1**

The purpose of the Triple P UK Data Protection Policy is to explain Triple P UK’s approach (and the approach of its related body corporate TPI) to ensure that when we collect, process and store the personal data that we need in order to operate our business, we comply with the requirements under the GDPR and Privacy Act 2018.

<b>Document type</b>	Data Protection Policy
<b>Date approved</b>	20/02/2020
<b>Date implemented</b>	20/02/2020
<b>Next review date</b>	<b>July 2021</b> or sooner should legislative change require.
<b>Policy author</b>	TPG Information Governance (IG) Team
<b>Applies to</b>	All Triple P UK Personnel  <b>Please Note:</b> This Policy also applies to all TPI Personnel who process personal data/information on Triple P UK’s behalf, as a result of Triple P UK outsourcing various business functions and tasks to the TPG head office. In those circumstances, references in this document to Triple P UK should be taken to be references to TPI.

**The local version of this document is the only version that is maintained. Any printed copies should therefore be viewed as “uncontrolled”, as they may not contain the latest updates and amendments. For the avoidance of doubt please see Triple P UKs Information Governance Lead.**

## **1. INTRODUCTION**

Triple P UK needs to collect and process various types of personal data from various types of data subjects, in order to carry out its business and provide its services (Open Enrolment and Agency Triple P training/accreditation and the Triple P Online Programme (“TPOL”)) and products (Triple P resources that assist practitioners and parents using Triple P. The lawful and proper treatment of personal information by Triple P UK and its related bodies corporate, is extremely important to the success of its business and to maintain the confidence of its service users, supporters and employees. Triple P UK must ensure that personal information is held and used lawfully and correctly, in line with this policy.

## **2. COLLECTION OF DATA**

### **2.1. Whose Data is Collected**

The people whose data Triple P UK (and/or TPG) requires (types of data subjects) includes:

1. Practitioners;
2. Personnel at organisations that Triple P UK works with;
3. Parents/Guardians who use TPOL;
4. Service Providers/Suppliers;
5. Triple P UK and TPG employees and independent contract trainers (present, past and prospective); and
6. Other business contacts.

### **2.2. When Data is Collected**

The occasions where personal information is collected may include:

1. When people (practitioners) register and attend Triple P Training/Accreditation courses;
2. When parents register to use TPOL;
3. When practitioners/agencies order Triple P materials;
4. When working with agencies (government bodies such as the NHS or government departments, charities, medical centres, child care centres etc)
5. Through the submission of queries online (via Triple P websites or social media accounts);
6. Through receipt of communication (emails, phone calls, letters etc);
7. At conventions/exhibitions or other events attended by Triple P personnel, where the person makes an expression of interest and seeks information regarding Triple P; and
8. When people apply to work with Triple P (ie in the recruitment process);
9. From people who work from Triple P in the course of their work (for example an employee disclosing personal information when making a leave request).

### **2.3. Why Data is Collected:**

The personal data is collected for a variety of purposes, including to facilitate the provision of Triple P training/accreditation, to provide access to online courses and online resources, to liaise with appropriate agency contracts for the development of projects and for marketing and promotional purposes etc. Triple P UK ensures that it identifies the purpose(s) and its lawful basis for collecting and using personal data, and that this information is included in Privacy Notices which are available to data subjects at the time their data is collected.

## **2.4. What Data is Collected**

The personal information collected/processed may include:

1. Their name;
2. Their address;
3. Their email address;
4. Their data of birth;
5. The organisation where they work;
6. Their role/job;
7. Whether they have undertaken any Triple P training/accreditation courses;
8. Their opinions; and
9. Other private and confidential information including sensitive information such as financial information or information about special needs or dietary requirements.

## **2.5. Special Category Personal Data**

Triple P UK understands that certain types of personal data are classified by the GDPR and associated legislation, as special categories of personal data and that this data cannot be processed except in a limited number of circumstances where an exception, defined in the GDPR, exists. Triple P UK will only collect and process this type of information where:

1. It has first obtained the data subject's express written consent (or the express written consent of a parent or guardian where the data subject is a child);
2. The processing is necessary to carry out Triple P UK's obligations and to exercise specific rights of the controller or data subject in the field of employment law;
3. The processing is necessary for the assessment of the working capacity of an employee;
4. The processing is necessary for the establishment, exercise or defense of legal claims; or
5. The processing relates to personal data which are manifestly made public by the data subject.

## **3. KEEPING DATA SUBJECTS INFORMED**

Triple P UK is required to let data subjects know what information it collects about them, how it will use that information, who it may share the information with and how it will protect and store the information, amongst other things. Triple P UK achieves this through:

1. The Privacy Policy posted on Triple P UK's public facing website; and
2. The Privacy Notices provided to data subjects at the point of data collection.

Triple P UK ensures that the information is provided in a manner where it is easy to access and easy to understand.

## **4. DATA QUALITY AND REUSE**

Triple P UK seeks to maintain standards of information quality and to avoid duplication, inaccuracy and inconsistencies across personal information held by Triple P UK and the wider Triple P Group. Triple P UK is committed to maintaining comprehensive records management policies in order to help avoid excessive retention or premature destruction of personal information.

Triple P UK will only use people's personal information where it is necessary and wherever possible, will use anonymised data.



## **5. DATA SUBJECTS' RIGHTS**

Triple P UK has a records management policy which ensures that individuals can exercise rights over their own personal data in line with GDPR/DPA18.

## **6. RECORD OF PROCESSING ACTIVITIES**

Triple P UK maintains an internal record of processing activities which includes the following: -

1. Purposes of the processing.
2. Description of the data processed
3. Details of who we send personal data to
4. Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
5. Description of technical and organisational security measures.

## **7. SECURITY**

Personal data should be kept secure at all times. Triple P UK ensures that there are adequate policies and procedures in place to protect against unauthorised access and against loss, destruction and damage.

## **8. TRANSFER OF DATA**

As an international organisation, the Triple P Group needs to transfer data around the world, in order to operate its business. Triple P UK utilises the services of its Australian related body corporate TPI, for the delivery of certain tasks and outsourced business functions. This included the IT function which involves the storage of data. Triple P UK recognises that appropriate safeguards are needed when transferring personal data internationally and that TPI must be provided with authorisation and instructions in order to process personal data on Triple P UK's behalf. Accordingly, Triple P UK and TPI have entered into Data Transfer and Data Processing Agreements, as required under the GDPR.

## **9. DISCLOSURE OF DATA**

Triple P UK has a policy governing in what circumstances personal data it controls may be disclosed both within the Triple P Group and to third-parties outside of the Group. This policy ensures that personal data is only shared where disclosure of the data is appropriate and Triple P UK has a lawful basis for doing so.

## **10. RETENTION OF DATA**

Triple P UK has a policy governing its retention of information, including personal data, which is used to ensure data is kept and destroyed as appropriate, in accordance with the data processing principles.



## TRIPLE P UK LIMITED

### Data Quality Policy

**Version No: 1**

The purpose of the Triple P UK Data Protection Policy is to identify what all Triple P UK employees need to do, to ensure the quality of data used by Triple P UK. This policy will enable everyone who works for Triple P UK to understand their responsibilities with regard to accurately recording of people's personal data

<b>Document type</b>	Data Quality Policy
<b>Date approved</b>	20/02/2020
<b>Date implemented</b>	20/02/2020
<b>Next review date</b>	<b>July 2021</b> or sooner should legislative change require.
<b>Policy author</b>	TPG Information Governance (IG) Team
<b>Applies to</b>	All Triple P UK Personnel  <b>Please Note:</b> This Policy also applies to all TPI Personnel who process personal data/information on Triple P UK's behalf, as a result of Triple P UK outsourcing various business functions and tasks to the TPG head office. In those circumstances, references in this document to Triple P UK should be taken to be references to TPI.

The local version of this document is the only version that is maintained. Any printed copies should therefore be viewed as "uncontrolled", as they may not contain the latest updates and amendments. For the avoidance of doubt please see Triple P UKs Information Governance Lead.

## 1. INTRODUCTION

Triple P UK is committed to taking reasonable and proportionate steps to ensuring the quality of its data. High quality information means Triple P UK is better serve its clients including the UK and Ireland based Triple P practitioners and identify anyone in the UK or Ireland who is falsely purporting to be trained or accredited to provide Triple P. High quality information also means Triple P UK is better able to work with organisations for the delivery of Triple P and is able to make better decisions, including with Triple P UK employees. Triple P UK notes that it does not work with or hold patient data, even when it works with NHS organisations to deliver access to Triple P. As such the data quality standards implemented by Triple P UK may be less than those implemented by NHS bodies, as appropriate and proportionate given the types of personal data Triple P UK holds.

## 2. RESPONSIBILITY

Responsibility for data quality rests with:

1. The IT Manager (with respect to maintaining the security and integrity of TPG's IT network, including physical IT infrastructure, the email network, TPG's servers and databases);
2. The Group General Manager (with respect to the operation of TPG's Client Relationship Management System);
3. The DPO and his support team, in terms of responding to rectification requests from data subjects; and
4. All people who work with Triple P UK to process the personal data they control, in terms of ensuring the data is recorded accurately and assisting the DPO to effect requests for rectification of data in a timely manner. It is their responsibility to ensure the information they generate is legible, complete, accurate, relevant, accessible and recorded in a timely manner.

Data Quality enables:

1. The more efficient delivery of services/products to Triple P UK's clients.
2. Triple P UK and its management to make decisions on the basis of accurate information.
3. To support TPG and the University of Queensland in further developing the evidence base that underpins the Triple P-Positive Parenting Program<sup>®</sup> and associated programs (Such as the Positive Early Childhood Education -PECE- Program).

All people who work at Triple P UK need to be able to rely on the accuracy of the information available to them, in order to provide timely and effective services regardless of their role.

## 3. DATA QUALITY STANDARDS

Triple P UK recognises that the data it holds should be:

### 3.1. Accurate and up to date:

All data must be correct and accurately. Where possible, personal data should be collected from the data subjects themselves. Where Triple P UK becomes aware that the data it holds may be incorrect/inaccurate, all reasonable and proportionate steps should be taken by Triple P UK to correct that data. This includes promptly referring requests for rectification of data to the DPO, and assisting the DPO to ensure the data is updated in all locations where it is stored.

Triple P UK is committed to ensuring that its employees and independent contract trainers receive appropriate training and are supported in their work, so that data is entered into Triple P UK's systems/databases accurately, the first time.

### 3.2. Complete:

Data should be captured in full. All personal data captured from data subjects should be stored in appropriate location(s). If Triple P UK becomes aware that there are data/records missing, Triple P UK must compile a list detailing the missing items, to be actioned later.

### **3.3. Timely:**

Data should be collected and recorded (added to the appropriate databases or systems) at the earliest opportunity.

### **3.4. Defined and consistent:**

Triple P UK employees should understand what data Triple P UK collects and the purposes for which it is collected, and should maintain consistency in the collection and processing of that data.

