STUART BATHURST CATHOLIC HIGH SCHOOL

Data Protection Impact Assessment (Schoolcomms)

Data Protection Impact Assessment (Schoolcomms)

Cloud computing is a method for delivering information technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server at the school. Stuart Bathurst Catholic High School operates a cloud-based system called Schoolcomms. As such Stuart Bathurst Catholic High 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.

Stuart Bathurst Catholic High School recognises that moving to a cloud service provider has a number of implications. Stuart Bathurst Catholic High 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 considering 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 cloud 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. Stuart Bathurst Catholic High School aims to undertake this Data Protection Impact Assessment on an annual basis.

What is the aim of the project?

To help deliver a cost-effective solution to meet the needs of the business. The cloud-based system will enable the school to contact those with parental responsibility in a timely and efficient way.

Schoolcomms provides an online platform which enables [insert name of school] to improve communication and the management of key stakeholder engagement including parents, whilst reducing staff time, paperwork and administration.

Schoolcomms is a system which is modular in approach comprising of the following:

Stuart Bathurst Catholic High School uses the following systems: SIMs Messaging, Online Payments, Parental Engagement.

Schoolcomms Parent Communication: Schoolcomms enables communication by text and email with the addition of a two-way app messaging service. Schools can send out messages to parent groups at no charge. Parents will receive these messages in the app. Any parents not using the app will still get a regular text message, so it remains inclusive of parents not using smartphones.

There is an expectation that parents will be updated in a timely manner about anything that will impact upon their child whilst they are at the school. The most appropriate method to provide parents with this information is via Schoolcomms which will ensure that important messages are delivered to parents without reliance on the pupil.

The school may, for example, post details of school closure on its website or via a local radio station. However, there is no guarantee that this information may reach those with parental responsibility in a timely manner.

The text and email messaging service will only be used to inform parents of school activities and issues which may impact on the child. Consent has been identified as the lawful basis for processing personal data in the Stuart Bathurst Catholic High School Privacy Notice (Pupil).

This facility provides a free app, with parents being enabled to submit absence explanation and provides staff with access to a web-based management dashboard for staff to manage comms from anywhere.

Schoolcomms Cashless Payments: Parents can use the app to pay for dinners, clubs, trips, uniform and more. Items appear in the app, then they can pay using card, Bank Transfer or PayPoint.

Pupils will no longer have to carry cash into school so there's no chance of trip money going missing. Parents can check their available balance and receive reminders when it gets low, staff will be able to monitor payments and use a range of financial reporting features. This module of Schoolcomms integrates with all the leading cashless catering systems.

Schoolcomms Club Management: By managing clubs with Schoolcomms, parents always know which clubs are on and when schedules change, parents just check the app. Being able to manage attendance and registers helps with child protection during after-school hours. Staff can use the dashboard to set up as many clubs as they like, parents can book their preferred sessions with the app, and staff can set place limits to control numbers and generate digital or printed registers.

Schoolcomms Meals Management: Meal Manager from Schoolcomms is a paperless and cashless solution that increases efficiency in school. Parents can select meals and pay in advance online or on the app.

Smart technology allows classroom selection, providing an opportunity for food education in class. Visual support for younger children. Shows only safe options for those with special dietary needs. Supports FSM and UIFSM so parents are not charged. Kitchen receives reports of meals booked and numbers allowing them to minimise waste. Parents can keep track of what their child has eaten and are only charged for meals taken.

Schoolcomms Medical Tracker: Schools can manage important pupil medical information and interact with parents, should an injury in school take place. Integrated with School Gateway and the school's management information system, Medical Tracker can store student medical histories, specific care plans, immediately alert parents to bumps and scrapes, and monitor medicine expiry dates, creating an all-encompassing incident monitoring system.

Schoolcomms Parents Evening System: Provides an easy setup via integration with the school's management information system and connects with the School Gateway to provide parents with easy access to booking. The system can be linked with Schoolcomms' parent app. The system cuts down on admin time and reduces the chance of missed appointments. The Video Appointments module enables remote meetings with parents.

Schoolcomms provides an intuitive, online school management solution for primary schools, academies, and MATs. Schoolcomms is designed to make planning for leaders, managers and teachers' workloads more manageable, helping to impact positively upon teaching, learning and inclusion. Schoolcomms can fully integrate with leading schools' management ICT systems including SIMS, RM Integris, and Scholar Pack using Wonde as an Application Programme Interface.

