Data Sharing and Processing Agreement

1. Purpose of this Agreement

1.1. This Agreement sets out the terms on which One Team Logic Limited, a company registered in England and Wales with registered number 09075059 (**OTL**) will process the Protected Data (as defined below) that it processes as a result of the Establishment's use of OTL's software product MyConcern® and forms part of the Contract (as defined below).

1.2. This Agreement is based around the principles of the Data Protection Laws, guidance[1] and advice[2].

2. Definitions and Interpretation

Applicable Law means:

- any law, statute, regulation, byelaw or subordinate legislation in force from time to time to which a party is subject and/or in any jurisdiction that services are provided;
- the common law and laws of equity as applicable to the parties from time to time;
- any binding court order, judgment or decree;
- any applicable industry code, policy or standard; or
- any applicable direction, policy, rule or order that is binding on a party and that is made or given by any regulatory body having jurisdiction over a party or any of that party's assets, resources or business;

Contract means the contract between OTL and the Establishment relating to the provision of MyConcern and associated services and includes the End User Licence Agreement, the Support and Maintenance Agreement, and this Data Sharing Agreement;

Data Controller has the meaning given to that term (or to the term 'controller') in Data Protection Laws;

Data Processor has the meaning given to that term (or to the term 'processor') in Data Protection Laws;

Data Protection Laws means as applicable and binding on the Establishment, OTL and/or the provision of MyConcern:

(a) in the United Kingdom:

(i) the Data Protection Act 1998 and any laws or regulations implementing Directive 95/46/EC (Data Protection Directive); and/or

(ii) the GDPR, and/or any corresponding or equivalent national laws or regulations;

---

[1] Records Management Toolkit for Schools (Version 5) – Information and Records Management Society (Feb 2016) - http://www.irms.org.uk/images/resources/2016_IRMS_Toolkit%20for%20Schools_v5_Master.pdf

[2] Cloud (educational apps) software services and the Data Protection Act (Department for Education - October 2014)

(b) in member states of the European Union: the Data Protection Directive or the GDPR, once applicable, and all relevant member state laws or regulations giving effect to or corresponding with any of them; and

(c) any Applicable Laws replacing, amending, extending, re-enacting or consolidating any of the above Data Protection Laws from time to time;

Data Protection Losses means all liabilities, including all:

(a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and

(b) to the extent permitted by Applicable Law:

(c) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority;

(d) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and

(e) the reasonable costs of compliance with investigations by a Supervisory Authority;

Data Subject has the meaning given to that term in Data Protection Laws;

Data Subject Request means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;

End User Licence Agreement means the agreement between OTL and the Establishment that sets out the terms on which OTL grants a licence of MyConcern to the Establishment and its Users;

Establishment means the establishment named in the End User Licence Agreement;

GDPR means the General Data Protection Regulation (EU) 2016/679;

Personal Data has the meaning given to that term in Data Protection Laws;

Personal Data Breach means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;

processing has the meanings given to that term in Data Protection Laws (and related terms such as process have corresponding meanings);

Processing Instructions has the meaning given to that term in clause 6.1.1;

Protected Data means the Personal Data and Special Category Data relating to pupils, parents, guardians or carers of pupils, of the Establishment that is stored on, transferred to or entered into MyConcern by the Establishment or taken from the MIS system operated by the Establishment;

Special Category Data has the meaning given in Article 9(1) of the GDPR;

Supervisory Authority means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;

Support and Maintenance Agreement means the agreement for ongoing maintenance and support entered into between OTL and the Establishment;

Users has the meaning given to it in the End User Licence Agreement.

In this Agreement:

(a) references to any Applicable Laws (including to the Data Protection Laws and each of them) and to terms defined in such Applicable Laws shall be replaced with or incorporate (as the case may be) references to any Applicable Laws replacing, amending, extending, re-enacting or consolidating such Applicable Law (including particularly the GDPR and/or the Revised UK DP Law) and the equivalent terms defined in such Applicable Laws, once in force and applicable; and

(b) a reference to a law includes all subordinate legislation made under that law.

3. Introduction

3.1. MyConcern® is OTL's web-based software and database package that helps educational establishments to report, record and manage safeguarding concerns. The MyConcern® database can be connected to other computer systems, such as the Establishment's Management Information System (MIS), for the purpose of sharing data between the systems to make users' experience better. Software components within MyConcern® extract the required information from the MIS and transfer it securely and in a uniform format to the desired location in MyConcern®, regardless of the source MIS.

