Data Protection Impact Assessment (MyConcern)

Greenfield Primary School operates a cloud based system or 'hosted solution', called MyConcern. Access to MyConcern is through the internet. Resources are retrieved from MyConcern via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to MyConcern is through a web browser. As such Greenfield Primary School must consider the privacy implications of such a system. The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

Greenfield Primary School recognises that using a 'hosted solution' has a number of implications. Greenfield Primary School recognises the need to have a good overview of its data information flow.

The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for a cloud based system and the impact it may have on individual privacy.

The school needs to know where the data is stored, how it can be transferred and what access possibilities the school has to its data. The location of the server is important to determine applicable law. The school will need to satisfy its responsibilities in determining whether the security measures the cloud provider has taken are sufficient, and that the rights of the data subject under the GDPR is satisfied by the school.

Greenfield Primary School aims to undertake a review of this Data Protection Impact Assessment on an annual basis. A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA.
2. Describe the information flow.
3. Identify data protection and related risks.
4. Identify data protection solutions to reduce or eliminate the risks.
5. Sign off the outcomes of the DPIA.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
What is the aim of the project? – My Concern is a software system which enables the recording and sharing of safeguarding information, including attendance and behavioural information of children and families at our school. The system is capable of being connected to other computer systems for the purpose of sharing data between systems to make users' experience better. Software components within MyConcern can extract the required information from the school's management information system and transfer it securely and in a uniform format to the desired location in MyConcern. By using MyConcern the school will address these issues. https://www.myconcern.co.uk/our-privacy-policy/ The system will be for internal use only and there will be no sharing of information with outside agencies. Information will be shared only as appropriate with parents, teachers and teaching assistants. MyConcern is a hosted system which means that all updates, maintenance and management can be performed in a central location by One Team Logic Ltd *(the owners of MyConcern)*. The platform enables Greenfield Primary School to improve their management of child safeguarding Information, including attendance and behavioural information, whilst reducing staff time, paperwork and administration. The platform enables Greenfield Primary School to centralise the data, share information with parents and carers by improving the level of granularity of data and relevant agencies. A meeting held with relevant parties can all be recorded on the system, in a safe, secure and searchable method. Recording sensitive pupil information electronically is password protected which will help mitigate against the risk of a data breach with the appropriate controls in place.

Greenfield Primary School will undertake the following processes:

1. Collecting personal data
2. Recording and organizing personal data
3. Storing personal data
4. Copying personal data
5. Retrieving personal data
6. Deleting personal data

By opting for MyConcern the school aims to achieve the following:

1. Management of sensitive pupil information in one place
2. Security and integrity of sensitive data through a secure document vault
3. Storage of information electronically rather than manually
4. Recording information and building a chronology around the pupil
5. Providing bespoke reports for difference audiences, e.g. Parents or agencies
6. Identifying trends and patterns
7. Ability to add information from staff across the school
8. Secure access across all devices wherever the setting

Cloud based systems enable the school to upload documents and other files to a hosted site to share with others within school. These files can then be accessed securely from a PC in the school.

MyConcern cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated accordingly.

The school is the data controller and One Team Logic Ltd is the data processor.

