道坦图英国监护数据保护政策

1. 引言与目的

本政策阐述了我们依据《英国通用数据保护条例 2016》和《数据保护法 2018》处理个人信息的方法。

根据本政策，道坦图是数据控制方，并在 ICO 注册，注册号为 ZB977664。

本政策的目的是解释我们如何根据相关数据保护法处理个人信息，并告知代表我们处理个人信息的员工及其他个人我们的相关期望。

2. 适用范围

本政策适用于道坦图英国监护所持有的个人信息的处理。这包括关于员工、志愿者、家长、学生、寄宿家庭、访客以及与我们互动的任何其他个人的个人信息。

本政策应与《道坦图英国监护隐私政策》一并阅读。

3. 定义

以下术语在本政策中通篇使用，理解其含义非常重要：

- 个人数据：任何与可被识别（直接或间接）的自然人相关的信息，通过参考标识符如姓名、身份证号、位置数据、在线标识符，或该自然人的生理、心理、遗传、精神、经济、文化或社会身份的一个或多个特定因素。
- 数据主体：个人数据所指向的已识别或可识别的在世自然人。
- 控制者：单独或与他人共同决定个人数据处理目的和方式的个人、公共机构、部门或其他机构。

- 处理者：代表控制者并根据其指示处理个人数据的个人或组织。
- 处理：对数据进行的任何操作，包括收集、记录、存储、使用、分析、组合、披露或删除。
- 特殊类别数据：揭示种族或民族出身、政治观点、宗教或哲学信仰、或工会会员资格的个人数据。还包括基因数据、生物识别数据，以及有关个人健康、性生活及性取向的数据。

4. 角色与职责

道坦图英国监护 是数据控制者，负责遵守英国 GDPR。

Director：Meng-Ting Chang 和 Wei-Ling Chang。

Director 负责确保本政策得到执行、采纳和遵守的日常责任，对象包括员工和所有其他代表道坦图英国监护处理个人信息的个人。

员工

所有员工及任何其他代表道坦图英国监护处理个人信息的个人，均有责任完全遵守本政策。

未能遵守本政策可能导致纪律处分或雇佣合同终止。

5. 数据保护原则

英国 GDPR 规定了若干关键原则，管辖道坦图英国监护如何处理个人信息。遵守这些原则有助于我们确保合法合规，并在数据保护方面建立良好实践。

原则规定个人信息必须：

- 以合法、公平和透明的方式处理（"合法性、公平性和透明度"）
- 为特定、明确和合法的目的而收集，且不以与这些目的不相容的方式进一步处理（"目的限制"）
- 充分、相关且限于必要范围（"数据最小化"）
- 准确，并在必要时保持更新（"准确性"）
- 保存时间不超过必要（"存储限制"）
- 以确保其安全的方式处理，采取适当的技术和组织措施（"完整性和保密性"）

英国 GDPR 要求我们能够证明我们遵守了这些原则。这被称为"问责原则"。

5A. 学生照片和图像的使用

道坦图英国监护在使用任何学生照片或图像用于宣传、推广材料或网站之前，将始终获取必要的同意。我们将采取保障措施，确保仅在获得家长和/或学生同意的情况下，并恰当地使用图像。

合法性、公平性和透明度

我们仅在存在合法依据的情况下处理个人信息。合法依据如下：

- 数据主体已同意处理
- 处理对于履行与数据主体的合同或订立合同是必要的
- 处理对于遵守我们所受的法律义务是必要的
- 处理对于保护数据主体或他人的重大利益是必要的
- 处理对于执行公共利益任务而言是必要的
- 处理对于追求道坦图英国监护或第三方的合法利益是必要的，除非此类利益被数据主体需要保护个人数据的利益或基本权利和自由所覆盖，尤其是在数据主体为儿童时。

我们仅在确定了上述列表中的合法依据，外加以下列表中的一项条件时，才会处理特殊类别数据：

- 数据主体已给予我们明确同意
- 处理对于行使或履行雇佣、社会保障和社会保护法律赋予道坦图英国监护的任何权利或义务是必要的
- 处理对于保护数据主体或他人的重大利益是必要的，且数据主体在身体上或法律上无法表示同意
- 处理对于法律索赔的确立、行使或辩护是必要的
- 处理出于重大公共利益的原因是必要的
- 处理对于评估员工工作能力是必要的