3.2 The Information Commissioner's Office has provided specific guidance on data protection in a cloud-based environment, which can be accessed at https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

4. Roles and Responsibilities

4.1 As defined in the Data Protection Laws, OTL is acting as Data Processor and processes Protected Data on behalf of the Establishment, who is the Data Controller.

4.2 As Data Controller, the Establishment must ensure that Personal Data is:

4.2.1 processed lawfully, fairly and in a transparent manner,

4.2.2 collected for specified, explicit and legitimate purposes,

4.2.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed,

4.2.4 accurate and where relevant, kept up to date,

4.2.5 kept in a form that permits identification of Data Subject for no longer than is necessary for the purposes for which the Personal Data is processed, and

4.2.6 processed in a manner that ensures appropriate security of the Personal Data.

4.3 The Establishment is also responsible for ensuring that it has the ability to share data with OTL in accordance with this Agreement and that there are relevant measures in place to ensure the above criteria is met, including a responsibility to ensure that sufficient security measures are employed within the Establishment and/or on the devices which the Users are using to access MyConcern. Guidance is appended in Annex A at the end of this document.

4.4 The Establishment warrants, represents and undertakes, that:

4.4.1. it will comply with all Applicable Laws in respect of the Personal Data and Special Category Data;

4.4.2 will comply with the terms of this Agreement;

4.4.3 all data recorded by the Establishment for use in connection with MyConcern, prior to such data being provided to or accessed by OTL for the performance of the services under the Contract shall comply in all respects, including in terms of its collection, storage and processing (which

shall include the Establishment providing, where relevant, all of the required fair processing information to, and obtaining all necessary consents from, Data Subjects), with Data Protection Laws;

4.4.4 all instructions given by it to OTL in respect of Personal Data shall at all times be in accordance with Data Protection Laws; and

4.4.5 it has undertaken due diligence in relation to OTL's processing operations, and it is satisfied that:

(a) OTL's processing operations are suitable for the purposes for which the Establishment proposes to use MyConcern and engage OTL to process the Protected Data; and

(b) OTL has sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.

4.5 As Data Processor, OTL shall only process the Protected Data on the instructions from the Data Controller and its nominated user(s) at the Establishment as set out in clause 6.1.1. As Data Processor OTL will comply with security obligations equivalent to those imposed on the Data Controller itself.

4.6 Without prejudice to the Establishment's obligations under clause 4.4 above, OTL considers that for the purposes of the GDPR, the processing of the Protected Data is carried out on the following lawful grounds:

4.6.1 where the Protected Data consists of Personal Data then processing is taking place pursuant to Article 6(1)(c) of the GDPR as processing is necessary for compliance with a legal obligation to which the Establishment is subject;

4.6.2 where the Protected Data consists of Special Category Data then processing taking place pursuant to:

(a) Article 9(2)(b) of the GDPR as processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;

(b) Article 9(2)(c) of the GDPR as processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.

5. Use of Data

5.1 OTL will only collect and use Personal Data that is necessary for the performance of MyConcern. The data that is necessary (which will contain Protected Data) will be extracted from the Establishment's MIS and stored securely in the MyConcern® database, so that it can be accessed by Users.

5.2 The data fields (when available within the MIS) that may be extracted are:

- Unique identifier IDs;
- First name (preferred and legal);
- Surname (preferred and legal);
- Date of birth;
- Gender;
- Ethnicity;
- Religion;
- First language;
- Photograph of the pupil (if available on the MIS system);
- Year group;
- Registration group/class/house/division;
- Flag to indicate whether the pupil record is active within the MIS;

- Contact details for the pupil's home address and mobile number;
- Names and contact details for parents/carers
- Database IDs for siblings within the same establishment;
- Flags to indicate whether disability, medical condition, pupil premium, free school meals and in care flags are set in the MIS;
- Campus;
- Attendance.

5.3 The data fields listed in clause 5.2 have been agreed as the data fields necessary for MyConcern to perform. The data fields may be varied from time to time to be used only for the purpose of displaying information for the authorised users of MyConcern®. The Data Protection Officer, or other responsible person as notified to OTL in writing from time to time, in the Establishment will be notified by OTL of any changes made to the extracted data set.

