Data Protection Impact Assessment (SchoolsBuddy)

Caslon Primary Community School operates a cloud-based system, called SchoolsBuddy. Access to SchoolsBuddy is through the internet. Resources are retrieved from SchoolsBuddy via the Internet, through a web-based application, as opposed to a direct connection to a server at the school.

As such Caslon Primary Community 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. Caslon Primary Community School recognises that using a cloud-based system has a number of implications. Caslon Primary Community 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.

Caslon Primary Community 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? – Caslon Primary Community School operated a number of systems to manage payments, manage the provision of after school clubs, parent communications and wraparound care management. Information was held either electronically or manually. SchoolsBuddy is a comprehensive software system for staff, parents and pupils providing an online platform which enables Caslon Primary Community School to manage activities including after school clubs, online payments, parent communications, school bookings, trip consent and management and wraparound care management. SchoolsBuddy will help reduce staff time, paperwork and administration. SchoolsBuddy has the following features: *Activities Management:* SchoolsBuddy helps organise activity programmes from sign up, to allocation, communication and management with an intelligent preference-based system. *Online Payments:* Working alongside SchoolBuddys other features, the system links online payments with events & bookings, and can be used for all types of school payments. *Events, Sports and Trip Management:* Organise all types of school events including bookings, trips, and sports fixtures with online invitations, sign up, consent, payments and attendance registers. *Parents Evenings:* Manage online appointment bookings for parent teacher conferences / parents' evenings with a booking system to avoid parents making double bookings. *Transport and Dismissal Systems:* Create multiple lists for pre-school, after-school and post activities with in-app mobile attendance registers. *Parent Communications:* SchoolsBuddy has built-in parent communications via email and mobile apps, with personal calendar for each user. SchoolsBuddy are part of Faria Education Group. SchoolsBuddy is a product offered by the Faria Education Group to provide comprehensive mobile and web-based extra-curricular management system for activities management and online payments.

Personal data from the school (data controller) is submitted to SchoolsBuddy platforms in three ways:

(1) directly by the users

(2) by representatives authorised by the users (e.g. the school technology director obtains data and then uploads it to our platform)

(3) via an integration with a third-party system

Data typically enters SchoolsBuddy systems via "student information systems" - Integris independently maintained and controlled by the school. SchoolsBuddy import data from third-party systems only under direct instruction from the school.

SchoolsBuddy use personal data under their protection only when they receive direct instructions from the school. The data stored on SchoolsBuddy systems belongs directly to the school, and only a handful of SchoolsBuddy staff have access to personal data under strict confidentiality and security.

SchoolsBuddy process personal data independently only if it is vital to the integrity or security of the service, or to analyze or evaluate the quality of the service provided.

Caslon Primary Community 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 SchoolsBuddy the school aims to achieve the following:

1. Management of assessment pupil information in one place
2. Security and integrity of sensitive data through a secure password protected login.
3. Storage of information electronically rather than manually
4. Recording information and building a chronology around the pupil
5. Alerting staff and setting up reminders as appropriate
6. Providing bespoke reports for difference audiences, e.g. Governors or Ofsted
7. Tracking vulnerable groups and identifying trends

8. Ability to add information from Teachers and HLTA's and a small number of TA's across the school
9. Secure access across all devices wherever the setting

The school currently holds the information in hard and electronic copy formats. The school recognizes that having a manual record has the potential for third party access to sensitive data or loss of information as a result of fire and flooding. By purchasing an electronic system this goes some way to mitigate against this risk.

Cloud based systems enable the school to upload information to a hosted site to share securely with other members of staff. These files can then be accessed securely from any location or any type of device.

SchoolsBuddy is the data processor and cannot do anything with the school's data (the data controller) unless they have been instructed by the school. The schools Privacy Notice will be updated accordingly. Caslon Primary Community School has included SchoolsBuddy 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 The Children Act and subsequent amendments, The Education Act and subsequent amendments and The Childcare Act 2006.

How will you collect, use, store and delete data? – SchoolsBuddy collects information from the school's management information system and/or csv file. The information is retained according to the school's Data Retention Policy.

What is the source of the data? – School Pupil Data includes information obtained from schools and organisations supporting schools (i.e. local authorities, academy trusts and other education providers) including, in addition to pupil data provided by the DfE, details of which pupils are on-roll, absence information, pupil estimates and targets, teacher assessments, assessment results from tests, allocation to pupil groups and data in respect of which teachers taught particular pupils.