### **3.5. Free from duplication and fragmentation:**

Triple P UK should not have duplicated information, except to the extent that it is necessary. For example, the personal data of a practitioner who attended Open Enrolment training/accreditation will be stored in TPG's CRM System, but may also be stored by Finance where necessary or contained in documents sent to Triple P Trainers. Triple P UK should maintain appropriate procedures to ensure that once that duplication is no longer necessary, the duplicate data is destroyed.

All Triple P UK employees should know what data they are permitted to access and use for the performance of their job, where to access that data and where to store any data which they collect in the performance of their job.

### **3.6. Kept Secure and confidential:**

Data must be stored securely and processed in line with relevant legislation and local policy in relation to confidentiality. All Triple P UK employees (and independent contract trainers) must have due regard to where and how they store information, what information they store and how they share information. They must ensure they comply with Triple P UK's policies and procedures as well as contractual obligations of confidentiality.

## **4. VERSION CONTROL**

Tight version control is essential where multiple people are working with the same documents. This includes policies and procedures. Version control is required so that all Triple P UK employees are following current policies and procedures.

## **5. MANAGEMENT RESPONSIBILITIES**

Triple P UK's CEO and TPI's Heads of Teams are responsible for ensuring that they have clearly documented:

- The types of information that people in their area of responsibility are authorised to access and use;
- When that information should be used;
- How it should be used; and
- Who is authorised to use the various types of information?

They must ensure that appropriate training on these matters is provided to the people in their area of responsibility. Where they believe there is a gap in the training necessary, they should liaise with the DPO/IG Head to facilitate the provision of appropriate training.

Triple P UK's CEO and TPI's Heads of Teams must ensure that they have appropriate procedures in place to monitor the access, use and the quality of the data. They must also ensure that information risks associated with the data used by their area of responsibility, are actively identified and being mitigated, where possible.



## TRIPLE P UK LIMITED

### Records Management Policy

**Version No: 1**

The purpose of the Triple P UK Records Management Policy is to provide guidance to Triple P UK employees and contractors (such as the independent contract trainers) to identify their corporate and personal record management responsibilities, support them in meeting their responsibilities and to document the governance arrangements that Triple P UK has in place for effective records management.

<b>Document type</b>	Records Management Policy
<b>Date approved</b>	20/02/2020
<b>Date implemented</b>	20/02/2020
<b>Next review date</b>	<b>July 2021</b> or sooner should legislative change require.
<b>Policy author</b>	TPG Information Governance (IG) Team
<b>Applies to</b>	All Triple P UK Personnel  <b>Please Note:</b> This Policy also applies to all TPI Personnel who process personal data/information on Triple P UK’s behalf, as a result of Triple P UK outsourcing various business functions and tasks to the TPG head office. In those circumstances, references in this document to Triple P UK should be taken to be references to TPI.

The local version of this document is the only version that is maintained. Any printed copies should therefore be viewed as “uncontrolled”, as they may not contain the latest updates and amendments. For the avoidance of doubt please see Triple P UKs Information Governance Lead.

## 1. INTRODUCTION

Triple P UK recognises that maintaining accurate and complete records is essential, as it provides evidence of actions and decisions taken by Triple P UK, enables Triple P UK to meet its various legislative and accountability requirements and its administrative needs, and is a useful tool to support daily functions and operation of Triple P UK. Triple P UK considers that the effective management of its records is essential to protect Triple P UK's rights and reputation.

This policy sets out the principles of records management for Triple P UK and provides a framework for Triple P UK employees and contractors to use, to ensure the consistent and effective management of records.

Triple P UK intends, through effective records management practices, to ensure that:

1. The right information is available when needed.
2. Triple P UK has accurate and reliable evidence of business transactions.
3. Support Triple P UK personnel in decision making and planning processes.
4. There is better, more efficient use of data storage facilities, including physical storage and server space.
5. There is greater efficiency, by minimising the time spent by Triple P UK personnel searching for relevant information.
6. There is compliance with applicable legislative requirements and applicable standards.
7. There is a reduction in Triple P UK's costs, through efficiencies detailed above.

## 2. DEFINITIONS

In addition to the overarching Definitions for all Triple P UK Information Governance & Data Security and Protection Policies, the following definitions apply to this policy:

Records:	means information that is recorded in any form or medium, created or received and maintained by Triple P UK in course of its business.
Health Records:	means records which contain information relating to health (physical health or mental health) that has been made by or on behalf of a health professional in connection with the care of the individual.
Corporate Records:	means records which relate to the corporate business of Triple P UK, including accounts, minutes and meeting papers, legal documents, administrative documents etc.
Records Management:	Means the process whereby Triple P UK manages its records, through the use of administrative systems that direct/control the following, with respect to Triple P UK's records: <ul style="list-style-type: none"><li>• creation</li><li>• version control</li><li>• distribution</li><li>• storage;</li><li>• filing;</li><li>• retention;</li><li>• disposal/destruction</li></ul>

The process is designed to ensure that Triple P UK's records are dealt with in appropriate, compliant ways whilst assisting Triple P UK to operate efficiently and maintaining a historical record of Triple P UK's business.

Records Lifecycle: means the period in which a record exists, beginning at its creation/receipt, including the period of its use and the period of time when it is no longer actively used and ending with either the confidential destruction of the record or the preservation of the record in Triple P UK's archive.

Triple P UK personnel: means all Triple P UK employees (whether full time, part time, permanent, fixed term, casual and/or volunteers) and the independent contract trainers who provide Triple P training/accreditation in the UK and Ireland.

### **3. RECORDS MANAGEMENT**

#### **3.1. Records Creation**

All records created by/in Triple P UK must be created in a way that ensures that they are clearly identifiable, accessible and can be retrieved when required. They must be created in a timely fashion, accurately reflect what was communicated, decided or undertaken and contain sufficient information for the purposes for which they are kept.

Triple P UK must ensure it maintains adequate records in order to be accountable for decisions, actions, outcomes or processes. For example, the minutes of a meeting, project documentation or payment of an invoice.

#### **3.2. Records Use and Maintenance**

All Triple P UK personnel are required to properly maintain and protect the records they use, which will include emails.

Triple P UK personnel are only authorised to use the records, or the data contained in those records (whether confidential data, identifiable personal data or other), if it is necessary for the performance of their role at Triple P UK. They are not permitted to access or use records that are not necessary for the performance of their role. Where appropriate, for example when dealing with sensitive information and/or special category personal data, Triple P UK will ensure that it uses appropriate access controls, in the various locations where data is stored.

Triple P UK senior management and the TPG IT Manager are responsible for the identification and safeguarding of vital records which are necessary for business continuity. Information regarding the safeguarding of these records should be included in Triple P UK's business continuity /disaster recovery plans.

Where Triple P UK personnel become aware that records are unavailable or may have been corrupted or lost, they are required to immediately report this by email to:

1. Triple P UK's CEO;
2. TPG's Group General Manager;
3. Triple P UK's (and TPG's) DPO (using the [dpo@triplep.net](mailto:dpo@triplep.net) email); and
4. TPG's IT Manager.

#### **3.3. Records Tracking**

It is essential that Triple P UK personnel understand where Triple P UK's records are located, if the information they contain is to be available when needed. Records are easily misplaced or lost if responsibility for the creation and storage of the records is not clearly defined, if they are not stored in the correct locations and if no record is made where records are forwarded to other Triple P UK personnel or sent to recipients outside of Triple P UK and/or TPG.

Triple P UK must ensure that it:

1. Understands the records/information that it holds;

2. Has designated the appropriate place for that records/information to be stored, and communicated this to the Triple P UK personnel who use the records/information in the performance of their role; and
3. The use and storage of records/data is monitored at appropriate intervals, by Country Leads, Department Heads and other Managers.

Triple P UK must also, with respect to the relevant TPI departments/personnel who process records/information on Triple P UK's behalf, ensure that:

1. It understands what records/information those departments/personnel process on Triple P UK's behalf;
2. It understands where the records/information are stored; and
3. The TPI departments who process records/information on Triple P UK's behalf, have appropriate tracking/audit systems in place and monitors the use and storage of records at appropriate intervals; and
4. The Managers of all TPI personnel who process records/information on Triple P UK's behalf, have appropriate tracking/audit systems in place and monitors the use and storage of records at appropriate intervals.

### **3.4. Records Transportation**

As it is an international business, TPG stores records/information in a number of ways and locations. In order to operate, TPG utilises a network of its own computers in multiple countries, private physical IT infrastructure and third-party service providers whose infrastructure is used to store data (collectively referred to as "designated data storage facilities"). Where this policy refers to records transportation, it is not referring to storing the records/information in the appropriate locations within the designated data storage facilities. Nor is it referring to Triple P UK personnel transferring the data to other Triple P UK personnel (whether by email or hard copy records within Triple P UK's office) or TPI personnel who process records/information on Triple P UK's behalf (by email or by post in accordance with approved procedures).

When records (electronic or hard copy) are transported, appropriate steps to protect the records must be taken. This includes:

1. Triple P UK personnel should not store Triple P UK records/information on portable external storage devices (such as a USB), unless they have obtained permission from the Triple P UK CEO and/or TPG IT Manager who believe in the circumstances that it is appropriate.
2. Where paper records are transported, if possible, they should be transported in a locked bag. They must never be left unattended during transit. They must be stored in a secure location whilst being stored outside Triple P UK's office.
3. Where work laptops are transported, they must be password protected (locked) and, if possible, should be transported in a locked bag. The lap top must never be left unattended during transit. The laptop must be stored in a secure location whilst stored outside Triple P UK's office and must remain locked when not in use and/or not attended.
4. Triple P UK personnel should not store Triple P UK records/information on their personal devices, such as having access to work emails or files on personal mobile phones or tablets, without first obtaining the permission of Triple P UK's CEO and TPG's IT Manager. If Triple P UK personnel choose to obtain this approval, it is their responsibility to liaise with the TPG IT Manager to ensure they have appropriate security measures in place on their personal device.
5. Where personal devices containing Triple P UK records/information are transported, they must be password protected (locked) and, if possible, should be transported in a locked bag. The devices must never be left unattended during transit. The devices must be stored in a secure location whilst outside Triple P UK's office and must remain locked when not in use and/or not attended.



For advice regarding appropriate steps to protect records, including appropriate storage of records outside Triple P UK's office, please contact the TPG IT Manager or Triple P UK's DPO.