5.4 The principal purpose for extracting data and storing it within MyConcern® is so that users can positively identify pupils within the Establishment and record concerns about them to comply with their legal obligations to record safeguarding concerns.

5.5 MIS data stored within MyConcern® database is kept up-to-date through a synchronisation process between MyConcern® and the MIS system on a daily basis. The MIS will always be the master record, so any inaccuracies within the MIS system will be transferred into MyConcern®. It is the responsibility of the Establishment to ensure that this data is accurate.

6. Data Processing

6.1 Insofar as OTL processes Protected Data on behalf of the Establishment, OTL:

6.1.1 unless required to do otherwise by Applicable Law, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Establishment's documented instructions ("**Processing Instructions**");

6.1.2 if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Establishment of any such requirement before processing the Protected Data (unless Applicable Law prohibits such information on important grounds of public interest); and

6.1.3 shall promptly inform the Establishment if the Supplier becomes aware of a Processing Instruction that, in the Supplier's opinion, infringes Data Protection Laws, provided that:

(a) this shall be without prejudice to the Establishments warranties and obligations in this Agreement;

(b) to the maximum extent permitted by mandatory law, OTL shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing in accordance with the Establishment's Processing Instructions following the Establishment's receipt of that information.

7. Data Retention

7.1 The arrangements for storing and archiving retained data will be agreed in advance with the Establishment. All Protected Data retained by OTL on behalf of the Establishment will be handled in accordance with the Applicable Laws and relevant statutory guidance[3].

7.2 Unless requested to delete, return or transfer data, OTL will archive/store data in accordance with the MyConcern Data Deletion Policy, which at all times complies with all Applicable Laws.

7.3 On receipt of a request to delete or return Protected Data, OTL will send to the Establishment confirmation of the request in writing.

7.4 OTL shall, if the Establishment confirms its request in writing, either delete or return all the Protected Data to the Establishment in such form as the Establishment reasonably requests within a reasonable time after the earlier of:

- the termination or expiry of the Contract; or
- the end of the provision of the relevant services related to processing; or
- once processing by OTL of any Protected Data is no longer required for the purpose of OTL's performance of its relevant obligations under this Agreement,

and delete existing copies.

8. Data Transfer

On receipt of a formal request from the Establishment's Data Protection Officer/authorised user, to transfer data to another education establishment, the data to be transferred will be made available and supplied in an agreed format. Examples of when a request for the transfer of data may be made include when pupils are leaving primary school to take up secondary education or when a pupil is moving from one school to another for other reasons and the two schools have agreed to share data between themselves.

9. Rights of Access

9.1 The data held in MyConcern® should be handled by you in accordance with the Establishment's Data Protection policy in the same way as any of the other Sensitive Personal Data held on paper or computer systems within the Establishment.

9.2 The Establishment's Data Protection Officer should respond to any requests for information held on MyConcern® in the same way that they would for any other Personal Data that you hold, using the Subject Access provisions to manage any such requests and applying the relevant exemptions should they apply (e.g. your Establishment would not disclose suspicions of physical abuse by a parent to that parent).

9.3 Given the nature of MyConcern and the purpose of the software, it is unlikely that OTL will receive any Data Subject Requests in respect of Protected Data. If OTL does receive such a request that it shall refer all such Data Subject Requests it receives to the Establishment within five Business Days of receipt of the request. If OTL receives more than three separate Data Subject Requests per calendar month, the Establishment shall pay OTL's reasonable costs calculated on a time and materials basis at OTL's then applicable rates.

[3] Including: Section 175 Education Act 2002; Limitation Act 1980; Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 – Guidance: "Dealing with Allegations of Abuse against Teachers and other staff" (November 2005).

9.4 OTL shall provide such reasonable assistance as the Establishment reasonably requires (taking into account the nature of processing and the information available to OTL) to the Establishment in ensuring compliance with the Establishment's obligations under Data Protection Laws with respect to:

- security of processing;
- data protection impact assessments (as such term is defined in Data Protection Laws);
- prior consultation with a Supervisory Authority regarding high risk processing; and
- notifications to the Supervisory Authority and/or communications to Data Subjects by the Establishment in response to any Personal Data Breach,

provided the Establishment shall pay OTL's Charges for providing the assistance in this clause 9.4, such Charges to be calculated on a time and materials basis at OTL's rates.