Department for Education (DfE) Pupil Data is provided to SchoolsBuddy by the DfE concerning current and former pupils including their name, date of birth, gender, language, ethnicity, school(s) attended, and the home census output area, school exam and assessment information, and any special educational needs and attendance and absence information.

Will you be sharing data with anyone? – SchoolsBuddy will not sell, exchange or otherwise distribute personal data to anyone without the consent of Caslon Primary Community School as the data controller. SchoolsBuddy Privacy Notice sets out the lawful basis for processing personal data including basis of legitimate interest.

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 UK. Access to information on SchoolsBuddy is controlled through passwords, with additional security to the most sensitive information.

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? – Details of which pupil are on-roll. Current and prior attainment data for each of the key stages covered by Caslon Primary Community School. Pupil absence information, pupil information from School Census, pupil estimates, targets and assessments and information on allocation of pupils to pupil groups. **Special Category data?** – The DfE Pupil Data and School Pupil Data SchoolsBuddy processes does include special categories of personal data. This data includes language, ethnicity and information about special educational needs and is used to ensure equality of opportunity and treatment. The lawful basis for collecting this information relates to Article 9 2 (b) *processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in respect to* The Children Act and subsequent amendments and The Education Act. The lawful basis is also covered by Schedule 1, part 2, paragraph 8 (Substantial Public Interest Conditions - equality of opportunity or treatment). **How much data is collected and used and how often?** – 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. It is reviewed termly and updated as necessary. The DfE also provides DfE Pupil Data. **How long will you keep the data for?** – SchoolsBuddy deletes personal data when instructed by the school, or if the contract between SchoolsBuddy and the school is terminated. The procedures around deleting school data upon termination of service are provided in the Terms of Service or in a Data Processor Agreement. An instruction to delete a user in SchoolsBuddy services can either be manually performed in the platform by a school representative or upon request to SchoolsBuddy support team. The school follows the good practice in terms of data retention as set out in the IRMS Information Management Toolkit for Schools and within the school's Data Retention Policy. **Scope of data obtained?** – How many individuals are affected 300. The geographical area covered is from Reception, and Year 1 to Year 6 210 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? – Caslon Primary Community School collects and processes personal data relating to its pupils to ensure the school provides education to its students delivering the National Curriculum. Through the Privacy Notice (Pupil) Caslon Primary Community 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 the software application. SchoolsBuddy provides secure role based access controls which is an approach to restricting system access to authorized users. Access to the data held on SchoolsBuddy will be controlled by username and password. Access to SchoolsBuddy can be revoked at any time. As a default, passwords must be changed every 90 days. The school will be able to upload personal data from its PC for the data to be stored remotely. Any changes made to files are automatically copied across and immediately accessible from other devices the school may have. **Do they include children or other vulnerable groups?** – All of the data will relate to children. The information will relate to assessment data including sensitive data. **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? Caslon Primary Community 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:** SchoolsBuddy will be storing personal data
  RISK: There is a risk of unauthorized access to information by third parties
  MITIGATING ACTION: Stored in multi-tenant encrypted SQL Server database. Row level security is implemented throughout the SchoolsBuddy solution. In terms of network security SchoolsBuddy uses firewalls and systems to detect suspicious behaviour, stop malicious attempts to gain access, or compromise the resilience of the service (e.g. DDOS attacks).

  SchoolsBuddy host with Microsoft Azure with the latest security patches available together with robust testing to ensure security. Access to SchoolsBuddy databases is via approved IP addresses only.

  Organisational security includes access policies, audit logs and confidentiality agreements. Physical security such as preventing unauthorized access to infrastructure processing personal data. Procedural security including IT management processes to minimize the risk of human errors, or testing regimes to identify software weaknesses before releasing new features to SchoolsBuddy cloud services, or policies to ensure data is only processed on instruction from SchoolsBuddy customers

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: All access to the SchoolsBuddy application is via SSL. SchoolsBuddy applies application security including traffic encryption, strongly hashed passwords, and additional safeguards against vulnerabilities such as cross site scripting, SQL injections, phishing and others

- **ISSUE:** Use of third party sub processors?
  RISK: Non-compliance with the requirements under GDPR
  MITIGATING ACTION: Unless SchoolsBuddy receive instruction/confirmation from the school or have a legal obligation to do so SchoolsBuddy will not share personal data with a third party. SchoolsBuddy take steps to prevent customers from sending data to third parties without complying with data protection regulations

- **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: Servers are located for schools in Dublin, Eire. All SQL Servers are encrypted

SchoolsBuddy will ensure that it implements appropriate data transfer mechanisms to protect the school's personal data. If data is transferred outside the EU, SchoolsBuddy will only transfer such data on the basis of a European Commission adequacy decision, Binding Corporate Rules or, the EU Model Clauses (Standard Contractual Clauses)

- **ISSUE:** SchoolsBuddy as a third-party processor and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: GDPR non-compliance
  MITIGATING ACTION: SchoolsBuddy acknowledges these rights and can assist in schools in meeting these requirements

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: GDPR non-compliance
  MITIGATING ACTION: SchoolsBuddy deletes personal data when instructed by the school, or if the contract between SchoolsBuddy and the school is terminated. The procedures around deleting school data upon termination of service are provided in the Terms of Service or in a Data Processor Agreement.