Greenfield Primary School has included MyConcern within its Information Asset Register.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
The Privacy Notices (pupil) for the school provides the legitimate basis of why the school collects pupil data. Specifically this relates to health and safety and safeguarding of vulnerable groups. MyConcern will be specifically referenced in the school's Privacy Notice (pupil). **How will you collect, use, store and delete data?** – MyConcern collects information from pupil records, Special Educational Needs (SEN) records, Education Health Care Plans (EHCP). Personal data concerning health is included which under data protection law is considered special category data. A manual export of information is required from the schools Management Information System which is then uploaded via a secure transfer method to the platform's portal. The information will be stored in the platform. The information is retained according to the school's Data Retention Policy. **What is the source of the data? –** Safeguarding records, SENCO records, Education Health and Care Plans, Pupil Records, and Common Assessment Framework. **Will you be sharing data with anyone?** – Greenfield Primary School may share information with the Designated Safeguarding Leads, Safeguarding and SEND professionals including the SENCo, Headteacher, Senior Leadership Team (SLT), Governors, Ofsted and local authority professionals. However, this does not mean that Greenfield Primary School shares MyConcern access to the third parties. **What types of processing identified as likely high risk are involved?** – The information is transferred securely from the school to the server which is hosted remotely on a server within the United Kingdom. Access to information on MyConcern is controlled through passwords and access controls.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
What is the nature of the data? – Pupil data relates to the name of the child, date of birth, gender and class group. Data also includes middle name and UPN. MyConcern contains electronic records of the work of the School in identifying SEND needs, monitoring progress and outcomes. **Special Category data?** – Data revealing medical details is collected by the school and contained in MyConcern. It may also include safeguarding, SEND and behaviour information. The lawful basis for collecting this information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.* **How much data is collected and used and how often?** – Personal details relating to pupils are obtained from parent/pupil information systems. Additional content is obtained from classroom/teacher observation/agency partners. One Team Logic will only collect and process data, including special category data, on behalf of the school that is necessary for the performance of MyConcern. Special category may be entered directly into MyConcern by the school or it may be electronically transferred into MyConcern. **How long will you keep the data for?** – The school follows the good practice in terms of data retention as set out in the IRMS Information Management Toolkit for Schools and also as set out within the school's data retention policy. Special category data is transferred to the receiving school as part of the pupil record. This is signed for by the receiving school. This is then kept by the receiving school from DOB of the child + 25 years then reviewed. MyConcern will allow export of the data from the platform which can then be shared with the receiving school as part of the pupil transfer process. **Scope of data obtained?** – The scope of data will include the following: name of pupil, date of birth, age, gender, home address, phone number, e-mail address, location data, online identifier, UPN, SEN, first language, photograph of the pupil (management information system), year group, registration group/class/house/division, contact details for the pupil's home address and mobile number, names and contact details for parents/guardians, database IDs for siblings within the same school, flags to indicate whether the pupil is

disabled, medical condition, pupil premium, free school meals, and in care flags. Behaviour. Racial and ethnic origin. Religious belief. Physical or mental health or condition, biometric or genetic data.

The geographical area covered is from pre school to Year 6 pupils.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

What is the nature of your relationship with the individuals? – Greenfield Primary School collects and processes personal data relating to its pupils to ensure the school provides education to its students with teaching staff delivering the National Curriculum.

Through the Privacy Notice (Pupil) Greenfield Primary School is committed to being transparent about how it collects and uses data and to meeting its data protection obligation.

How much control will they have? – Not all staff will have access to safeguarding and SEND and behaviour information. MyConcern can restrict access so that only designated staff see information that is relevant to them. Access to the data held on MyConcern will be controlled by username and password. The platform will be used internally only from devices based within the school. Access to the platform can be revoked at any time.

Do they include children or other vulnerable groups? – All of the data will relate to children. The information will relate to safeguarding and SEND and behaviour information and ways to assist those children's individual needs.

Are there prior concerns over this type of processing or security flaws? – How is the information stored? Does the cloud provider store the information in an encrypted format? What is the method of file transfer? How secure is the network and what security measures are in place?

Greenfield Primary School recognises that moving from a manual system to an electronic system which holds sensitive personal data in the cloud raises a number of General Data Protection Regulations issues as follows:

- **ISSUE:** MyConcern will be storing personal data
  RISK: There is a risk of unauthorized access to information by third parties
  MITIGATING ACTION: One Team Logic hold Cyber Essentials Plus' certification, against which they are independently audited on an annual basis. Part of this audit involves external penetration testing of our own network and systems to prove that data is held securely

  One Team Logic will not have access to personal data held on the server unless access is specifically granted and authorised by the school

  Furthermore, personal 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

- **ISSUE**: Transfer of data between the school and the cloud.
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: One Team Logic Ltd use technical and organisational measures in accordance with good industry practice to safeguard the schools personal data, including the use of data encryption

  When personal data is transmitted between the school and MyConcern across a network, and when it is stored on the server, it will be encrypted using appropriate encryption algorithms