Wonde and Third-Party Apps/Vendors

Wonde's core service is used by a large percentage of schools in the UK to control the Management Information System (MIS) data it shares with third party vendors used at the school. These vendors include solutions for assessment, maths, English, library management, parent communications, parent payments, Multi Academy Trusts, voucher systems, Google/Microsoft syncing, classroom content providers etc.

Wonde is ISO27001 accredited and the majority of schools use Wonde to manage their MIS data sharing and syncing with multiple third-party vendors. An overview of how schools do this can be found here https://www.wonde.com/school-data-management.

When a vendor (app), or vendors, requests to be connected to a school via Wonde - if the school approves that vendor(s) request and for Wonde to facilitate it, then Wonde will complete a base integration with the schools' MIS.

Wonde request (but do not extract) the permissions that are required for the majority of vendors that use its services. Wonde will then only extract and send data that has been approved by a school to send onwards to their chosen vendors. For clarity, Wonde does not extract data that is not approved by the schools for the vendors they are using.

Stuart Bathurst Catholic High School can reduce the requested Wonde permissions upon the integration taking place, and Wonde can assist schools with this. Stuart Bathurst Catholic High School also has the ability to change the permissions whenever it likes, but in doing so ensures that it has considered how that may affect its use of approved vendors (i.e. the flow of data to those vendors via Wonde for the vendors to provide the agreed service).

The school will be complying with Safeguarding Vulnerable Groups Act, and Working together to Safeguard Children Guidelines (DfE). Stuart Bathurst Catholic High School will undertake the following processes:

- Collecting personal data
- Recording and organizing personal data
- Structuring and storing personal data
- Copying personal data
- Retrieving personal data
- Deleting personal data

By opting for a cloud-based solution the school aims to achieve the following:

- Scalability
- Reliability
- Resilience
- Delivery at a potentially lower cost
- Supports mobile access to data securely
- Good working practice

Schoolcomms will enable the user to access information from any location or any type of device (laptop, mobile phone, tablet, etc).

The cloud service provider cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated especially with reference to the storing of pupil in the cloud.

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 and subsequent amendments.

How will you collect, use, store and delete data?

The information collected by the school is retained on the school's management information system. Schoolcomms also collects information from online contact forms, import of data from the school management information system, verbal and written from nominated administrator contact within the school. 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.

Will you be sharing data with anyone?

Stuart Bathurst Catholic High School routinely shares pupil information with relevant staff within the school, schools that the pupil attends after leaving, the Local Authority, the Department for

Education, Health Services, Learning Support Services, RM Integris and various third-party Information Society Services applications.

What types of processing identified as likely high risk are involved?

Transferring personal data from the school to the cloud. Storage of personal data in the Cloud

What is the nature of the data?

Schoolcomms holds information from customer schools about both pupils and employees for the purpose of providing a service in accordance with the terms and conditions for contracted services. This information is held and processed in compliance with the General Data Protection Regulation (GDPR).

The customer school remains the 'Data Controller' in respect of pupil data at all times. As such the school is obliged to ensure that the information provided is accurate and up-to-date. As part of the school's obligation as 'Data Controller', it must have identified a lawful basis to collect pupil personal data.

Pupil's Personal Data includes personal information such as achievement records, behaviour records, assessment records, full name, absence records, club attendance records, assessment reports, pupil premium status, linked contacts, groups from MIS system, dinner payments, club bookings, mobile number, email address, postal address, PIN, class, year group, pre-admission status, Schoolgateway transaction history, MIS ID, phone type (iOS/ Android), roll number, UPN, nationality, gender, FSM status, paypoint card number.

Schoolcomms uses pupil data to allow schools: (1) to monitor, track and report on pupil progress and attainment; (2) to provide relevant services (sending electronic school to parent communications, creating SEND documentation, etc), and (3) to perform analysis on pupil data (attendance and absence management, etc).

Schools Data: includes School ID, unique user ID, website URL, description, address, contact number, email address, billing address, billing email address, billing telephone number, purchased Schoolcomms products, DFE number, images, email attachments, bank account details, disbursement history, inbound SMS number, inbound email address, links shared with external websites, MIS system.

Staff: includes full name, username, memorable data, password, professional email address, role, dinner payments, personal email address, mobile number, PIN, phone type (iOS/ Android), Schoolgateway transaction history.

Schoolcomms use the employee data to: (1) allow suitable staff members to log in and use the Schoolcomms system, and (2) allow the school to perform relevant services (school wide employee emails, professional employee names on reports, etc).

Parents: includes full name, email address, mobile number, PIN, linked students, parental responsibility, prime parent status, SIMS priority number, postal address, phone type (iOS/ Android), bank details, Schoolgateway transaction history, messages sent to school via Schoolgateway app.