10. Data Security

10.1 OTL shall implement and maintain, at its own cost and expense, technical and organisational measures, taking into account the nature of the processing, that are necessary to ensure that the Protected Data is processed in accordance with the Data Protection Laws. In particular, OTL shall take all measures required pursuant to Article 32 of the GDPR;

10.2 When data is transmitted between the MIS and the MyConcern® database it is encrypted using appropriate Secure Sockets Layer (SSL) technology.

10.3 Once the installation of MyConcern® in your Establishment is complete, OTL does not have any access to the software that your Establishment is using unless access is specifically granted by an Authorised User of the Establishment. Furthermore, the Protected Data held within the database (data at rest) is encrypted and therefore not in a human-readable format, even to a database administrator who may have direct access to the database tables held on the servers used to host MyConcern.

10.4 The Establishment should not need to disclose any Protected Data to OTL. However, from time to time, OTL's support staff may be requested by your Establishment to assist with a technical issue. In these circumstances, and only at your request, OTL may use remote support tools, or on occasion, visit your Establishment to view the screen(s) that a user from the Establishment is viewing. The Establishment user should remain present during the entirety of the support session to supervise access to any Protected Data.

10.5 The Establishment should not send Protected Data to OTL directly.

10.6 OTL will not share, or permit anyone other than your Establishment and your Users, to view the Protected Data.

10.7 OTL's servers are located within the EEA and OTL will not transfer Protected Data outside of the EEA without the prior written authorisation of the Establishment.

10.8 OTL warrants that it will provide a secure and resilient hosting service – further information on security is available in OTL's security policy. The person responsible for security in OTL is the Director of Operations & Security. All OTL staff have been provided with the appropriate training regarding security and data protection.

10.9 The Establishment must, as a minimum, adhere to the basic steps stated in the attached questionnaire at Annex A. Whilst compliance may be seen as an additional burden, it is deemed to be in the best

interests of the Establishment, pupils/students and OTL that assurance is provided around the delivery of the end-to-end service and use of MyConcern®.

10.10 OTL shall not engage any sub-processor for carrying out any processing activities in respect of the Protected Data without the Establishment's written authorisation.

11. Record Information and Audit

11.1 OTL shall maintain, in accordance with Data Protection Laws binding on OTL, written records of all categories of processing activities carried out on behalf of the Establishment.

11.2 OTL shall, in accordance with Data Protection Laws, make available to the Establishment such information as is reasonably necessary to demonstrate OTL's compliance with its obligations under Article 28 of the GDPR (and under any Data Protection Laws equivalent to that Article 28), and allow for and contribute to audits, including inspections, by the Establishment (or another auditor mandated by the Establishment) for this purpose, subject to the Establishment:

11.2.1 giving OTL reasonable prior notice of such information request, audit and/or inspection being required by the Establishment;

11.2.2 ensuring that all information obtained or generated by the Establishment or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by Applicable Law);

11.2.3 ensuring that such audit or inspection is undertaken during normal business hours, with minimal disruption to OTL's business, and the business of other customers of OTL; and

11.2.4 paying OTL's reasonable costs for assisting with the provision of information and allowing for and contributing to inspections and audits.

12. Breach Notification

In respect of any Personal Data Breach involving Protected Data, OTL shall, without undue delay on discovering such breach:

- notify the Establishment of the Personal Data Breach; and
- provide the Establisment with details of the Personal Data Breach.

13. Liabilities and Indemnities

13.1 The Establishment shall indemnify and keep indemnified OTL in respect of all Data Protection Losses suffered or incurred by, awarded against or agreed to be paid by, OTL arising from or in connection with any:

13.1.1 non-compliance by the Establishment with the Data Protection Laws;

13.1.2 processing carried out by OTL pursuant to any Processing Instruction that infringes any Data Protection Law; or

13.1.3 breach by the Establishment of any of its obligations under this Agreement,

except to the extent OTL is liable under this clause below 13.2.

13.2 OTL shall be liable for Data Protection Losses (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with this Agreement:

13.2.1 only to the extent caused by the processing of Protected Data under this Agreement and directly resulting from OTL's breach of clauses 4-12 (inclusive); and

13.2.2 in no circumstances to the extent that any Data Protection Losses (or the circumstances giving rise to them) are contributed to or caused by any breach of this Agreement by the Establishment (including in accordance with clause 6.1.3(b).

