SCHEDULE 1: DATA SHARING AGREEMENT

Introduction

This document forms a Data Sharing Agreement between ImpactEd and the Subscriber for the transit and protection of Data provided by the Subscriber while using the ImpactEd Platform. This Agreement outlines the purpose of Data sharing, the protections taken by ImpactEd and the roles and responsibilities of ImpactEd and the Subscriber.

Data Movement Overview

ImpactEd operates a secure, cloud-based Platform which processes Data in order to support school-led monitoring and evaluation. Personal Data processing takes place through the Platform and is protected through a number of mechanisms:

- All Data is encrypted in motion (256-bit SSL/TLS) and at rest (128-bit AES)
- All HTTP requests are made over HTTPS using SSL encryption
- All Personal Data is processed within the European Economic Area or under adequacy arrangements approved by the European Commission as offering equivalent levels of protection unless the Subscriber provides prior written consent otherwise

Data is processed relating to school staff and students (see details below). On setup, staff Data is provided to Administrators for the purposes of setting up User accounts. This can then be amended as new staff members are added to the Platform, or existing staff details are updated.

Student Data takes two forms. Enrolment Data relates to the variables required to setup students on the platform. This is transferred securely from school MIS to the Platform through a REST API or via an encrypted spreadsheet template accessed within the Platform, and can be updated as required by the Subscriber within the Platform. Self-Assessment Data relates to student responses to surveys taken through the Platform, which are generated and stored within the Platform, and can be exported by Users as needed.

Transfer and Use of Personal Information

Data is processed for (i) offering the monitoring and evaluation services provided by the Platform and (ii) anonymised research and statistical purposes to provide improvements to the Platform. ImpactEd will only process Data provided by the Subscriber or any User (i) in accordance with the written instructions of the Subscriber (including this Agreement) or (ii) where required to do so by applicable law, court, regulatory process or regulation, in which case ImpactEd shall, to the extent permitted by the Data Protection Legislation inform the Subscriber of that legal requirement before the relevant processing of the affected Data.

The data areas processed can be reviewed by the Subscriber at any time within the Platform, and a current list is provided below. While the Subscriber may determine access to the Data being processed at its sole discretion, the functionality of the Platform may be affected by Subscribers not providing specific fields.

ImpactEd will comply with all obligations and procedures set out under the Data Protection Legislation. Except as expressly stated, the Subscriber is the Controller and ImpactEd is the Processor.

Data Security and Processing Obligations

ImpactEd will implement and maintain all appropriate technical and organisational security measures: (i) to ensure a level of security appropriate to the risk to the Data when it is processed by ImpactEd including, as appropriate, the measures referred to in Article 32(1) of the GDPR, and (ii) to assist the Subscriber in the fulfilment of its obligations to comply with the Data Protection Legislation.

ImpactEd will:

- comply with all applicable requirements of the Data Protection Legislation
- take all reasonable steps to ensure that access to the Data is limited to those personnel who require access to it for the purpose of complying ImpactEd's obligations under this Agreement and that such personnel are bound by enforceable obligations of confidentiality, shall be in possession of a valid Disclosure and Barring Service (DBS) certificate, and shall receive regular training relating to their obligations under the Data Protection Legislation;
- promptly, and in any event within 24 hours of becoming aware of any breach of security leading to, or reasonably believed to have led to, the accidental or unlawful destruction, loss, alteration, damage, unauthorised disclosure of or access to the Personal Data notify the Subscriber of the Security Breach and provide the Subscriber with details of the Security Breach;
- not process the Personal Data in any country which is either outside the European Economic Area or does not have adequacy arrangements approved by the European Commission as offering equivalent levels of protection without the prior written consent of the Subscriber;
- at the Subscriber's election, delete, amend, transfer or return all Personal Data to the Subscriber, and delete all existing copies unless applicable law requires their retention, in each case within 30 working days of such request;
- make available to the Subscriber all information reasonably necessary to demonstrate compliance with the obligations set out in Article 28 of GDPR, including the conduct of data protection impact assessments, subject access requests and requests for exercising a Data Subject's rights under the Data Protection Legislation, and allow for and contribute to audits, including inspections, reasonably conducted by the Subscriber or its representatives, in each case solely in relation to ImpactEd's processing of Personal Data;
- promptly inform the Subscriber if it is asked to enter into Data processing activities which may infringe either Parties' obligations under the Data Protection Legislation;
- employ an authorised Data Protection Officer, who may be reached at hello@impacted.org.uk;
- treat the appointment of any new Subprocessors according to ImpactEd's Terms and Conditions.