- **ISSUE:** Use of third party sub processors?
  RISK: Non compliance with the requirements under GDPR
  MITIGATING ACTION: One Team Logic will not engage another data processor for carrying out any processing activities in respect of the personal data without the data controller's (the schools) prior written consent and, if such consent is given, only provided if the other data processor agrees to be bound by the same terms as under the One Team Logic's data sharing agreement and remains liable for the acts of its subcontractors as if they were its own

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: Data is stored in UK secure Data Centres, with backups as standard. All MyConcern data is stored and processed only within the UK

- **ISSUE:** Cloud solution and the geographical location of where the data is stored
  RISK: Within the EU, the physical location of the cloud is a decisive factor to determine which privacy rules apply. However, in other areas other regulations may apply which may not be Data Protection Law compliant
  MITIGATING ACTION: In operating the MyConcern website it will only transfer data that is collected from the data controller to secure data centres in the UK for processing and storing

  According to the data sharing agreement One Team Logic will not transfer any personal data to any country outside the United Kingdom or to any international organisation without the school's prior written consent and, if consent is given, then only strictly in accordance with the schools instructions

  For EU Data Controllers, data held outside of the EEA shall be subject to contracted Model Clauses as defined in the OTL-SD44 Brexit Schedule – Standard Contractual Clauses

- **ISSUE:** The right to be informed; the right of access; the right of rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object
  RISK: The school is unable to exercise the rights of the individual
  MITIGATING ACTION: MyConcern Privacy Policy states the various legal rights of the data subject to their personal data and that if those rights wished to be exercised then this should be made in writing providing enough information to identify the data subject in order for MyConcern to respond to the request

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: GDPR non-compliance
  MITIGATING ACTION: The school is responsible for adding and deleting data from the MyConcern platform, the arrangements for storing and archiving retained data will be agreed in advance with the school. Additionally, MyConcern Privacy Policy states that it will only keep personal data for as long as is needed and for the purposes set out in the policy; it is the school's responsibility to inform One team Logic should they need to make changes

  Within the data sharing agreement it states unless requested to delete, return or transfer data by the data controller, One Team Logic will archive/store data in accordance with the MyConcern Data Deletion Policy, which at all times complies with all Applicable Laws

  On receipt of a request to delete or return Protected Data, One Team Logic will send to the data controller (school) confirmation in writing

One Team Logic shall, if the customer (the school) confirms its request in writing, either delete or return all the protected data to the customer in such form as the customer reasonably requests within a reasonable time after the earlier of for example; termination or expiry of the contract, end of the provision of relevant services related to processing, or processing is no longer required in respect to the fulfillment of the contract

- **ISSUE:** Responding to a data breach
  RISK: GDPR non-compliance
  MITIGATING ACTION: In respect of any personal data breach involving personal data, One Team Logic without undue delay upon discovering such breach notify the school of the data breach

  The school will recognize the need to define in their contract with One Team Logic Ltd a breach event and procedures for notifying the school and the school managing it

- **ISSUE:** Data is not backed up
  RISK: GDPR non-compliance
  MITIGATING ACTION: Data is stored in UK secure Data Centres, with backups as standard. All MyConcern data is stored and processed only within the UK

- **ISSUE:** No deal Brexit
  RISK: GDPR non-compliance
  MITIGATING ACTION: Data is stored in UK secure Data Centres, with backups as standard. All MyConcern data is stored and processed only within the UK

- **ISSUE:** Subject Access Requests
  RISK: The school must be able to retrieve the data in a structured format to provide the information to the data subject
  MITIGATING ACTION: MyConcern Privacy Policy states the various legal rights of the data subject to their personal data and that if those rights wished to be exercised then this should be made in writing providing enough information to identify the data subject in order for MyConcern to respond to the request

- **ISSUE:** Data Ownership
  RISK: GDPR non-compliance
  MITIGATING ACTION: As Data Controller the school maintains ownership of the data. One Team Logic is the data processor

  As data processor, One Team Logic will only process personal data on the instructions from the data controller (the school) and its nominated authorised user(s)