13.3 If a party receives a compensation claim from a person relating to processing of Protected Data, it shall promptly provide the other party with notice and full details of such claim. The party with conduct of the action shall:

13.3.1 make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of the other party (which shall not be unreasonably withheld or delayed); and

13.3.2 consult fully with the other party in relation to any such action[, but the terms of any settlement or compromise of the claim will be exclusively the decision of the party that is responsible under this Agreement for paying the compensation.

13.4 The parties agree that the Establishment shall not be entitled to claim back from OTL any part of any compensation paid by the Establishment in respect of such damage to the extent that the Establishment is liable to indemnify OTL in accordance with clause 13.1.

13.5 This clause 14 is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

13.5.1 to the extent not permitted by Applicable Law (including Data Protection Laws); and

14.5.2 that it does not affect the liability of either party to any Data Subject.

14. More Information

If you require any further information, have any concerns, questions, or would like to make a complaint about OTL's data processing practices, please email dataprotection@oneteamlogic.co.uk.

15. Agreement

In order to use MyConcern, your Establishment must understand and accept this Agreement and confirm that you have taken adequate steps to protect Personal Data.

More information on your responsibilities for complying with the Data Protection Act can be found at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

Annex A: Security Questionnaire for Establishments

It is suggested that the Establishment reviews its IT Security Policy using the following questionnaire as a guide to ensure that personal data is protected from within the Establishment's own network.

What is the Establishment's policy in relation to...	Brief Explanation
End Point Security?	Endpoint security is an approach to network protection that requires each computing device on a network to comply with certain standards before network access is granted. When a client attempts to log onto the network, the user's credentials should be validated and the device scanned to make sure that it complies with defined security policies before allowing access to the network. Required elements may include an approved operating system, a VPN client and anti-virus software with current updates. Devices that do not comply with policy should be given limited or no access.
Media Controls?	To control the use of removable media access onto a network to reduce the possibility of virus and malware infection. This may include restricting USB port access or CD/DVD drive use and or ensuring that any media is checked and scanned for malicious software.
Account Management?	The management of user accounts or access to shared information or network services should be tailored on a "Need to Know" basis e.g. Normal User/Privileged User. There should be a policy in place that covers access controls for external accounts as well as those managed centrally.
Credentials?	This refers to the creation of a unique user name and password that only allows access to the correct authorised users. A strong password creation and renewal policy should also be in place e.g. minimum number of both uppercase/lower case alphanumeric characters including symbols like hash, full stop, etc.
Destruction of Hardware and Media?	This refers to the destruction and disposal of any hardware or media that has contained information relating to sensitive data.
Audit of Users?	This refers to the capture of data/information of a user's interaction with a system (System & Event log); this then provides an audit trail of usage that can be reviewed in line with your IT policy.
Patching and Anti-Virus?	A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance. AV (Anti-Virus) software should be updated as soon a new release is available to reduce the threat to the system/applications. A patch management strategy and a plan of what patches should be applied to which systems at a specified time should be in place.
Hardware Controls?	Refers to the controlling the use of ports (Port Lockdown) to limit or stop access and egress of data from a system i.e. Port 80 for internet access.

What is the Establishment's policy in relation to...	Brief Explanation
Physical Access?	Refers to the physical ability to gain access to Hardware/Firewalls/Routers and other sensitive equipment and the controls that are in place to reduce unauthorised access.
Printing Controls?	Refers to printing information to a known printer and its location (preferably in line of sight).
Timed Lockout?	Ensuring the user is redirected back to the login screen after a set period of inactivity.
Screensaver Lockout?	As above
Utilisation of Firewalls?	Firewalls are designed to block unwanted intrusion into your network. Have you configured your firewall to only allow the services and ports that your Establishment needs to conduct its daily business? Your firewall must be correctly configured and managed, with access to it controlled/restricted.
Mobile User Devices?	If you are accessing MyConcern® from a mobile device, such as a tablet or smart phone, you should ensure that the appropriate user and access controls are in place. The device should as a minimum: • Have a PIN to unlock and activate the device; • Be kept up to date with IOS refreshes and updates; • Be set to lock out after 1 minute's lack of user activity • Be kept secure and used in controlled environments.