  An instruction to delete a user in SchoolsBuddy services can either be manually performed in the platform by a school representative or upon request to SchoolsBuddy support team

- **ISSUE:** Responding to a data breach
  RISK: GDPR non-compliance
  MITIGATING ACTION: Depending on the nature of the data breach, SchoolsBuddy customers might be required to promptly notify both the users affected and the Information Commissioners Office. SchoolsBuddy is required to notify its customers when becoming aware of a data breach, and to help them to fulfill obligations in notifying users

- **ISSUE:** No deal Brexit
  RISK: GDPR non-compliance
  MITIGATING ACTION: If required SchoolsBuddy can move data and applications to the Azure UK for UK only schools

- **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: School users have strong rights to transparency, information, and data access. Any data subject can request a copy of all personal data stored, provided that it does not adversely impact other users, or if the data is not already

directly available. If the school grant a data subject the right of access, SchoolsBuddy will, either through its software or its support services, help execute these rights.

SchoolsBuddy systems were built for transparency across all stakeholder groups, so the majority of data stored about a user is directly accessible via the individual user profile

- **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: SchoolsBuddy acknowledges these rights and can assist in schools in meeting these requirements

- **ISSUE:** Data Ownership
  RISK: GDPR non-compliance
  MITIGATING ACTION: SchoolsBuddy is the data processor and therefore does not decide the purpose or lawfulness of the data processed and stored. SchoolsBuddy are trustees acting on behalf of the school as data controllers. As data controllers, schools remain ultimately responsible for documenting and deciding how data enters SchoolsBuddy systems. However, GDPR regulations do impose new and stricter regulations on processors. SchoolsBuddy will fully comply with these requirements for all of its services, including SchoolsBuddy, ManageBac, OpenApply & Atlas, and Integration partners

- **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: This should be monitored to address any changes in technology and its impact on data to enable GDPR compliance

- **ISSUE:** Security of Privacy
  RISK: GDPR non-compliance
  MITIGATING ACTION: Faria Education Group is ISO/IEC 27001 certified (BSI under certificate number IS 664562). ISO 27001 demonstrates a commitment to information security at every level of the organisation.

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 for assessment will realise the following benefits: 1. Management of sensitive assessment data for pupils in one place 2. Security and integrity of sensitive data through a secure server 3. Storage of information electronically rather than manually 4. Recording information and building a chronology around the pupil 5. Alerting staff and setting up reminders as appropriate 6. Providing bespoke reports for difference audiences, e.g. Governors or Ofsted 7. Tracking vulnerable groups and identifying trends 8. Ability to add information from staff across the school 9. 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 and the Board of Governors 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: ▪ The Education Act ▪ The Childcare Act 2006 ▪ The Children Act The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law SchoolsBuddy 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 EU, Certified, ISO 270018	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:	Headteacher and Governors	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Headteacher and Governors	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? Stored in multi-tenant encrypted SQL Server database. Row level security is implemented throughout our solution. (2) To determine applicable data protection laws where is/are the servers located? Servers located for your schools in Dublin, Eire (3) Do you store the information in an encrypted format? All SQL Servers are encrypted. (4) What is the method of file transfer from school to the remote server and vice versa? *(Is it via a secure network?)* All access to the SchoolsBuddy application is via SSL. (5) How secure is the network? We host with Microsoft Azure with the latest security patches available together with robust testing to ensure security. Access to our databases is via approved IP addresses only. (6) What security measures are in place? *(Firewalls, etc.?)* See https://www.schoolsbuddy.com/terms/gdpr and links from this page. (7) SchoolsBuddy (parent company) has is ISO 27001 registered. Does it have any other accreditations such as Cyber Essentials Plus, etc? See https://www.schoolsbuddy.com/terms/gdpr & links from this page. (8) What contingency plans are in place in the event of a no deal Brexit? If required we can move our data and applications to the Azure UK instance for our UK only schools.		
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:	Headteacher and Governors	The DPO should also review ongoing compliance with DPIA