As data processor One Team Logic will comply with security obligations equivalent to those imposed on the data controller itself

- **ISSUE:** Cloud Architecture
  RISK: The school needs to familiarise itself with the underlying technologies the cloud provider uses and the implications these technologies have on security safeguards and protection of the personal data stored in the cloud
  MITIGATING ACTION: Data is stored in UK secure Data Centres, with backups as standard. All MyConcern data is stored and processed only within the UK

- **ISSUE:** GDPR Training
  RISK: GDPR non-compliance
  MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to MyConcern

- **ISSUE:** Security of Privacy
  RISK: GDPR non-compliance
  MITIGATING ACTION: One Team Logic Ltd is registered with the UK Information Commissioner's Office both as a data processor for our customers' data and as a data controller for our own company's data

  One Team Logic Ltd have attained two specific accreditations for information management. ISO27001 requires One Team Logic Ltd is required to comply with 114 individual controls covering every aspect of information management and security

  One Team Logic Ltd also hold the UK Government's 'Cyber Essentials Plus' certification, against which they are independently audited on an annual basis. Part of this audit involves external penetration testing of our own network and systems to prove that data is held securely

  One Team Logic will ensure that all One Team Logic personnel processing personal data are subject to a binding written contractual obligation with the data controller to keep the personal data confidential

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
The school moving to a cloud based solution will realise the following benefits: 1. Management of sensitive pupil information in one place 2. Security and integrity of sensitive data through a secure document vault 3. Storage of information electronically rather than manually 4. Recording information and building a chronology around the pupil 5. Providing bespoke reports for different audiences, e.g. Parents or agencies 6. Identifying trends and patterns 7. Ability to add information from staff across the school 8. Secure access across all devices wherever the setting

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
The views of senior leadership team will be obtained. Once reviewed the views of stakeholders will be taken into account The view of YourIG has also been engaged to ensure Data Protection Law compliance

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
The lawful basis for processing personal data is contained in the school's Privacy Notice (Pupil). The lawful basis includes the following: ▪ Health and Safety at Work Act ▪ Keeping Children Safe in Education ▪ Safeguarding Vulnerable Groups Act ▪ Working together to Safeguard Children Guidelines (DfE) The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law MyConcern will enable the school to uphold the rights of the data subject; the right to be informed; the right of access; the right of rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; and the right not to be subject to automated decision-making; these rights will be exercised according to safeguarding considerations. The school will continue to be compliant with its Data Protection Policy.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Data transfer; data could be compromised	Possible	Severe	Medium
Asset protection and resilience	Possible	Significant	Medium
Data Breaches	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium
Upholding rights of data subject	Probable	Significant	Medium
Data Retention	Probable	Significant	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
Data Transfer	Secure network, end to end encryption	Reduced	Medium	Yes
Asset protection & resilience	Data Centre based in the UK	Reduced	Medium	Yes
Data Breaches	Documented in contract and owned by school	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Upholding rights of data subject	Technical capability to satisfy rights of data subject	Reduced	Low	Yes
Data Retention	Implementing school data retention periods as outlined in the IRMS Information Management Toolkit for Schools	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Claire Stylianides	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Claire Stylianides	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Technical recommendations to be clarified with third party as follows: *(1) How is the information stored on the server? (e.g. is the server shared with other schools, what security is in place to maintain the integrity of the school's data?)* *(2) Where is the server located?* *(3) Is personal data stored in an encrypted format? (if not how is the information stored?)* *(4) What is the method of file transfer from school to the remote server and vice versa? (is it via a secure network?)* *(5) How secure is the network? (The school wishes to mitigate against the risk of compromise or unlawful access when personal data is transferred)security* *(6) What mitigating actions are put in place when appointing third party sub contractors* *(7) What security measures are in place? (firewalls, etc?)* *(8) How and when is data backed up?* *(9) Confirmation that personal data relating to MyConcern is kept on servers located in the UK including backup servers?*		
DPO advice accepted or overruled by:	Accepted	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	N/A	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Clare Benson	The DPO should also review ongoing compliance with DPIA