### 3.5. Records Storage

Triple P UK's records must be stored in appropriate locations, as described in Triple P UK's Privacy Notices and using access restrictions for sensitive or special category personal data. For example:

Type of Records/Information	Storage Location
Triple P courses - open enrolment registration information:	<p>Previously this information was stored in a private document database (P Drive) located on TPG's private server, which is located in TPI's private office. Now the information captured through open enrolment registration is stored in File Cloud. File Cloud is housed on Amazon's EC2 (Elastic Compute Cloud) server in the Republic of Ireland.</p> <p>Some of the open enrolment registration information will be entered into a private database that links to TPG's Provider Network. The database is stored in a private third-party (NetSuite) data warehouse located in the United States.</p>
Agency registration information	<p>Stored in a private document database (P Drive) located on TPG's private server.</p> <p>Information will be entered into a private database that links to TPG's Provider Network. The database is stored in a private third-party (NetSuite) data warehouse located in the United States.</p>
Disclosure forms re Impairment or Special Needs or special dietary requirements for course attendees	<p>Stored in restricted access folders in a private document database (P Drive) located on TPG's private server.</p> <p>Information about impairment/special need/dietary requirement may be communicated within TPG and with external parties (such as the course venue) where appropriate and necessary. This may be communicated via email. Where the information is provided to a third party, the third party should be asked to confirm they have destroyed that information, after the course has been completed (when they will no longer have a valid reason for holding the data)</p> <p>Where the data subject has agreed for the information to be shared with the Trainer, it will also be noted on the Electronic Bundle that is sent to them prior to Training.</p>
Booklets completed by attendees at Triple P courses	<p>Hard copy booklets are sent to TPI via the post. Hard copy booklets are stored in TPI's private office in Brisbane, Australia. Electronic (scanned) copies of the booklets are stored in a private document database (P Drive) located on TPG's private server.</p> <p>Information contained in the booklets is entered into a private database that links to TPG's Provider Network. The database is stored in a private third-party (NetSuite) data warehouse located in the United States.</p>
Trainer eBundles	<p>Sent to/from Trainers by email. Trainers send their completed EB's to a Triple P email group which has 7 recipients. Trainers instructed to delete the record from their system after it has been returned to Triple P UK/TPI post training/accreditation course. Bundles are stored in a private document database (P Drive)</p>

	<p>located on TPG's private server. For agency training, they are saved in folders associated with the individual agencies, within P Drive.</p> <p>(contains some information about the course attended and it is sent to Trainers prior to training/accreditation courses. Trainers may add notes to the bundles which is returned after the course)</p>
Agency Information	<p>These records are kept in a private database stored in a private third-party (NetSuite) data warehouse located in the United States. Previously, Agencies send various documents (e.g. Training Request Form, and Training Coordination form and the excel list of attendees) to Triple P UK by email. Previously these documents were filed in a private document database (P drive) located on TPG's private server. These documents will now be filed in File Cloud. If Triple P UK has an ongoing need to retain email communication with an agency (for example discussions regarding the terms of the agreement between the agency and Triple P UK, the emails will also be stored in File Cloud.</p>
Triple P Online (TPOL)	<p>TPOL is stored in a private database, hosted on the Amazon infrastructure in the EU and the United States. (The personal data in the TPOL records is controlled by TPI)</p>
Triple P UK Personnel Information (for HR purposes)	<p>These records are kept by the TPI HR Department and are stored in the HR Department's folders in the private document database (P Drive) located on TPG's private server. Access restrictions are in place for the HR Department's records.</p> <p>Records may also be kept by appropriate Triple P UK senior management (such as the CEO). These records will be kept in that personnel's folders on the private document database (P Drive) located on TPG's private server. Access restrictions will be in place for these folders.</p>
Triple P UK Personnel's Financial Information (for payroll purposes)	<p>TPI Finance Department holds financial records relating to Triple P UK personnel for payroll purposes. The information held includes banking info, pension info, tax info, pay slips etc. These records are stored in the Finance Department's folders in the private document database (P Drive) located on TPG's private server. Access restrictions are in place for the Finance Department's records.</p> <p>The Financial records/information is also held by the accounting firm in Edinburgh that Triple P UK uses for payroll. The Finance Department provides the accountants with the information by email. The only data not shared with the accountants are the payslips, which are sent by the Finance Department directly to the Triple P UK employees.</p>
Recruitment	<p><u>Information collected during recruitment process</u></p> <p>This may include CVs, cover letters, notes re interview answers, emails etc.</p> <p>These records will be stored in the HR Department's folders in a private document database (P drive) located on TPG's private server.</p> <p>Hard copy records may be necessary, during the recruitment process. Any hard copy records will be stored in the HR</p>

	<p>Department’s lockable cabinets within TPI’s private office in Brisbane, Australia. Once they are no longer needed, the hard copy documents will be securely destroyed.</p> <p>HR personnel and relevant Triple P UK personnel can transfer these records to each other, via email.</p> <p><u>Right to work in the UK Documents</u></p> <p>A hard copy of the document(s) will <b>not</b> be made.</p> <p>electronic (scanned) copy of the document(s) by a senior Triple P UK employee and emailed to the HR Department at TPI.</p> <p>The senior Triple P UK employee will not to retain a copy of the document(s). They will delete any copy they have, including from their email.</p> <p>HR Department will retain an electronic copy of the document(s) and associated emails and details. These will be stored in the HR Department’s folders in a private document database (P drive) located on TPG’s private server. Access restrictions are in place for the HR Department’s records. The HR personnel will delete any copy they have in their emails.</p> <p>TPI’s IT Department and/or Legal Department would also be able and authorised to access the HR Department’s restricted part of the database, if necessary and appropriate.</p> <p>Where the HR personnel share the documents/information for the purposes of establishing the person’s right to work in the UK or for the purpose of reporting concerns, the documents/information may be transmitted by email to legal advisers and/or relevant Government Officers.</p>
Electronic Direct Marketing Subscription Preferences	These records are kept in a private database stored in a private third-party (NetSuite) data warehouse located in the United States.
Project Documents	These records were previously stored in a private online document management system (TPOD) which TPG uses for the storage of documents. The online system is controlled by TPI and is stored on Amazon’s data warehouse in Sydney, Australia. These documents will now be stored in File Cloud.
Minutes of Meetings	These records were previously stored in a private online document management system (TPOD) which TPG uses for the storage of documents. The online system is controlled by TPI and is stored on Amazon’s data warehouse in Sydney, Australia. These documents will now be stored in File Cloud.
Financial Records	These records (i.e. revenue, expenses, invoices etc.) will be stored by TPI’s Finance Department in their folders in the private document database (P Drive) located on TPG’s private server. Access restrictions are in place for the Finance Department’s records.
DPO Records	These records will be stored in a private online document management system (TPOD) which TPG uses for the storage of documents. The online system is controlled by TPI and is stored on Amazon’s data warehouse in Sydney, Australia.

	<p>The records may include information relating to subject access requests, data breaches, etc.</p> <p>These records may also be stored on the work computers of the DPO and his support team and in their folders on the private document database (P Drive) located on TPG's private server. Access restrictions will be in place for these folders.</p> <p>These records may include emails between appropriate Triple P UK and TPI personnel, including Triple P UK's CEO, Triple P UK's Operations Manager and Triple P UK's Implementation Consultant.</p>
--	--

### 3.6. Retention

Triple P UK collects different types of personal data, from different types of data subjects, for different purposes. There is no one retention period. The retention periods for data controlled by Triple P UK (and/or its related bodies corporate) will vary. The retention periods will be determined by the IG Team (which includes the DPO and Triple P Group General Manager) in consultation with Triple P UK Management and the Heads of TPI Departments who process data on Triple P UK's behalf. The retention periods will depend on the type of record. The IG Team will take into account the purposes for which the data was collected and processed and any legal requirements to retain the data, when determining the appropriate data retention period.

The retention periods are set out in the Triple P UK Data Retention Policy and associated Data Retention Schedule. These documents identify minimum and maximum lengths of time that the records should be retained, where personal data is in an identifiable form. The Responsible Departments are required to destroy the personal data at some point during that period. This is achieved either through the secure destruction of the electronic and/or hard copy records or through the anonymisation of the personal data within the electronic and/or hard copy records.

These documents also set out the process to be followed where there is a desire to keep a record longer than the identified maximum period.

### 3.7. Disposal and destruction of records

Once the retention period for a record expires, if there is no justification for continuing to hold the record, they should be disposed of appropriately.

Paper records that are of a confidential nature and/or which contain people's personal data should be:

1. Put in the confidential waste bin provided by the company contracted (by Triple P UK or TPI re the records kept in Australia) to appropriately destroy the records; or
2. Shredded using a cross shredder that meets the appropriate standard (please contact the IT Manager to confirm any cross-shredder is appropriate).

Electronic records must be deleted from the device and not simply moved into the Trash folder, known as double deleting. This applies to records stored on databased, emails, computer hard drives etc.



## TRIPLE P UK LIMITED

### Access to Information Policy - Subject Access Requests (“SAR”)

**Version No: 1**

The purpose of the Triple P UK Policy re Access to Information Policy - Subject Access Requests, is to outline, for all Triple P UK personnel, how to deal with subject access requests received and, if they are asked, how to direct people to make a SAR.

<b>Document type</b>	Access to Information Policy - Subject Access Requests (“SAR”)
<b>Date approved</b>	20/02/2020
<b>Date implemented</b>	20/02/2020
<b>Next review date</b>	<b>July 2021</b> or sooner should legislative change require.
<b>Policy author</b>	TPG Information Governance (IG) Team
<b>Applies to</b>	All Triple P UK Personnel  <b>Please Note:</b> This Policy also applies to all TPI Personnel who process personal data/information on Triple P UK’s behalf, as a result of Triple P UK outsourcing various business functions and tasks to the TPG head office. In those circumstances, references in this document to Triple P UK should be taken to be references to TPI.

The local version of this document is the only version that is maintained. Any printed copies should therefore be viewed as “uncontrolled”, as they may not contain the latest updates and amendments. For the avoidance of doubt please see Triple P UKs Information Governance Lead.

## 1. INTRODUCTION

The current Data Protection laws in the UK (GDPR/DPA18) provide rights to all living individuals, including the right, subject to certain exemptions, to have access to their personal data/records that are held by Triple P UK (or TPI on behalf of Triple P UK). This is known as a ‘subject access request’ or ‘SAR’.

This Policy should be read with Triple P UK’s Guidance on Rights of Individuals under GDPR that has been produced for Triple P UK personnel. The Guidance contains further information to assist in recognising a SAR and details about the actions that should be taken if you receive a possible SAR.

## 2. WHAT IS A SAR

The right to access relates to electronic and hard copy information. It includes personal information held within electronic systems, spreadsheets, databases or word documents and also includes handwritten notes, photographs, audio recordings and CCTV images etc.

Individuals are entitled to be given a description of the following re their personal data/records:

1. What information Triple P UK holds;
2. What Triple P UK uses the information for;
3. Who might use the information;
4. Who Triple P UK may disclose it to;
5. Where the information was obtained (e.g. from the person themselves or a third party).

The GDPR also provides that individuals must be given information regarding:

1. Expected retention periods re their data;
2. Their right to request rectification or erasure of the data; and
3. Their right to object to the processing of their data.