Cashless Retailers: includes retailer ID, retailer name, username, memorable data, password.

The information is sourced from Stuart Bathurst Catholic High School from the management information system either via manual import or automated transfer.

Special Category data?

Data revealing health, racial or ethnic origin, and religious beliefs are collected by the school and contained in Schoolcomms. 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 the field of employment and social security and social protection law in so far as it is authorized by domestic law (see section 10 of the 2018 Act) or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and interests of the data subject.*

How much data is collected and used and how often?

Personal data is collected for all pupils and their respective parent/guardians. Additionally, personal data is also held respecting school administrative contact details, school name and address, school e-mail address, school contact telephone number, and staff information (staff name, staff e-mail address, staff teaching groups).

How long will you keep the data for?

The school will consider the data retention period as outlined in the IRMS Information Management Toolkit for Schools

The school provides education to its students with staff delivering the National Curriculum

What is the nature of your relationship with the individuals?

Stuart Bathurst Catholic High School collects and processes personal data relating to its pupils and employees to manage the parent/pupil and employment relationship.

Through the Privacy Notice (pupil/workforce) Stuart Bathurst Catholic High 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?

Schoolcomms users (students, parents, staff) may have individual user accounts to log into Schoolcomms to retrieve communications.

Do they include children or other vulnerable groups?

All of the data will relate to children. The information will relate to free school meals, medical information, pupil attendance and behaviour, etc.

Are there prior concerns over this type of processing or security flaws?

All data kept on Schoolcomms servers are encrypted at rest using 256-bit Advanced Encryption Standard (AES) encryption. Schoolcomms secure identity server encrypts user access credentials that are required to access Schoolcomms. Schoolcomms are a Level 2 PCI-DSS certified organisation and operate an ISO27001 compliant security programme to help protect school data at all times.

In terms of application security, users (parents, pupils, staff) can log into the Schoolcomms IOS and android mobile applications and view user specific data. Schoolcomms have a number of options to control the level of access to data for a user.

Stuart Bathurst Catholic High School has the responsibility to consider the level and type of access each user will have.

Stuart Bathurst Catholic High School recognises that moving to a cloud-based solution raises a number of General Data Protection Regulations issues as follows:

ISSUE: The cloud-based solution will be storing personal data including sensitive information
RISK: There is a risk of uncontrolled distribution of information to third parties
MITIGATING ACTION: All accounts used within Schoolcomms attribute to a uniquely identifiable staff member. The only accounts that are shared are School "Support User" accounts used by

members of the support team and are individual to each school. The usage of these accounts is restricted to only Support team personnel and audit logs are recorded to prevent misuse

Failed logins to internal systems are recorded and users will be locked out after a varying number of attempts. Access to the Schoolcomms and Schoolgateway products is also denied after several failed login attempts

Schoolcomms has a password policy which ensures that all staff members are aware of the importance of a strong password. Schoolcomms policy ensures a strict password criterion is met including being over 10 characters in length and containing at least one upper case letter and one special character. Passwords must be changed every 3 months and old passwords cannot be re-used. Users are also prompted to change their password upon first login.

Account lockouts are in place to prevent brute force attacks. Accounts will be locked after a number of failed login attempts (between 3 and 5 depending on the system)

The password policy forbids the storage of passwords via plaintext documents. Employees are encouraged to use one of two authorised password manager applications to safely and securely store and share passwords internally. Passwords are currently hashed with SHA1

Access to secure systems and Schoolcomms VPN requires two factor authentications

Database access is strictly controlled and monitored. Access is protected by multi-factor authentication, available only via whitelisted dedicated management nodes, and subject to full audit trail logging. Only Database administrators and senior members of the IT tech team have any database access

Schoolcomms uses the SNORT intrusion detection system to detect suspicious activity on the network. It can also be used to identify and log failed login attempts, brute force attacks and other security events. Schoolcomms has implemented the Tenable.io system to scan for vulnerabilities within the infrastructure

Schoolcomms uses antivirus solutions provided by Trend Micro on all office workstations and servers

An automated patch management strategy is in place using ManageEngine Desktop Central to routinely distribute security patches and updates for Operating Systems and third-Party applications

ManageEngine Desktop Central is able to monitor and detect any unauthorised changes made to software installations. Snort IDS is able to inform of suspicious changes to the network. Tenable.io will reveal exposed vulnerabilities that are realised due to unauthorised changes

Annual penetration tests are conducted on the Schoolcomms and Schoolgateway applications

All Schoolcomms employees have had training specific to the GDPR and Data Protection to make sure they understand their obligations to Data Protection and the confidentiality of Personal Information

