Data Protection Impact Assessment (Bounce Together)

Summerhill School operates a cloud based system or 'hosted solution', called Bounce Together. Access to Bounce Together is through the internet. Resources are retrieved from Bounce Together via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to Bounce Together is through a web browser. As such Summerhill 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. Summerhill School recognises that using a 'hosted solution' has a number of implications. Summerhill 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 UK GDPR is satisfied by the school.

Summerhill 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.

Contents

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? – Children's overall level of wellbeing impacts on their behaviour and engagement in school and their ability to acquire academic competence in the first place.

The culture, ethos and environment of a school influences the health and wellbeing of pupils and their readiness to learn.

Promoting physical and mental health in schools creates a virtuous circle reinforcing children's attainment and achievement that in turn improves their wellbeing, enabling children to thrive and achieve their full potential.

There is evidence to show that PSHE (Personal, social, health and economic) education can address teenage pregnancy, substance misuse, unhealthy eating, lack of physical activity, and emotional health.

Bounce Together provides schools with a survey platform for measuring and monitoring physical and mental wellbeing and the attitudes of pupils, staff and parents. Bounce Together is designed to not only collect wellbeing data but also in doing so endeavouring to make a difference to the individual.

Bounce Together is a hosted system which means that all updates, maintenance and management can be performed in a central location by Bounce Together Limited.

Bounce Together enables Summerhill School schools to improve its management of health and wellbeing for its students and workforce.

Understanding the mental health and wellbeing needs of the school's students is key to any whole school approach. The benefits of using Bounce Together for pupils are as follows:

(1) Gain a deep insight into pupils' mental health and wellbeing needs across key categories

(2) Identify key areas of concern to inform subsequent action plans at whole school, cohort, group or individual level

(3) Identify target pupils, run individual interventions and monitor progress over time
(4) Encourage pupils to express their thoughts and feelings in a safe environment

(5) Build objective data to support applications for additional funding or external support

(6) Build an understanding of the whole child beyond statutory academic data

Good staff wellbeing is essential for creating a mentally healthy school environment. It is recognised that teachers can have as much influence on pupils' happiness as they can on academic outcomes. The benefits of using Bounce Together for staff are as follows:

(1) Gain confidential insights to help the school to measure progress and focus on the tangible, practical actions that will make the most difference in school

(2) Encourage and develop 'Staff voice,' support job satisfaction and improve staff motivation and engagement

(3) Reduce recruitment and retention challenges

(4) Collect regular data to inform the whole school wellbeing strategy

(5) Demonstrate this commitment as required by Ofsted

(6) Making comparisons over time and evidence the impact of any initiatives or actions taken. Segment findings by age, gender, role and experience

(7) Support staff to become role models and prioritise their own mental health and wellbeing. A positive state of mind amongst adults in school has a constructive effect on pupils

Bounce Together is an intuitive system to help with the management of health and wellbeing amongst students and staff. Bounce Together allows the recording in one place sensitive information within an electronic format which is held securely on a remote server.

Summerhill 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 Bounce Together 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.

Bounce Together 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 Bounce Together is the data processor.

Summerhill School has included Bounce Together 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 lawful basis of why the school collects pupil data. Specifically this relates to health and safety and safeguarding of vulnerable groups. Bounce Together is referenced in the respective Privacy Notices.

How will you collect, use, store and delete data? – Bounce Together collects information from pupil records, Special Educational Needs (SEN) records, Education Health Care Plans (EHCP). Bounce Together links into Summerhill School Management Information System drawing pupil data into the application. The information will be stored on Bounce Together. The information is retained according to the school's Data Retention Policy.

What is the source of the data? – Pupil information is collected via registration forms when pupils join the school, pupil update forms the school issue at the start of the year, Common Transfer File (CTF) or secure file transfer from previous schools. Pupil information also includes classroom work, assessments and reports. SENCO records, Education Health and Care Plans, Pupil Records, and Early Help Assessment.

Bounce Together collects personal data from the school's management information system which is Arbor.

Will you be sharing data with anyone? – Summerhill School may share information with SEND professionals including the SENCo, Headteacher, Senior Leadership Team (SLT), Governors, Ofsted, the local authority, i.e. Educational Psychologist, Occupational Therapist and Speech and Language Therapist. However, this does not mean that Summerhill School shares Bounce Together access to the third parties.