In addition to asking for a copy of the information an organisation holds about them, individuals are entitled to be:

1. Told whether any personal data is being processed;
2. Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
3. Given a copy of the personal data; and
4. Given details of the source of the data (where this is available).

Personal data includes opinions expressed about the individual. It also includes indication of the intentions of people with respect to the individual. Also, there are some types of personal data that are exempt from the right of subject access. The DPO will consider whether any exemptions apply and will make appropriate redactions before responding to a SAR.

## 3. IMPORTANT INFORMATION

If Triple P UK receives a SAR:

1. Triple P UK must respond to the request and provide the information without delay and at the latest within one month of receipt (unless limited exceptions apply).
2. If Triple P UK fails to comply with a SAR, the maximum fine that can be issued by the UK Information Commissioner is 4% of global turnover or 20 million euros, whichever is higher, and individuals also retain the right to pursue a claim in court.

#### **4. RECOGNISING A SAR**

A SAR does not need to be made in writing and does not need to be referred to as a SAR, or refer to Data Protection/GDPR.

A SAR can be made by a variety of methods including:

1. Email;
2. Fax;
3. Post;
4. Social media;
5. Triple P website;
6. In person; or
7. Over the phone.

Sometimes it may not be clear that the request is a SAR. For example, requests referring to other legislation such as the Freedom of Information Act 1998 may amount to a SAR. If someone in the UK (or elsewhere in the EU) asks for something that involves their personal data, you should refer it to the Data Protection Officer as a possible SAR.

Examples of subject access requests:

1. What information do you hold about me;
2. Do you have any photos of my child;
3. Do you have a record of the Triple P Training I have completed;
4. Can you send me a copy of my HR file; or
5. I am a solicitor acting on behalf of my client and request a copy of their employment record (where an appropriate authority is enclosed).

#### **5. REQUESTS MADE ABOUT OR ON BEHALF OF OTHER INDIVIDUALS**

If Triple P UK receives a request which is made by a third party on behalf of another living individual, then Triple P UK must obtain appropriate and adequate proof of that the person has provided their consent to the third party to make the request or obtain evidence of a legal right of the third party to act on behalf of that individual. For example, a third party may make a request if they hold a power of attorney and a solicitor may make a valid SAR on behalf of an individual who is their client.

#### **6. REQUESTS BY OR ON BEHALF OF A CHILD**

The rights of children under the GDPR are the same rights as adults have over their personal data. This includes the rights to access their personal data. The ICO has identified that a child can exercise their rights as long as they are competent to do so and, where a child is not considered to be competent, an adult with parental responsibility may usually exercise the child's data protection rights on their behalf.

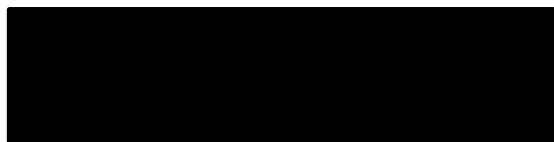
If Triple P UK receives a request which is made by or on behalf of a child, it will need to carefully consider how to respond. The DPO will consider ICO guidance at the time of any request, and if appropriate, may seek further guidance from the ICO.

#### **7. PROCESS**

Requests for information held about an individual must be directed to TPG's IG Team (the Privacy and Data Protection Team) who manage SARs:

1. By emailing [dpo@triplep.net](mailto:dpo@triplep.net):
  - c. A copy of the request (if it was made in writing); or
  - d. All information about the request (if it was made verbally).

2. By forwarding the above email to:



The DPO will acknowledge the request, log it and notify the requestor of the next steps. The requestor may be asked to provide further relevant information, including documents for ID verification.

*It is important that a SAR is identified and sent to the IG Team/DPO quickly. There is a short timeframe (within one month of receipt) for Triple P UK to respond to the request.*

## **8. RESPONDING TO REQUESTS**

A detailed Standing Operating Procedure (SoP) has been produced which gives full details as to how the TPG IG Team responds to individual SARs. This SoP is available through the DPO. The SoP includes making a record of all requests received. The record will include:

1. The date received;
2. The date the response is due;
3. The applicant's details;
4. The information requested;
5. Any exemptions applied (if applicable);
6. Details of information disclosed; and
7. When and how supplied (for example, hard copy and by post).





## TRIPLE P UK LIMITED

### Freedom of Information (FOI) Policy

**Version No: 1**

The purpose of the Triple P UK Freedom of Information Policy is to outline what Triple P UK should do if it receives a FOI request or if it receives a request to assist an organisation working with Triple P UK, to respond to a FOI request which they have received.

<b>Document type</b>	Freedom of Information Policy
<b>Date approved</b>	20/02/2020
<b>Date implemented</b>	20/02/2020
<b>Next review date</b>	<b>July 2021</b> or sooner should legislative change require.
<b>Policy author</b>	TPG Information Governance (IG) Team
<b>Applies to</b>	All Triple P UK Personnel  <b>Please Note:</b> This Policy also applies to all TPI Personnel who process personal data/information on Triple P UK’s behalf, as a result of Triple P UK outsourcing various business functions and tasks to the TPG head office. In those circumstances, references in this document to Triple P UK should be taken to be references to TPI.

The local version of this document is the only version that is maintained. Any printed copies should therefore be viewed as “uncontrolled”, as they may not contain the latest updates and amendments. For the avoidance of doubt please see Triple P UKs Information Governance Lead.

## 1. INTRODUCTION

The Freedom of Information Act 2000 (FOIA) provides for public access to information held by public authorities. Public authorities include government departments, local authorities, the NHS, state schools and police forces. Just because an organisation receives public money, does not mean it will be considered a public authority. For example, the FOIA does not apply to some charities that receive government grants and some private sector organisations that perform public functions.

The IG Team considered the definition of “public authority” within the FOIA and guidance issued by the UK Information Commissioner’s Office and has concluded that Triple P UK would not be considered a public authority and therefore would not be subject to the requirements of the FOIA. However, the IG Team acknowledges that Triple P UK works with organisations who are subject to the FOIA. Should those organisations receive a Freedom of Information (FOI) request, they must consider the request and:

1. Inform the requester whether it holds the information requested;
2. Supply the requested information (subject to relevant exemptions within the FOIA).

Triple P UK may have contractual obligations to assist those organisations in the event of their receipt of a FOI request.

## 2. RECOGNISING A FOIA REQUEST


A FOI request must be:

1. Received in writing (this may be in hard copy or electronic form i.e. an email)
2. Identify the name of the requester.
3. Provide the requester’s address for correspondence; and
4. Clearly describe the information requested.

## 3. WHAT TO DO IF YOU RECEIVE A REQUEST FOR INFORMATION

If you receive a request, it must *immediately* be passed to TPG’s IG Team (the Privacy and Data Protection Team). Failure to do this may result in a delay in the IG Team processing the request. Any delays may result in Triple P UK breaching contractual obligations under project agreements. This may also result in a failure, by the public authority working with Triple P UK, to comply with the FOIA.

Please notify the IG Team of a request by emailing the request to [dpo@triplep.net](mailto:dpo@triplep.net) and cc’ing:

1. 
2. 
3. 

If the FOI request was directed to Triple P UK (or its related bodies corporate), the IG Team will inform the requester that the organisation is not subject to the FOIA. If the requester is not happy with that response, the IG Team will inform them that they may make a complaint to the ICO.

If the FOI request was directed to a public authority working with Triple P UK, the IG Team will liaise with the public authority to identify the assistance sought from Triple P UK. The IG Team will manage the process of locating and disclosing any relevant information (subject to applicable exceptions) to the public authority. Triple P UK will not disclose information directly to the requester. The public authority will be responsible for communicating directly with the requester.

## 4. EXEMPTIONS

Organisations subject to the FOIA may only refuse to disclose the requested information if there is an applicable exemption within the FOIA that limits people’s rights to the information. Some of the exemptions contained within the FOIA provide an absolute exemption while others require

organisations to consider whether there is a public interest in disclosing the information and to weigh that against other factors.

Where assisting public authorities with a FOI request, the IG Team will consider if Triple P UK has any obligation to assist the authority with their response, and if so, whether any of the information held by Triple P UK or the authorities behalf, that is within the scope of the request, is subject to any exemptions within the FOIA.

## **5. TIME LIMITS FOR COMPLIANCE WITH REQUESTS**

Under the FOIA, public authorities are required to provide the information requested within 20 working days of a request. There are some circumstances where this timeframe may be extended under the terms of the legislation.

## **6. MONITORING AND EVALUATION**

Triple P UK will monitor the FOI requests it receives and the requests it received from public authorities, to assist them in responding to FOI requests. The IG Team will provide annual FOI reports to Triple P UK Senior Management. These reports will identify:

1. Number of FOI requests Triple P UK had received;
2. Number of requests Triple P UK had received, to assist Public Authorities with FOI requests;
3. Response times (detailed explanations where response time wasn't appropriate)
4. Justification of any exemptions applied;
5. Complaints; and
6. Any requests escalated to the ICO.



## TRIPLE P UK LIMITED

### Network and IT Security Policy

**Version No: 1**

The purpose of the Triple P UK Network and IT Security Policy is to describe the controls and processes put in place to maintain the confidentiality, integrity, and availability of information stored and processed on the IT Infrastructure used by Triple P UK and its related bodies corporate.

<b>Document type</b>	Network and IT Security Policy
<b>Date approved</b>	20/02/2020
<b>Date implemented</b>	20/02/2020
<b>Next review date</b>	<b>July 2021</b> or sooner should legislative change require.
<b>Policy author</b>	TPG Information Governance (IG) Team
<b>Applies to</b>	<p>All Triple P UK Personnel who have access to TPG’s computer systems and communications networks, whether they are Triple P UK employees, volunteers, contractors or are suppliers granted access for support purposes.</p> <p><b>Please Note:</b> This Policy also applies to all TPI Personnel who process personal data/information on Triple P UK’s behalf, as a result of Triple P UK outsourcing various business functions and tasks to the TPG head office. In those circumstances, references in this document to Triple P UK should be taken to be references to TPI.</p>

The local version of this document is the only version that is maintained. Any printed copies should therefore be viewed as “uncontrolled”, as they may not contain the latest updates and amendments. For the avoidance of doubt please see Triple P UKs Information Governance Lead.

## **1. INTRODUCTION**

Triple P Group recognises that the information stored in its IT Systems/Network is valuable corporate asset and that the confidentiality, integrity and availability of that information must be protected, including from any breach, loss, or unavailability of TPG's Information Systems.

In operating as a business, disseminating the Triple P – Positive Parenting Programme ® throughout the world, TPG is provided with people's confidential and personal information. TPG recognises that it is essential to preserve the confidentiality and integrity of the information entrusted to it, whilst also enabling the effective and appropriate use of that information.