公平性原则意味着个人信息的使用方式应符合数据主体的合理预期。

英国 GDPR 将"同意"定义为"数据主体通过声明或明确的肯定行动，自愿给出的、具体的、知情的且不含糊的对其个人数据处理的意愿表示"。

当我们依赖同意作为处理个人信息的依据时，我们将确保数据主体能够像给予同意时一样容易地、随时撤回其同意。

我们将始终使用最合适的依据来处理个人信息。

透明度原则要求我们确保向数据主体提供的关于其个人信息将如何处理的任何信息，都应简洁、易于获取、易于理解且使用平实语言书写。

目的限制

我们将从一开始就明确收集个人信息的原因以及我们打算如何使用它。

我们仅为特定、明确和合法的目的收集个人信息，并且不会以任何与这些目的不相容的方式处理信息。

如果情况发生变化，我们打算将个人信息用于不同目的，我们将确保新用途是公平、合法和透明的。在使用个人信息用于新目的之前，我们将始终告知数据主体，并且如果原始目的所依赖的合法依据是同意，我们将重新获得该同意。

我们可能会与家长、学生、代理、寄宿家庭、学校、地方儿童服务部门或其他相关机构共享个人数据，只要这对于保障安全或教育目的是必要的，并符合数据保护法。

数据最小化

道坦图英国监护收集和处理的个人信息将是充分的、相关的，并且限于处理目的所必需的范围。

准确性

道坦图英国监护收集和处理的个人信息将是准确的，并在必要时保持更新，并且在我们被告知信息不准确时，将立即更正或删除。

所有员工在知悉任何个人信息不准确时，都必须更新所有相关记录。

存储限制

我们不会保留个人信息超过我们需要的时间。

我们仔细考虑保留个人信息的时间，并证明我们保留它的理由。我们的大多数保留期限由法律时限决定。例如，与所得税缴纳相关的个人信息。

我们制定了保留计划，详细说明了我们持有的个人信息类型、持有原因和保留期限。该计划是我们处理活动记录的一部分（请参阅第 12 节）。

我们定期审查我们持有的数据，并在不再需要时删除或安全销毁。

完整性和保密性

我们非常重视数据保护法下的责任，并将始终确保采取适当的安全措施来保护我们持有的个人信息。

这意味着我们将采取适当措施，防止个人信息遭到未经授权或非法的处理、意外丢失、破坏或损坏。

道坦图英国监护的员工有责任确保在其履行职责和任务过程中处理的个人信息的安全。

6. 保护个人信息安全

我们采取了适当的技术和组织措施，以确保安全地处理个人信息，并防止我们持有的个人信息意外或故意受损。

技术措施:

- 我们执行强密码策略;密码在适当间隔更换，不与他人共享或使用
- 我们确保包含个人信息的笔记本电脑、U盘/存储棒和其他便携设备经过加密
- 我们部署了防火墙、防病毒和反恶意软件
- 我们限制对系统的访问，因此只有那些工作需要的人才可以访问个人信息
- 电子方式持有的个人信息在每个工作日进行备份，使用 AES 256 密码强度加密
- 包含个人信息的纸质文件在不再需要时使用碎纸机安全销毁

组织措施:

- 我们在所有员工入职培训期间及之后每年提供数据保护意识培训
- 我们制定了适当的政策和程序，以确保我们的员工充分理解他们在数据保护法下的责任
- 我们确保我们的员工和任何其他代表道坦图英国监护处理个人信息的个人了解他们在数据保护法下的个人责任以及这些责任如何适用于他们的工作领域
- 我们迅速调查所有可疑的个人数据泄露事件；我们始终进行适当的外部通知（如适用），并寻求从事件中吸取教训以降低再次发生的风险
- 包含个人信息的纸质文件在不使用时安全锁存
- 包含个人信息的纸质文件在不再需要时使用碎纸机安全销毁
- 员工利用一切机会确保我们持有的个人信息准确并保持更新
- 员工不向任何未经授权的人员（无论是外部还是道坦图英国监护内部）披露个人信息
- 我们定期测试、评估和评估已实施措施的有效性，并根据测试结果（当它们指出需要改进的领域时）采取行动

7. 管理个人数据泄露

我们制定了管理和响应个人数据泄露的程序。

个人数据泄露是指导致个人数据遭到意外或非法破坏、丢失、更改、未经授权的披露或访问的安全漏洞。

个人数据泄露的例子包括：

- 将个人数据发送给错误的人
- 未经授权的第三方访问个人数据
- 包含个人数据的设备或器材丢失或被盗

所有可疑的个人数据泄露和安全事件必须立即向Director Meng-Ting Chang报告。所有个人数据泄露都将得到及时调查，并记录在我们的内部数据泄露登记册中。