What types of processing identified as likely high risk are involved? – Transferring 'special category' data from the school to the cloud. Storage of personal and 'special category data in the Cloud.

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 personal identifiers and contacts (such as forename and surname, date of birth, MIS number, unique pupil number, registration group, gender). Characteristics include additional funding indicators such as Free School Meals, eligibility to Pupil Premium, SEN Provision, and gifted.

Bounce Together contains electronic records of the work of the School in identifying SEN provision information and specific needs, monitoring progress and outcomes.

Workforce data relates to personal information (such as forename and surname, gender and date of birth) and basic staff details (staff ID, current employee status, job role).

School data include School Name, Governance Education, Phase Address, DFE ID LEA Sponsor.

Special Category data? – The lawful basis for collecting any data revealing racial or ethnic origin, medical details collected by the school and contained in Bounce Together which is considered as special category information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest and is authorised by domestic law.*

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. This also includes recorded information and reports.

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 the schools data retention policy.

Scope of data obtained? – How many individuals are affected (approximately 1052 for safeguarding issues and concerns) and for pastoral issues (approximately 1052). The geographical area covered is from Year 7 to Year 11.

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? – Summerhill 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.
It also collects and processes personal data relating to its pupils to manage the parent/pupil relationship. Personal data is collected for the workforce to assist reports, trends and profiling produced by Bounce Together.

Through the Privacy Notice (Student) and (Workforce) Summerhill 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 Bounce Together information. Bounce Together can restrict access so that only designated staff only see information that is relevant to them. Access to the data held on Bounce Together will be controlled by username and password.

Additionally whilst Bounce Together works on any device with access to the internet, staff that are granted access to the system will have to utilise an additional password to their own, which is only shared between authorized members of staff at the school.

Do they include children or other vulnerable groups? – All of the data will relate to children and the school's workforce. The information will relate to SEND, health plans, pupil attendance and assessment, etc.

Are there prior concerns over this type of processing or security flaws? – Bounce Together use a reputable, SOC2 and ISO:27001 accredited hosting provider - Microsoft Azure. Encryption is applied to every incoming/outgoing connection and the database is encrypted at rest and in transit.

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

- **ISSUE:** Bounce Together will be storing personal data
  RISK: There is a risk of unauthorized access to information by third parties
  MITIGATING ACTION: Bounce Together use a reputable, SOC2 and ISO:27001 accredited hosting provider - Microsoft Azure. Encryption is applied to every incoming/outgoing connection and the database is encrypted at rest and in transit.

  Bounce Together support industry methods of Single-sign-on. Access control, auditing and authorisation policies. Continuous network/security monitoring

  Microsoft designs, builds, and operates datacentres in a way that strictly controls physical access to the areas where your data is stored. Microsoft have an entire division devoted to designing, building, and operating the physical facilities supporting Azure. They maintain state-of-the-art physical security

  Microsoft takes a layered approach to physical security, to reduce the risk of unauthorised users gaining physical access to data and the datacentre resources. Datacentres managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacentre floor

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred
  MITIGATING ACTION: Data is transferred securely from a school's MIS (e.g. SIMS, Arbor, Bromcom etc) via Groupcall Xporter and through to Bounce Together.

  Bounce Together web traffic is secured via TLS and on top of this they also utilise third-party companies to employ WAF, DDOS Protection, Challenge Pages, Browser Integrity Checks and Edge SSL. Bounce Together use Transparent Data Encryption (TDE) with Azure SQL Managed Instance against the threat of malicious offline activity by encrypting data at rest. It performs real-time encryption and decryption of the data, associated backups, and transaction log files at rest. TDE performs real-time I/O

encryption and decryption of the data at the page level. The built-in server certificate is unique for each server and the encryption algorithm used is AES 256

- **ISSUE:** Understanding the cloud-based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: Bounce Together Ltd's servers are based within the United Kingdom. Personal data will never be processed outside the European Economic Area (EEA)

- **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: Bounce Together Ltd servers are hosted by Microsoft Azure data centres in the UK (South and West) to ensure school data is retained within the European Economic Area

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Bounce Together has the capability to provide the schools with access to the data stored within. Where Subject Access Requests are made for specific areas of school data Bounce Together can either provide, or will provide, means for authorised client users to carry out activities directly

  If the school wishes to exercise this right on behalf of a requestor is may contact Bounce Together support team on: support@bouncetogether.co.uk