This policy is part of Triple P UK's Information Governance strategy, with information regarding TPG's approach to:

1. Data Protection;
2. Data Security;
3. Data Quality;
4. Confidentiality;
5. Information Sharing; and
6. Records Management

## **2. SYSTEMATIC APPROACH TO IT/CYBER SECURITY**

For the purposes of this policy, a reference to IT/Cyber Security is a reference to the technical and organisational measures, including technologies, processes and practices used by Triple P UK and its related bodies corporate, to protect TPG's network, its infrastructure (including computers and servers) and its data.

TPG utilises a systematic approach to protect the confidentiality, integrity and availability of TPG's data and IT systems, that includes:

1. People (with clearly defined duties and responsibilities);
2. Policies and Processes reinforced by external and in-house training;
3. IT systems; and
4. Risk management processes.

### **2.1. Policies and Processes**

Triple P UK recognises that disclosure of many of its policies and procedures regarding IT Security, could compromise the security of Triple P UK and the Triple P Group's Network and IT Facilities and compromise the security of the information stored there. For this reason, this publicly available policy will outline Triple P UK's commitment to the security of its Network and IT Infrastructure and will refer to various policies which are not disclosed to anyone outside of the Triple P Group. These include our:

1. Password Policy
2. IT Department password management procedure
3. Email and Internet Acceptable Use Policy
4. Disaster Recovery Plans
5. Business Continuity Plans

## 2.2. People and HR:

All recruitments follow a screening process according to the principles of the Triple P Group ('TPG') approach to background checks. Further, in each employment contract there are provisions re confidentiality and compulsory data protection training.

The responsibilities and duties with respect to Triple P UK/TPI personnel regarding matters of IT security, are clearly defined in this policy.

## 2.3. Awareness/Training

Triple P UK is committed to providing regular awareness training regarding data protection, including on the GDPR, to all Triple P UK employees and TPI employees who process information on Triple P UK's behalf. This involves:

- External Training
  - All new TPG personnel are required to undertake external training on the GDPR which is provided by GRC eLearning.
  - TPG personnel, for these purposes, refers all TPG employees regardless of whether they are casual, permanent, full time or part time. It also applies to volunteers or independent contractors such as contract trainers. Triple P recognises the importance of this training, which is why completion of this training is a requirement under any employment contract or contractor agreement and why the training is provided to Contract Trainers at Triple P's expense.
  - All existing TPG personnel completed this training in 2018/2019.
  - Full time employees must complete the training within 2 months of their start date.
  - Part-time employees must complete the training within 2 or 3 months of their start date, dependant on the number of days they are working.
  - Casual employees must complete the training within 2 or 3 months of their start date, dependant on the number of hours they are working.
  - Contract Trainers must complete the training within 2 months of completing their training/accreditation as a Triple P Trainer.
  - Contract Implementation Consultants must complete the training within 2 months of completing their training/accreditation as an Implementation Consultant
- In-house Training
  - In 2020 an in-house training video series focusing on privacy, data protection, information governance and IT/cyber security, is being rolled out.
  - The training is being sent to all TPUK employees (and select contractors) and to TPI employees who process data on TPUK's behalf or who process data controlled by TPI, that relates to people living in the EU (including the UK).
  - Triple P UK and the wider Triple P Group recognise that people are one of the keys to information and IT security, and that developing awareness and associated changes in behaviour, is a process. For that reason, Triple P has developed a training program that involves regular, short training videos, which are usually between 5 minutes and 15 minutes in length. The refer to policies, procedures and guidance documents that provide further information on the topics covered. The different topics are also repeatedly touched on throughout the series, as Triple P recognises that repetition of training is essential to promoting awareness, understanding and behavioural change.
  - The training videos and associated documents are currently being released every Monday and Wednesday, with the first video in the series was released on 13 January 2020. The topics that will be covered include, but are not limited to:

- Data Breaches and Triple P's Data Breach Response Plan;
- An overview of the GDPR;
- The Principles of Data Processing;
- Lawful bases for processing data;
- Special category personal data;
- The Rights of Data Subjects;
- Information Security;
- Appropriate Use of email and the internet;
- Passwords;
- Cyber risk, including phishing, Malware, ransomware, hacked passwords and enforcement action;
- Managing risk;
- Subject Access Requests;
- Social Media Use;
- Data Retention; and
- Data Destruction.

#### **2.4. Physical Security and paper records:**

Throughout the Group:

- Access control and visitor management systems are implemented for all visitors/guests;
- Physical access to all data centres is controlled by both physical and electronic locks;
- Physical access reviews as per defined periodicity;
- Secure printing, process implemented;
- Except with prior specific authorisation, laptops and desktops are not taken off-site;
- Fire alarm and fire-fighting systems implemented for employee safety; and
- Fire evacuations drills are conducted at specified frequencies.

#### **2.5. Remote end user device is protected:**

For remote users working with laptop and desktop on the TPG secured network the following security measures are, additionally, incorporated:

- Domain Authentication;
- Centrally managed anti-virus protection;
- Management and monitoring of the software to control an authorised software installation;
- Vendor supplied updates are installed;
- Login ID and password controls are implemented to access information;
- Periodic access review is implemented;
- E-mails are automatically scanned by anti-virus and anti-spam software; and
- Any other set up of connections needs to be upfront approved by the security department.

## **2.6. Communications & operations security**

- Termination of access connection in Demilitarized Zone;
- All connectivity to and from TPG's secured network encrypted using not less than 128 bit encryption; and
- Multiple layers of firewalls & intrusion detection need to be passed.

## **2.7. Access control to Personal Data**

Employees with access to information held by Triple P UK or its related bodies corporate, including personal data, are only authorised to access and use information that is necessary for their job, i.e. for them to carry out the activities they are responsible for.

There are restricted storage facilities on the Drives and Databases where data is stored. Triple P UK's processes require that sensitive information (such as payment information) and/or special category personal data only be stored in restricted locations. Access authorisation is provided based on the 'need to know' and 'need to access' and is either role based or name based. Access logs are in place with most systems and the responsibility for access control is assigned.

Triple P IT's Department have put the following measures in place:

- User (password) codes for access to Private Data;
- Access managed according to Role Based Access Control principles;
- Differentiated access regulations (e. g. partial blocking); on all systems containing PI data;
- Access Logging and control on most systems; and
- Procedures for Checking compliance with procedures and work instructions are in place.

## **2.8. Security and confidentiality of personal data**

The measures/actions taken by Triple P to protect the confidentiality and security of personal data, is based on a risk assessment and TPG will ensure a level of security appropriate to the risk, if any, including:

- The anonymization, pseudonymisation (e.g. tokenization) and encryption of Personal Data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- Ensure a logical separation between its own data and the data of its customers and suppliers;
- Access log systems used with for the purposes of being able to detect unauthorised access attempts on most systems; and
- Customer Data (including back-ups and archives) will only be stored for as long as it serves the purposes for which the data was collected unless there is a legal or contractual obligation to retain the data for a longer period of time.
- Use of anti-virus software that mitigates the risk of a computing device being infected with or affected by malware.



## **2.9. Business continuity management**

Disaster recovery plans and procedures are in place to restore data and access to data within 48 hours. This is used in place of a dedicated Business continuity plan. These plans and procedures are confidential and are never publicly disclosed.

## **2.10. Organisation control**

Triple P maintains its internal organisation by:

- Internal data processing policies and procedures, guidelines, work instructions, process descriptions and regulations for programming, testing and release; and
- Having an emergency plan with procedures and allocation of responsibilities (backup plan).

## **3. DUTIES AND RESPONSIBILITIES**

Triple P UK's IT function is outsourced to the TPI IT Department. Whilst ultimate responsibility for IT security rests with Triple P UK's Director, the Director has delegated day to day responsibility for IT Security to the IT Manager.

### **3.1. The IT Manager**

The IT Manager is responsible for:

- Developing, managing and implementing IT Security policies/processes;
- Conducting risk assessments re IT security for new IT projects, equipment, applications and software. This includes identifying vulnerabilities and appropriate counter measures;
- Regularly reviewing IT security risks;
- Providing information and advice to Triple P UK's Director and TPG's Group General Manager regarding:
  - Any threats to Triple P UK's (or TPG's) IT Security and ways to address those threats; and
  - IT security topics or developments, where appropriate.
- Providing advice to all IT personnel regarding implementation of this policy as required;
- Monitoring and enforcing compliance with this policy by IT personnel;
- Assisting, recording and investigating IT security related incidents;
- Auditing and monitoring the erasure of data in accordance with identified data retention periods and the disposal of IT equipment and media.
- Overseeing the physical security of IT work areas (including the Server Room located in TPI's private office)
- Implementing monitoring of computer/internet/email user activity, as and when instructed by Triple P UK's Director;
- Authorising all external and remote connections to the TPG Network, including through @triplep.net email accounts, as appropriate;
- Acting as the IT Department representative for the TPG Information Governance Team/ Privacy and Data Protection Team;
- Providing ad-hoc security information or training to Triple P UK personnel on IT security issues;
- Conducting ad-hoc security awareness testing of Triple P UK personnel, for example by sending emails to test Triple P UK personnel's ability to recognise fishing/malware emails.

### 3.2. The IT Department

The IT Department is responsible for:

- Maintaining the confidentiality, integrity and availability of the Network and IT systems and the data stored there
- Creating, deleting or disabling Triple P UK personnel's IT access/accounts, including
  - Access to allocated computer;
  - Access to @triplep.net email accounts
  - Access to electronic storage/databases including TPG's local Drive, online document management system and customer relationship management system;
- Managing the IT Systems Change Control process;
- Ensuring only licensed, approved software is installed on IT systems and managing requests for the installation of software on work devices (IT Manager approval is required to install);
- Managing requests for and maintaining a record of employee access to triplep.net email accounts on personal devices (IT Manager approval is required to install);
- Responding to requests for information regarding IT matters raised internally and by Triple P UK's clients (for example queries relating to access to Triple P Online, ASRA or the Provider Network);
- Arranging collection of IT equipment and media for secure disposal on an ad-hoc basis as needed and on an employee's departure
- Erasing TPOL data in accordance with identified data retention periods and procedures;
- Auditing and facilitating the erasure of data stored electronically by Triple P UK employees, in cooperation with the Data Protection Officer and accordance with identified data retention periods and procedures;
- Assisting the IT Manager in responding to IT security incidents
- Invoking and conducting disaster recovery operations when required;
- Managing, implementing, auditing and monitoring information back-up schedules and processes;
- Responding to IT support requests;
- Providing external remote connections to TPG's Network and IT Systems for authorised users;
- Providing relevant system security advice for Triple P UK employees;
- Complying with security incident (including Data Breach) response plans and reporting procedures;
- Managing and/or assisting with testing TPG's disaster recovery and continuity plans;
- Auditing information back-up procedures;
- Managing access controls and password use in accordance with approved policies;
- Conducting spot checks to confirm compliance with security policies and procedures; and
- Removing access to work emails from personal devices of employees, and/or recovering work devices, prior to an employee's departure from employment with TPI or TPUK.