Director Meng-Ting Chang负责决定是否需要将个人数据泄露向 ICO 和数据主体报告。

通知 ICO 和其他外部机构

如果个人数据泄露可能导致数据主体的权利和自由面临风险，我们将在意识到泄露后的 72 小时内通知 ICO。

我们可能被要求向其他外部机构通知个人数据泄露。例如，我们可能被要求通知警方或资助机构。Director Meng-Ting Chang负责批准所有外部通知。

通知数据主体

如果个人数据泄露可能导致数据主体的权利和自由面临高风险，Director Meng-Ting Chang将毫不延迟地将个人数据泄露情况告知数据主体。

在告知数据主体有关泄露信息时，我们将使用清晰、平实的语言提供以下信息：

- 泄露性质的详细信息
- 组织联系点的姓名和联系方式，数据主体如需进一步信息可与之联系
- 泄露可能造成的后果
- 为解决泄露已采取或建议采取的措施，包括为减轻可能的不利影响而采取的措施

8. 响应个人的请求("数据主体权利")

英国 GDPR 赋予数据主体多项关于其个人信息的权利。

这些权利包括：

- 要求获取我们持有的关于其个人信息的副本的权利
- 要求更正关于其不准确或不完整信息的权利
- 要求删除其个人信息的权利
- 要求限制其个人信息处理的权利

- 数据可携权
- 反对处理其信息的权利
- 如果对其个人信息的处理方式不满意，或认为其数据保护权利受到侵犯，向 ICO 投诉的权利

我们将尽力毫不延迟地响应所有请求，并在收到请求后的一个月内完成。在某些情况下，我们可能需要延长响应请求的时候限制。如果出现这种情况，我们会告知提出请求的个人并随时告知进展。

在响应请求之前，我们可能需要询问更多信息和/或核实请求者的身份。

上述权利可能存在例外情况；我们收到的每个请求都将根据具体情况进行审查。

9. 文件保留

我们不会保留个人信息超过我们需要的时间。

我们仔细考虑保留个人信息的时间，并证明我们保留它的理由。我们的大多数保留期限由法律时限决定。例如，与所得税缴纳相关的个人信息。

我们制定了保留计划，详细说明了我们持有的个人信息类型、持有原因和保留期限。该计划是我们处理活动记录的一部分（请参阅第 12 节）。

我们定期审查我们持有的数据，并在不再需要时删除或安全销毁。

10. 通过设计与默认方式实现数据保护

我们在所做的一切事情中预先考虑数据保护和隐私问题。这是英国 GDPR 对我们的要求。

我们确保在设计和实施新的组织系统、服务或实践时，在开始之前就考虑数据保护问题。我们还确保，默认情况下，我们仅在必要时处理个人信息。

11. 数据处理者

每当我们使用第三方代表我们处理个人信息时，我们始终会进行适当的尽职调查，并确保签订数据处理协议。

我们只使用能向我们提供其安全措施充分保证的处理者。

12. 处理活动记录

道坦图英国监护根据英国 GDPR 第 30 条的要求，维护其处理活动记录。

该记录以电子格式保存，包含以下信息：

- 我们的组织名称和联系方式
- 我们处理的个人信息的描述
- 数据主体类别
- 处理目的
- 个人信息接收者
- 我们向其传输个人信息的任何英国以外国家或组织的名称，以及有关现有保障措施的信息
- 保留期限
- 我们技术和组织安全措施的总体描述（例如，加密、访问控制和培训）

我们定期审查我们处理的个人信息，并相应地更新此记录。

如果 ICO 要求，此记录将可供查阅。

13. 数据保护影响评估

数据保护影响评估是一个过程，帮助我们识别和最小化与涉及处理个人信息的项目、流程或活动相关的数据保护风险。

我们需要对任何可能导致个人面临高风险的处理进行 DPIA。我们也会对任何其他需要处理个人信息的主要项目进行 DPIA，因为这是良好实践。

DPIA 将：

- 描述处理的性质、范围、背景和目的

- 评估必要性、相称性和合规措施
- 识别和评估对个人的风险
- 识别任何减轻这些风险的额外措施

我们将记录 DPIA 的结果并实施已确定的措施。

14. 数据保护官的任命

根据英国 GDPR 第 37 条，如果满足以下条件，控制者和处理者需要任命数据保护官：

- 处理由公共机构或团体执行
- 控制者或处理者的核心活动包括需要对个人进行大规模定期和系统监控的处理操作
- 控制者或处理者的核心活动包括大规模处理特殊类别数据或与刑事定罪和犯罪相关的个人数据

我们组织的状况和处理活动的范围意味着我们不需要任命数据保护官。

如果我们的处理活动发生变化，我们将持续审查此决定。

15. AEGIS

作为黄金标准认证过程的一部分，道坦图英国监护需要向 AEGIS 办公室发送其所有寄宿家庭和合作学校的联系方式副本。他们还将提供学生姓名。这些数据由 AEGIS 安全持有，并在检查过程结束后销毁。

16. 审查

我们承诺对各项政策及相关良好实践规范进行至少每年一次的定期审查。

本政策最后审阅于 2026 年 1 月，审阅人：Limin Chen。