  Bounce Together will process the request without undue delay and at the latest within 1 month, unless the request is complex or numerous in which case Bounce Together may take up to 3 months, but they will inform the school within 1 month if this is the case

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Bounce Together Ltd will only retain data on behalf of the school for the duration of the contract with Bounce Together. In the event that the contract ends all personal data is deleted

Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 compliant. For hard drives that can't be wiped, Microsoft use a destruction process that destroys it and renders the recovery of information impossible. This destruction process can be to disintegrate, shred, pulverize, or incinerate. We determine the means of disposal according to the asset type. Microsoft retain records of the destruction

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: BounceTogether shall inform the Customer in writing if, in BounceTogether's opinion, an instruction from the Customer infringes the Data Protection Legislation but only in relation to a breach of General Data Protection Regulation ((EU 2016/679)) and/or other UK data protection provisions and not jurisdictions outside of these areas

- **ISSUE:** Third party processor and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: The school is unable to exercise the rights of the individual
  MITIGATING ACTION: Bounce Together use sub-processors to store its data safely and securely. All survey data is stored in the EEA and all Bounce Together sub-processors have robust security features to ensure that they have the appropriate technical and organisation measures to keep personal data secure

  Bounce Together do not transfer school data to outside of the EEA. Any data (unless the school consent otherwise) is stored in the EEA at all times. The school may withdraw that consent at any time by contacting Bounce Together at support@bouncetogether.co.uk

- **ISSUE:** Data is not backed up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Bounce Together utilise Microsoft Azure's platform for data resilience and backups and it's encrypted at rest. Backups are taken every 10 minutes

  Bounce Together data is backed up in a separate physical premises with appropriate technical and organisational measures in place. This is to ensure that school data is not lost or destroyed should the original be destroyed without the school's instructions

  Bounce Together utilise Microsoft Azure and their scaling profiles. Currently, it is not automatically scaled on demand but it is monitored to ensure Bounce Together provide continuity and scaling changes can be made within 10 minutes

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Bounce Together servers are hosted in 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: Bounce Together has the capability to provide the schools with access to the data stored within. Where Subject Access Requests are made for specific areas of school data Bounce Together can either provide, or will provide, means for authorised client users to carry out activities directly.

  If the school wishes to exercise this right on behalf of a requestor is may contact Bounce Together support team on: support@bouncetogether.co.uk

  Bounce Together will process the request without undue delay and at the latest within 1 month, unless the request is complex or numerous in which case Bounce Together may take up to 3 months, but they will inform the school within 1 month if this is the case

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: As Data Controller the school maintains ownership of the data. Bounce Together is the data processor

- **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: Bounce Together Ltd through Microsoft Azure use multiple protective layers with the cloud platform to protect its services. These include encryption and firewalling. Microsoft carry out routinely vulnerability and penetration testing and promptly address any issues identified. This should be monitored to address any changes in technology and its impact on data. The school should maintain ownership of the Cloud technologies used ensuring the current and future technologies enable UK GDPR compliance

- **ISSUE:** UK GDPR Training

  RISK: UK GDPR non-compliance

  MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to Bounce Together

- **ISSUE:** Security of Privacy

  RISK: UK GDPR non-compliance

  MITIGATING ACTION: Bounce Together Ltd is registered with the ICO (registration number: ZA526338)

  Microsoft design and manage the Azure infrastructure to meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. Microsoft also meet country- or region-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate

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 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

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.

Bounce Together 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 in UK, ISO 27001 Certification	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 and data retention policy	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Vicki Poole	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Tim Harris	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) What is the 'upload' process? If through a website portal, how is the data secured in transit between the school and Bounce Together servers? i.e. Does the browser utilise TLS/SSL connections with AES-256bit encryption? (2) Is any data transferred or shared with partners or third-parties outside of the UK? (3) Should demand unexpectedly increase, can your server hosting service scale their facilities to meet demand? (4) What resiliency does the server hosting service provide for the availability of data? E.g. mirrored data centres, how often are backups taken and how long would it take to restore from an outage? Does the service manage all security updates for the service? (5) What is the data breach notification process?		
DPO advice accepted or overruled by: Accepted If overruled, you must explain your reasons		
Comments:		
Consultation responses reviewed by: If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by:	Vicki Poole	The DPO should also review ongoing compliance with DPIA