### **3.3. Triple P UK's CEO**

Triple P UK's CEO is responsible for:

- Understanding:
  - What information is held by Triple P UK;
  - Why it holds that information;
  - How it uses that information;
  - Where that information is stored;
  - Who has access to it (and why);
  - How long that information should be kept by Triple P UK; and
  - For personal data, the lawful basis for Triple P UK to process the data.
- Ensuring that TPUK personnel use the information within the law;
- Completing and ensuring that all TPUK personnel complete training released by the Information Governance Team and/or Data Protection Officer, which relates to data protection and cyber security or other related topics.

### **3.4. Heads of TPI Departments processing Triple P UK's data**

The Head of each Department is responsible for:

- Understanding:
  - What information is held by their Department;
  - Why it holds that information;
  - How it uses that information;
  - Where that information is stored;
  - Who has access to it (and why);
  - How long that information should be kept by the Department; and
  - For personal data, the lawful basis for the Department processing the data.
- Ensuring that the personnel within their Department use the information within the law;
- Completing and ensuring that all their Department's personnel complete training released by the Information Governance Team and/or Data Protection Officer, which relates to data protection and cyber security or other related topics.

### **3.5. The Human Resources Department**

The Human Resources Department is responsible for:

- Ensuring that all contracts of employment for new employees include data security requirements (for example completion of mandatory external GDPR training within identified period of start date and obligations re confidentiality and complying with TPUK's policies and procedures);
- Ensuring the IT Department is notified in a timely manner of new employees (for account creation) and of employee departures (for IT to deactivate accounts);
- Ensuring that any physical security devised, such as access swabs for the TPI office, are collected from employees prior to departure from employment; and
- Taking disciplinary action as appropriate against any employee in breach of this policy or related policies.

### 3.6. Line Managers

Line Managers are responsible for:

- Ensuring that all employees under their management (direct report) are aware of this policy and associated policies & procedures and understand their responsibilities as outlined by those documents;
- Ensuring that when a direct report leaves TPI/TPUK, that work-related data that may have been in that person's individual account (email account) or in restricted storage locations on drives, databases etc, is relocated to an appropriate location where the line manager can access it. This will involve liaising with the employee and the IT Department, as necessary;
- Following the Data Breach Response Plan where a breach or possible breach is reported to them by a direct report. This includes supporting their direct report to take appropriate mitigating actions and ensuring they follow the response plan, then completing the assessments to be undertaken by managers within the incident report and passing the matter to the DPO.

### 3.7. All employees

Every TPUK Employee (or TPI employee who processes TPUK's data) is responsible for:

- Reporting any IT security incident (including a data breach or possible data breach or cyber-attack etc) in accordance with TPG's Response Plan, including:
  - Immediately notifying their Line Manager (or other appropriate people if the line manager isn't immediately available), the DPO and the IT Manager;
  - Taking appropriate mitigating actions, if any; and
  - Completing the relevant sections of the incident report.
- Setting and changing their passwords in accordance with the Password Policy;
- Never disclose their passwords to others (except in accordance with Password Policy);
- Not allow others to use their individual work accounts (e.g. their email account) for any purpose;
- If there is a need for a 'shared' account, this should be discussed with the IT Department and only created and used with their approval;
- Not connect any private hardware to any TPG computing equipment or TPG's network without prior written approval from the IT Manager;
- Not install or attempt to install any software on TPG's computing equipment without prior written approval from the IT Manager;
- Comply with applicable laws re data protection;
- Only access information, including personal data, that is held by TPUK or its related bodies corporate where they need that information for the performance of their job;
- Never disclose or provide access to information held by TPUK or its related bodies corporate, to any unauthorised recipients of that information, regardless of whether the recipient is within TPUK, TPG or is an external third-party;
- Only provide access to information held by TPUK or its related bodies corporate, to people within TPG in accordance with Triple P UK's Data Sharing Policy, if they need the information for the performance of their job;
- Only provide access to information held by TPUK or its related bodies corporate, to people outside of TPG, in accordance with Triple P UK's Data Sharing Policy;

- Not access, view and/or extract any information stored on Triple P UK's (or TPG's) IT Systems for personal reasons or attempt such action. For example, looking at friends' files or at information out of curiosity;
- Lock or log off if leaving any workstation unattended;
- Shut down their workstation overnight and on weekends. This will allow installation of software and/or software updates deployed remotely by the IT Department.
- Manage their records (e.g. emails, files, folders, documents), saving the records in approved locations and securely destroying them in accordance with data retention policies and document destruction procedures; and
- If leaving employment with TPUK (or TPI):
  - Return all work equipment, (e.g. computers, phones, tablets) to the IT Department;
  - Remove access to work emails from personal devices (such as phones) and confirm this has occurred with the HR and IT Departments;
  - Move data in personal accounts (e.g. email) or private storage locations on TPG drives, databases etc, in accordance with instructions from their Line Manager and the IT Department; and
  - Destroy hard copy and electronic copy documents securely in accordance with data retention policies and document destruction procedures.



## TRIPLE P UK LIMITED

### DATA SECURITY POLICY

**Version No: 1**

The purpose of the Triple P UK Data Security Policy is to outline how we prevent data security breaches and how we react to them when prevention is not possible. A data breach is a security incident in which the confidentiality, integrity or availability of data is compromised. A breach can either be purposeful or accidental.

<b>Document type</b>	Data Security Policy
<b>Date approved</b>	February 2020
<b>Date implemented</b>	February 2020
<b>Next review date</b>	<b>July 2021</b> or sooner should legislative change require.
<b>Policy author</b>	TPG Information Governance (IG) Team
<b>Applies to</b>	All Triple P UK Personnel and to the processing of all confidential information, including all personal data, whether it is in hard copy or electronic form.  <b>Please Note:</b> This Policy also applies to all TPI Personnel who process personal data/information on Triple P UK’s behalf, as a result of Triple P UK outsourcing various business functions and tasks to the TPG head office. In those circumstances, references in this document to Triple P UK should be taken to be references to TPI.

The local version of this document is the only version that is maintained. Any printed copies should therefore be viewed as “uncontrolled”, as they may not contain the latest updates and amendments. For the avoidance of doubt please see TPUKs Information Governance Lead.

## **1. INTRODUCTION**

Triple P UK is committed to safeguarding and protecting the sensitive personal information and confidential information that it holds, as is required by law (including, but not limited to, the Data Protection Act 2018 (“**DPA**”) and the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”).

This Data Security Policy covers:

1. Physical Access Procedures;
2. Digital Access Procedures;
3. Data Security Breach procedures; and
4. Responsibilities.

## **2. PHYSICAL ACCESS PROCEDURES**

Employees with access to information held by Triple P UK or its related bodies corporate, including personal data, are only authorised to access and use information that is necessary for their job, i.e. for them to carry out the activities they are responsible for. Access to hard copy records is based on a ‘need to know’ and ‘need to access’ basis.

All Triple P UK personnel receive training about confidential information and this is incorporated into the induction process. The training includes data protection laws, cyber security, and how they should use, store and share confidential information. Triple P UK personnel are only told where particular records are physically stored, if those records are needed for the performance of their role.

Locked storage cabinets in Triple P UK’s offices in the UK and in Triple P International’s office in Brisbane, Australia. There are also physical security access controls with respect to those offices.

Our personnel must store hard copy personal and confidential data securely in locked storage cabinets when not in use, and must not leave the keys in the filing cabinets. There are designated locations where the individual keys are kept. Only those entitled to access the records will be informed of the key location.

Triple P UK’s Record of Processing Activities and Data Retention Schedule identify where it stores the different types confidential information, including personal data, that it holds. The records reflect where data is stored in Hard Copy form. Triple P UK personnel understand that we may conduct ad hoc spot checks to ensure that hard copy records are stored in the appropriate locations and are properly secured.

## **3. DIGITAL ACCESS PROCEDURES**

Employees with access to information held by Triple P UK or its related bodies corporate, including personal data, are only authorised to access and use information that is necessary for their job, i.e. for them to carry out the activities they are responsible for.

There are restricted storage facilities on the Drives and Databases where data is stored. Triple P UK’s processes require that sensitive information (such as payment information) and/or special category personal data only be stored in restricted locations. Access authorisation is provided based on the ‘need to know’ and ‘need to access’ and is either role based or name based. Access logs are in place with most systems and the responsibility for access control is assigned.

Triple P IT’s Department have put the following measures in place:

- User (password) codes for access to Private Data;
- Access managed according to Role Based Access Control principles;
- Differentiated access regulations (e. g. partial blocking); on all systems containing PI data;

- Access Logging and control on most systems; and
- Procedures for Checking compliance with procedures and work instructions are in place.

Triple P UK personnel who require access to the digital systems used by the Triple P Group for their job role, will be trained on the use of those system as part of the induction process. The IT Department will provide user login details to those personnel, on instructions from senior management.

The digital storage systems used by Triple P UK, allow IT to identify which personnel have access to restricted folders. Where changes are made to a person's to user access requirements for their role, the change must be approved by the person's manager and the Data Protection Officer.

Triple P UK's Record of Processing Activities and Data Retention Schedule identify where it stores the different types confidential information, including personal data, that it holds. The records reflect where data is stored in electronic form. Triple P UK personnel understand that we may conduct ad hoc spot checks to ensure that electronic records are stored in the appropriate digital storage facilities.

The IT Department is responsible for the security measures in place to protect the digital storage facilities used by Triple P UK. However Triple P UK makes clear to all personnel that they are all responsible for the security of the information we hold. As such they are provided with training and are required to follow the company's policies and procedures. Triple P UK has robust password policies and management procedures in place.

As soon as an employee leaves, all their access to the digital system are revoked. This is part of the Leaving Procedure that Triple P UK has in place.

When not in use all screens will be locked.

#### **4. DATA SECURITY BREACH PROCEDURES**

In order to mitigate the risks of a security breach, Triple P UK has:

1. Robust physical and digital security measures in place;
2. A clear Data Breach Response Plan in place to appropriate respond to a suspected security breach;
3. Provided the Data Breach Response Plan to all Triple P UK personnel;
4. Provided an "immediate action" poster to all Triple P UK personnel, so they know what immediate first steps to take if they suspect a breach. We have asked all personnel to keep a copy of this poster in easy sight at their workstations.
5. Provided training to all Triple P UK personnel on data protection and cyber security. The training includes how to recognise a potential data breach, how to mitigate the risk of a breach and what to do in the event of a breach.
6. Ensured our personnel understand the importance of immediate action in the event of suspected security breach, understand what procedures to follow and how to escalate the incident to the correct people in order to determine if a breach has taken place and take appropriate action to mitigate the effect of the breach.

If it appears that a data security breach has taken place:

1. The person who noticed the breach (or potential breach) will:
  - Immediately notify certain key personnel; and
  - Complete the first section of the Data Breach Incident Report.