The Subscriber will:

- comply with all applicable requirements of the Data Protection Legislation
- have at all times during the term of this Agreement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to protect any Data;
- ensure that it has necessary licences and permissions from Data Subjects where required;
- ensure that adequate privacy notices describing the Data processing are provided to Data Subjects as required;
- ensure that it has an applicable legal basis for the transfer of Data to ImpactEd and to the processing of that Data by ImpactEd; and
- indemnify on demand, defend and hold harmless ImpactEd against all loss, liability, damages, costs, fees, claims and expenses which ImpactEd may incur or suffer by reason of any breach of the Data Protection Legislation by the Subscriber.

Technical Safeguards

ImpactEd takes a number of technical safeguards to protect Data processed in the Platform.

- All personal data originating from schools is transported and stored using best-practice encryption technologies. All HTTP requests are made over HTTPS using a high level of SSL security, monitored by an external service. All Data is protected by encryption, including 256-bit SSL/TLS encryption in motion and 128-bit AES at rest.
- ImpactEd's test suite is automatically run on every commit. This also checks all dependencies for security updates and blocks the build if any are found.
- All services are configured with individual passwords and permissions to limit access.
- All ports are locked down and only designated services are permitted to communicate with each other.
- Access to infrastructure is given on a need to know basis and is strictly limited to a list of authorised Administrators.
- Student-level data is only accessed on an anonymised basis by system Administrators. The only exceptions to this are where a Subscriber explicitly grants access to inspect data, for example to provide technical support. Where this is the case, permission is on an 'as needed' basis and data access is revoked once the technical problem is resolved.

Data Lifecycle

Data will be processed for the duration of the Subscription Agreement. Upon termination or expiry of the Subscription Agreement, save where applicable legislation prevents this, all Personal Data will be fully anonymised and retained by ImpactEd for research purposes. ImpactEd hereby undertakes that no individual will be personally identified or identifiable by such retained and anonymised Data, and the Subscriber acknowledges that any anonymised Data does not fall under the protection of the relevant Data Protection Legislation. Prior to termination of the Agreement and the subsequent full anonymisation, the Subscriber will retain the option to access, export and delete Personal Data.

Data Shared

For the purposes of operating the Platform, the Platform requires specific personal information about school staff and students. The Subscriber may determine access to the Data being processed at its sole discretion, although the functionality of the Platform may be affected by Subscribers not providing specific fields. Please note that ImpactEd system Administrators are only able to access student-level data on an anonymised basis, expect where a Subscriber explicitly grants access to inspect data, for example to provide technical support. Where this is the case, permission is on an 'as needed' basis and data access is revoked once the technical problem is resolved.

This personal information is based on a range of criteria. An indicative overview of the data types shared is outlined below; school requirements and data availability mean that in many cases a lesser level of data than listed is actually transferred. A full list of fields processed is visible at all times within the Subscriber's data sharing dashboard provided by Wonde and is maintained at: http://tiny.cc/IEpermissions which should always be taken as the latest version of the Data processed. The Subscriber may approve or revoke data access at any time through the Wonde dashboard. Please note that denial of access to requested fields may affect or reduce Platform functionality, and that a large number of data fields are optional – usage of optional data fields will be at the discretion of the Subscriber based on planned usage of the Platform.

Overview of data types shared

Data pertaining to school staff:

- On-boarding Data to create a User Account (name and email address)
- Data relating to User activity and usage of the Platform, including internet protocol (IP) address used by the Users' devices to access the Platform, connection information such as browser type and version, operating system and platform, login details, and cookie numbers.

Data pertaining to school students:

- Enrolment data, such as name, gender and pupil premium status
- Assessment data, such as results in school examinations
- Self-assessment data: comprised of student responses to self-report questionnaires as provided through the ImpactEd Platform
- School attendance and behavioural data
- Teaching group and form group data

Subprocessors

ImpactEd uses certain Subprocessors to assist it in delivering the Platform. ImpactEd requires its Subprocessors to satisfy the same Personal Data processing requirements as it has agreed to with the Subscriber. ImpactEd undertakes to use a commercially reasonable selection process by which it evaluates the security, privacy and confidentiality practices of proposed Subprocessors that will or may have access to or process Personal Data. ImpactEd shall remain fully liable to the Subscriber for the performance of the Subprocessor's Data protection obligations within the liability as outlined in our Terms and Conditions. The following page contains an up-to-date list (as of the date of this Agreement) of authorised Subprocessors used by ImpactEd to process Data: http://tiny.cc/IEsubprocessors.