2. The Data Breach Incident Report is then provided to their Manager, who will complete the Manager's section of the form and undertake some initial assessments to determine if there has been a breach, and what next steps are appropriate.
3. Once the Manager has updated the Data Breach Incident Report, it is handed to the Data Protection Officer or, if they are not available, to a member of the DPO's support Team.
4. Where the breach involves a cyber element, or where there are concerns that the server is down, the IT Manager is immediately notified, is required to complete a specific part of the Response Plan and will work with the DPO to ensure the matter is properly investigated, documented and appropriate mitigating actions are taken.
5. The Data Protection Officer will:
  - Complete the rest of the Incident Report, reviewing the information provided by the person who observed the suspected breach and the information and assessments undertaken by the Manager;
  - Consider whether the matter should be escalated to the full response team;
  - Consider whether mandatory reporting requirements are triggered (for a data breach involving personal data, mandatory reporting is required in the UK & EU where it is likely that there will be a risk to the rights and freedoms of an individual data subjects).
6. Where mandatory reporting is required, Triple P UK will report the matter to the ICO, as soon as practicable, but at least within 72 hours of our discovery of the breach.
7. Where the breach involves NHS controlled personal data, and it is likely that there will be a risk to the rights and freedoms of an individual data subjects, Triple P UK will report the breach to the NHS via the DSPT Incident Reporting Tool ([www.dsptoolkit.nhs.uk/incidents/](http://www.dsptoolkit.nhs.uk/incidents/)) as soon as practicable, but at least within 72 hours of our discovery of the breach.

A report to the ICO would include the following details:

1. The nature of the personal data breach (i.e. confidentiality, integrity, availability);
2. The approximate number of data subjects concerned;
3. The categories of data subject concerned (e.g. employees, practitioners, electronic direct marketing mailing lists etc);
4. The categories of data concerned (including whether any special category personal data is involved);
5. The approximate number of personal data records concerned;
6. The name and details of Triple P UK's Data Protection Officer;
7. The likely consequences of the breach;
8. A description of the measures taken, or which Triple P UK intends to take, to mitigate any possible adverse effects of the breach; and
9. Whether the data subjects have already or are still to be informed that their personal data has been breached (only informed if it is likely that there is a high risk to their rights and freedoms. In those circumstances Triple P UK will inform those individuals directly and without any undue delay).

Triple P UK maintains a register where it records any data breach. This includes details of the breach, mitigating action taken, whether the ICO, data subjects etc were notified of the breach, and whether a change to the business' processes/procedures is needed in light of the circumstances that led to the breach;

## **5. RESPONSIBILITIES**

IT Manager is responsible for physical security and digital security measures of the IT infrastructure at the TPI Office.

Triple P UK's CEO and Operational Manager are responsible for physical security of the Triple P UK offices.

Triple P UK's CEO, with the assistance of the DPO, is responsible for updating the record of data breaches and record of processing activities.

The DPO is responsible for managing responses to breaches.



## TRIPLE P UK LIMITED

### POLICY REGARDING SHARING PERSONAL DATA WITH THIRD PARTIES

**Version No: 1**

The purpose of the TPUK policy regarding Sharing Personal Data with Partner Organisations is to minimise the risk of loss, unauthorised disclosure, modification or removal of information held by Triple P UK and clarify the appropriate ways that the organisation may share information, in order to support its operations.

<b>Document type</b>	Policy Regarding Sharing Personal Data with Third Parties
<b>Date approved</b>	March 2020
<b>Date implemented</b>	March 2020
<b>Next review date</b>	<b>July 2021</b> or sooner should legislative change require.
<b>Policy author</b>	TPG Information Governance (IG) Team
<b>Applies to</b>	<p>All Triple P UK Personnel. It applies to the sharing of all forms of personal data (hardcopy and electronic) with all third parties, whether processors or joint data controllers.</p> <p><b>Please Note:</b> This Policy also applies to all TPI Personnel who process personal data/information on Triple P UK's behalf, as a result of Triple P UK outsourcing various business functions and tasks to the TPG head office. In those circumstances, references in this document to Triple P UK should be taken to be references to TPI.</p>

The local version of this document is the only version that is maintained. Any printed copies should therefore be viewed as “uncontrolled”, as they may not contain the latest updates and amendments. For the avoidance of doubt please see TPUKs Information Governance

## 1. INTRODUCTION

Triple P UK is part of the Triple P Group (“TPG”), a group of related bodies corporate that are responsible for disseminating the Triple P-Positive Parenting Program® (“Triple P”) and the Positive Early Childhood Education Program (“PECE”) throughout the world. The provision of training and accreditation services and associated materials for Triple P and PECE, requires the sharing of information within TPG and with (external) third parties including, but not limited to the University of Queensland (the creators of Triple P and PECE) and various service providers.

This document sets out the overarching principles and commitments that will underpin the secure and confidential sharing of information between Triple P UK and other individuals or organisations, for the continued operation of the business. Triple P UK acknowledged that there is a balance between the need to share personal data for the business to operate and the protection of confidentiality. An effective and structured approach is essential, so that we can share information carefully and responsibly and assure the practitioners, agencies and families who use our products and services, and our personnel, that information Triple P UK holds about them is shared securely and appropriately, whilst respecting their right to privacy and confidentiality.

## 2. GLOSSARY OF TERMS

Term	Acronym	Meaning
Data Controller	-	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Joint Controllers	-	Where multiple parties are data controllers, and therefore may make decisions about the processing of personal data.
Data Processor	-	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Act 1998	DPA 1998	An Act for the regulation of the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information
Data Protection Act 2018	DPA18	Act replaced DPA 1998 above
Freedom of Information Act 2000	FOIA	The Freedom of Information Act 2000 provides public access to information held by public authorities
General Data Protection Regulation	GDPR	The General Data Protection Regulation (EU) 2016/679

Personal Data	-	Information that relates to an individual who can be identified either directly or indirectly
Special Category Personal Data	-	Particular types of personal data classified by the GDPR (see Article 9) which have additional conditions that must be met in order to lawfully collect, use and share the data.
Data Sharing	-	The disclosure of personal data from Triple P UK to a third party (another organisation or individual), including the sharing of data between Triple P UK and TPI, as Triple P UK has outsourced various business functions to TPI.
Internal Data Sharing	-	The sharing of data with TPI (or any other company within TPG)
External Data Sharing	-	The sharing of data with organisation or individual who are not part of TPG
Systematic data sharing	-	The routine sharing of data sets between organisations/individuals for an agreed purpose, including situations where organisations/individuals 'pool' their data for specific purposes.
Exceptional Data Sharing	-	Where Triple P UK decides, or is asked, to share data in situations which are not routine.

### 3. OVERVIEW - HOW WE SHARE PERSONAL DATA

As a Data Controller, Triple P UK makes decisions about how and why data is processed. Some of Triple P UK's own data is processed in-house. Other data is processed by our related body corporate, TPI, who perform various outsourced business functions for Triple P UK. Triple P UK and TPI have entered into written Data Processing and Data Transfer Agreements. The Data Processing Agreement contains detailed instructions regarding what processing TPI may undertake with respect to the personal data Triple P UK controls.

For an overview of how Triple P UK shares personal data see Annexure 1 to this Policy. The Schedule in Annexure 1 sets out (in general terms):

8. What information is shared with third parties;
9. The lawful basis for sharing information;
10. The common purposes for holding and sharing data;
11. How information will be stored; and
12. The third parties (individuals and organisations) who data is shared with.

## **4. GENERAL PRINCIPLES OF INFORMATION SHARING**

The general principles of information sharing that Triple P UK follows are:

1. Personal data must only be shared in appropriate circumstances, where there is a lawful basis for sharing the data.
2. Special Category Personal Data must only be shared where the data subject has given explicit consent to the sharing of the data with the recipient.
3. Only Triple P UK (and TPI) personnel who are authorised to share personal data as part of their role, may disclose personal data to other organisations.
  - They are authorised to undertake Systematic Data Sharing;
  - They may only undertake Exceptional Data Sharing where they have sought the approval of their Manager and the DPO.
4. The minimum necessary amount of personal data must be shared, having regard to the purpose for the processing of the personal data. Triple P UK must not share personal data where the other individual/organisation does not need that data to fulfil the purpose for which it was collected.
5. Where possible, data should be shared in anonymised form. That is, if the recipient does not need the data to identify the individual data subjects and can still use the data to achieve the defined purpose, then they should be provided with anonymised data, not personal data. Triple P UK ensures that when it shares anonymised data, that the data does not identify an individual, either directly or indirectly, when combined with other information that the recipient has access to.

## **5. RESPONSIBILITIES**

Where Triple P UK is the Data Controller, it is responsible for compliance with current data protection laws (including the DPA18 and the GDPR) and for satisfying itself that the organisations and individuals with whom it shares personal data, are also compliant with those laws.

### **5.1. Information Users**

All Triple P UK personnel (including independent contract trainers and implementation consultants) receive training from Triple P UK on matters of data protection. Triple P UK personnel are responsible for complying with data protection laws when they interact with personal data in the performance of their role. Where a decision is taken to share information with relevant individuals or organisations, the person disclosing the information is responsible for ensuring that they are authorised to disclose the information, that the individual/organisation is an authorised recipient, and that the recipient understands the confidentiality of the information

### **Data Protection Officer (SIO)**

The DPO (with the assistance of the Data Protection and Privacy Project Team) is responsible for providing Triple P UK with information and advice on matters of data protection and assisting Triple P UK to collect and process data in compliance with applicable data protection laws.

### **5.2. Triple P UK CEO**

Triple P UK's CEO has the responsibility of overseeing the business' compliance with applicable data protection laws and of developing good data protection practices within the company. The CEO may ask the DPO and the Data Protection and Privacy Project Team to assist in developing good data protection practices within Triple P UK. The CEO is responsible for overseeing and authorising data sharing by Triple P UK and must ensure that appropriate controls are in place.

### **5.3. TPI Heads of Department**

The Heads of the Departments at TPI that perform outsourced business functions of or provide business services to Triple P UK, are responsible for monitoring their Department's compliance with applicable

data protection laws and for developing good data protection practices within their Department. This includes how their Department shares personal data (both internal and external data sharing). Head of Department may ask the DPO and the Data Protection and Privacy Project Team to assist in developing good data protection practices within their Department. The Heads of Department are responsible for the information assets of their Department and for overseeing and authorising how their Department shares data, including by ensuring that appropriate controls are in place.

#### **5.4. Managers/Supervisors**

Managers and supervisors should ensure that the people they manage/supervise only share personal data with appropriate individuals and organisations.

**Annexure 1 – Overview of Internal and External Data Sharing**

Category	Data Type	Details	Controller	Transferred to	Description of Recipient	Purpose	Lawful Basis	Notes
Practitioner Data	CRM Record	name, contact info, work info, qualifications, training/ accreditation details, subscription preferences etc	Triple P UK	NetSuite	IT Infrastructure Provider (Customer Relationship Management System)	Data Storage	Legitimate Interest	
	Registration Data	Name, contact info, info re work and qualifications, course interested in attending	Triple P UK	TPI – Data Entry Team	Internal Sharing (within TPG)	1) Enter into NetSuite for Data Storage 2) Set up Provider Network access	1) Legitimate Interest 2) Performance of a Contract	
	Registration Data for Open Enrolment	As above plus payment information	Triple P UK	As Above plus TPI – Finance Team	Internal Sharing (within TPG)	Facilitate payment for course	Performance of a Contract	
				Geoghegans	Geoghegans is an Edinburgh-based firm of chartered accountants. (external)	Business Purpose	Legitimate Interest	
	Special Dietary Requirements	May be/reveal special category personal data (e.g. health or religion)	Triple P UK	TPI (Email Network)	Internal Sharing (within TPG)	Data Storage and sending/receiving by email	Consent	Catering Provider (external) not provided with personal data. Just told what the requirement is. E.g. 1 gluten free meal and 2 halal meals
	Impairment of Special Need	May be special category personal data (health)	Triple P UK	Venue	External	To accommodate the practitioner’s impairment/special need (if possible) when attending the training	Consent	
				Triple P Trainer running the course	Internal/External (some trainers are TPG employees and other are contractors)	To accommodate the practitioner’s impairment/special need (if possible) when attending the training	Consent	
				TPI (Email Network)	Internal Sharing (within TPG)	Data Storage and sending/receiving by email	Consent	
	Data Collected at Training	Contact info, eDM Consent, Parent Consultation Skills Checklist, Training Workshop Evaluation Survey, signature re benefits of and the conditions for acquiring accreditation statement etc	Triple P UK	TPI – Data Entry Team	Internal Sharing (within TPG)	1) Compile a register of persons trained to deliver Triple P 2) Administrative purposes 3) Optional/discretionary information gathered for statistical purposes 4) To send eDM emails re Triple P UK	1) Legitimate Interest 2) Legitimate Interest 3) Legitimate Interest 4) Consent 5) Legitimate Interest 6) Legitimate Interest	



						5) Provide feedback re Trainer(s) and course for continuous improvement 6) Show agreement to T&Cs of accreditation		
	Communication (email/phone/ letter)	Practitioner enquiries/complaints	Triple P UK	TPI – DPO	Internal Sharing (within TPG)	Investigating and responding	Legitimate Interest	
		Complaint re Trainer/Course	Triple P UK	TPI – Head of Training	Internal Sharing (within TPG)	Investigating and responding	1) Legitimate Interest 2) Consent*	*Where complaint relates to efforts to accommodate impairment/special need/special dietary requirement at the course, the practitioner is asked to complete a further statement of consent authorising the investigation of the complaint by Triple P UK & by TPI etc
	Record of Trained/ Accredited Practitioners	Name, what aspects of Triple P have undertaken training/accreditation in etc	Triple P UK	The University of Queensland (UQ)	External. UQ are the creators of Triple P and PECE	Complying with Reporting Requirements	Legitimate Interest	
	eDM Lists	Name, email address, subscription preferences	Triple P UK	TPI – Comms Team	Internal Sharing (within TPG)	Sending eDM to Agency Contacts in line with their subscription preferences	Consent (Previously Legitimate Interest)	
				Bureau Blanco	External Sharing (Contractor that oversees TPG’s communications function)	Sending eDM to Agency Contacts in line with their subscription preferences	Consent (Previously Legitimate Interest)	
Agency Data	CRM Record	Name and contact details of key people at agency, past orders re materials and training etc	Triple P UK	NetSuite	IT Infrastructure Provider (Customer Relationship Management System)	Data Storage	Legitimate Interest	
	Project Development	Name, contact information, job role and place of work etc	Triple P UK	TPI – Dissemination/ Implementation Support Team & Business Services Providers & DPO	Internal Sharing (within TPG)	Assisting Triple P UK in tender process, designing project, completing PIA, negotiating and finalising documentation etc	Legitimate Interest	
	eDM Lists	Name, email address, subscription preferences	Triple P UK	TPI – Comms Team	Internal Sharing (within TPG)	Sending eDM to Agency Contacts in line with their subscription preferences	Consent (Previously Legitimate Interest)	
				Bureau Blanco	External Sharing (Contractor that oversees TPG’s communications function)	Sending eDM to Agency Contacts in line with their subscription preferences	Consent (Previously Legitimate Interest)	
Government Contacts	Names and contact information for TPUK contacts at government departments	Triple P UK	PLMR	PLMR is a London based Public Affairs agency (external)	Public Affairs support services for business development purposes	Legitimate Interest	Contact details for key stakeholders across target areas for public affairs work	

	Contacts re Trials	Names and contact information for TPUK contacts at settings/agencies participating in trials	Triple P UK	PLMR	PLMR is a London based Public Affairs agency (external)	Public Affairs support services for business development purposes	Legitimate Interest	Data shared with PLMR for recruitment of EEF trial
TPOL User Data	Registration Data	Name, email, TPOL Code, password	TPI	N/A	N/A	Administrative support purposes	Performance of a Contract	
	Program Responses	observations, answers to questions and working through exercises	TPI	N/A	N/A	Enabling the user to work through the program	Performance of a Contract	Access very restricted (only IT experts are able to access the data, however they have instructions not to do so.
	Management System Data (individual users)	Name, email, data re use of/progress through TPOL	TPI	N/A	N/A	Administrative support purposes	Performance of a Contract	
	Management System Data (project users)	Name, email, data re use of/progress through TPOL	TPI & Agency	Agency (Joint Controller)	External	Administrative support purposes and shared to comply with project agreements	Performance of a Contract	Where the user's TPOL code is paid for by an agency (e.g. government departments, NHS bodies, charities) the agency may have access to the Management System Data. No other Agency would have access. No agency will Ever have access to the other TPOL data (registration and program responses)  As joint controller, the agency will make their own decisions regarding how they will use that data.
PECE User Data	Registration Data	Name, email, PECE Code, password	TPI	N/A	N/A	Administrative support purposes	Performance of a Contract	
	Program Responses	observations, answers to questions and working through exercises	TPI	N/A	N/A	Enabling the user to work through the program	Performance of a Contract	Access very restricted (only IT experts are able to access the data, however they have instructions not to do so.
	Management System Data (individual users)	Name, email, data re use of/progress through PECE	TPI	N/A	N/A	Administrative support purposes	Performance of a Contract	
	Management System Data (project users)	Name, email, data re use of/progress through PECE	TPI & Agency	Agency (Joint Controller)	External	Administrative support purposes and shared to comply with project agreements	Performance of a Contract	Where the user's PECE code is paid for by an agency (e.g. government departments, NHS bodies, charities) the agency may have access to the Management System Data. No other Agency would have access. No agency will Ever have access to the other PECE data (registration and program responses)  As joint controller, the agency will make their own decisions regarding how they will use that data.

Triple P UK Employees	HR Data	Name, contact info, job details, employment contracts, leave (annual, carers, parental, sick leave etc) health information etc.	Triple P UK	TPI – HR Team	Internal Sharing (within TPG)	HR Purposes - (including hiring, performance management, liaising with employees, managing leave and health issues, investigating complaints etc)	Performance of a Contract  Legitimate Interest	NB Where processing of special category personal data is involved in the HR business function (including right to work checks at recruitment and managing health issues re employees etc) the Article 9 (GDPR) exception relied on is either that the processing is necessary to carry out obligations and to exercise specific rights of the controller or data subject, in the field of employment law or is necessary for the assessment of the working capacity of an employee.
	Payroll Data	Name, salary, pension info, tax info	Triple P UK	TPI – Finance Team	Internal Sharing (within TPG)	Payroll Purposes	Performance of a Contract	
			Triple P UK	Geoghegans	Geoghegans is an Edinburgh-based firm of chartered accountants. (external)	Business Purpose	Performance of a Contract	
		Name, salary, pension info, DOB	Triple P UK	Royal London  (The Royal London Mutual Insurance Society Limited)	Royal London is a London based Pension provider (external)	Business Purpose	Performance of a Contract	The data shared with Royal London is needed for them to ensure compliance with minimum contributions
		Some of the payroll information	Triple P UK	St James Place Wealth Management  (██████████)	St James Place Wealth Management is a UK based wealth management business and ██████████ acts as Triple P UK's pensions advisor (external)	Business Purpose	Performance of a Contract	Some payroll information has been shared with the pensions advisor in the past.
	Mobile Phone Data	Limited data of employees, such as names and records re use of phone (e.g. phone numbers re calls made)	Triple P UK	EE & O2	EE and O2 are the mobile phone service providers used by Triple P UK	Business Purpose	Performance of a Contract	24month contracts
	Corporate Credit Card & Banking	Contact details and personal identifying data for a limited number of TPUK/TPI staff	Triple P UK	HSBC	HSBC is the banking institution Triple P UK banks with (external)	Business Purpose (Banking and Financial transactions)	Performance of a Contract	Company Corporate Card accounts contain personal contact details, inc mother's maiden names etc, for TPUK staff plus contacts for TPI staff (accessing for administrative purposes). The system also seems to store historical personal data related to previous card holders e.g have left the company
Triple P UK Contractors (Trainers and ICs)	Contract Information	Name, whether working under a company, contact info, availability to conduct training etc	Triple P UK	TPI – Training Coordination Team, HR Team, Business Services etc	Internal Sharing (within TPG)	Issuing Contracts e.g. for training/accreditation courses	Performance of a Contract	
	Similar to HR Data for employees	contracts, health issues etc impacting ability to work	Triple P UK	TPI - Training Coordination Team, HR Team, Business Services etc	Internal Sharing (within TPG)	Managing issues e.g. any accommodations that need to be made, unavailability for training etc	Legitimate Interest	Where a contractor discloses special category information such as health matters, Triple P UK will seek a statement of explicit consent as the lawful basis (and Article 9 GDPR exception) for processing the data.

	Payment Data	Name, whether working under a company, banking information	Triple P UK	TPI – Finance Team	Internal Sharing (within TPG)	Process invoice payment etc	Performance of a Contract/Legitimate Interest	
				Geoghegans	Geoghegans is an Edinburgh-based firm of chartered accountants. (external)	Business Purpose	Performance of a Contract/Legitimate Interest	
Suppliers	Invoices etc	Name and contact details of people at supplier company/or of supplier where an individual	Triple P UK	NetSuite?	IT Infrastructure Provider (Customer Relationship Management System)	Data Storage	Legitimate Interest	
				TPI – Finance Team	Internal Sharing (within TPG)	Process invoice payment etc	Performance of a Contract/Legitimate Interest	
				Geoghegans	Geoghegans is an Edinburgh-based firm of chartered accountants. (external)	Business Purpose	Performance of a Contract/Legitimate Interest	