Schoolcomms have a number of Certified EU General Data Protection Regulation Practitioners (EU GDPR P) and Foundation levels (EU GDPR F), and all employees have undertaken a combination of eLearning courses and face-to-face workshops

ISSUE: Transfer of data between the school and the cloud
RISK: Risk of compromise and unlawful access when personal data is transferred
MITIGATING ACTION: To protect data in transit between Schoolcomms servers and the web browsers/mobile devices that run the Schoolcomms application, Secure Sockets Layer (SSL)/Transport Layer Security (TLS 1.1 and above) is used to create secure tunnel protected by 256-bit Advanced Encryption Standard (AES) encryption. Data in the Schoolcomms database is encrypted at rest using 256-bit Advanced Encryption Standard (AES) encryption

ISSUE: Use of third party sub processors?
RISK: Non-compliance with the requirements under UK GDPR
MITIGATING ACTION: Schoolcomms use a range of trusted service providers to help deliver their services. All of their suppliers are subject to appropriate safeguards, operating in accordance with Schoolcomms specific instructions and limitations, and in full compliance with Data Protection Law. These service providers include:

Payment Processors- to securely process bank transfer and card payments (Schoolcomms do not see, or store payment card details)

SMS Providers – to send out SMS notifications or messages sent by Customers using Schoolcomms Products and Services

Email Providers – to send out email notifications or messages sent by Customers using Schoolcomms Products and Services

Hosting Providers – to manage Schoolcomms secure enterprise datacentres

Security Providers – to protect Schoolcomms systems from attack

Telephony Providers – Schoolcomma might record calls for training, quality and security purposes

Support Portal (ZenDesk) – so that schools can easily ask for help

Wonde (Data Integrator) – so that schools can safely manage their data

Feedback Platforms (Optional) – working with SurveyMonkey

Schoolcomms may also have access to your personal information as part of delivering the service. If Schoolcomms need to change or add additional third parties, Schoolcomms will always update its Privacy Notice accordingly.

Schoolcomms will only disclose your information to other parties in the following limited circumstances; (1) where Schoolcomms are legally obliged to do so, e.g. to law enforcement and regulatory authorities, (2) where there is a duty to disclose in the public interest, (3) where disclosure is necessary to protect Schoolcomms interest e.g. to prevent or detect crime and fraud, and (4) where schools give Schoolcomms permission to do so e.g. by providing consent within the Schoolcomms Products and Services or via an online application or consent form

ISSUE: Understanding the cloud-based solution chosen where data processing/storage premises are shared?
RISK: The potential of information leakage
MITIGATING ACTION: Schoolcomms stores its data within Microsoft's Azure cloud infrastructure. This utilizes automatic 'scale up' features within Microsoft's Azure cloud platform

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 compliant with EU Data Protection Law
MITIGATING ACTION: The Schoolcomms Products and Services only processes your personal information in the UK. Schoolcomms data is stored in Edinburgh and London

ISSUE: Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
RISK: UK GDPR non-compliance
MITIGATING ACTION: Schoolcomms Privacy Notice states that data subjects have the right of access to their personal information that Schoolcomms process and details about that processing. This can usually be accessed directly within the Schoolcomms Products and Services (self-service).

However, should this not be possible, schools can raise a Data Subject Access Request (DSAR) to receive this information in another format

ISSUE: Implementing data retention effectively in the cloud
RISK: UK GDPR non-compliance
MITIGATING ACTION: Schoolcomms will only retain information for as long as is necessary to deliver the service safely and securely. Schoolcomms may need to retain some records to maintain compliance with other applicable legislation – for example finance, taxation, fraud and money laundering law requires certain records to be retained for an extended duration, in some cases for up to seven years

ISSUE: Data Back ups
RISK: UK GDPR non-compliance
MITIGATING ACTION: Backups of the Schoolcomms databases are taken on a regular basis. These are secured and encrypted to ensure that personal data is protected against accidental destruction or loss while hosted. Full database backups are tested on a monthly basis

Recovery point objective is 5 minutes. Recovery time objective will vary depending on the nature of the disaster. A full data recovery can be completed within 12 hours.

ISSUE: Business Continuity
RISK: The school needs to be satisfied that plans are inplace to ensure system resilience
MITIGATING ACTION: Schoolcomms operations and infrastructure is fully resilient and prepared to handle a comprehensive set of serious failures. These are exercised regularly through various mechanisms. Schoolcomms operates a secondary datacentre for use in a Disaster scenario. All critical systems are frequently backed up and replicated to the secondary site

System performance and resources are closely monitored on a 24x7x365 basis. Activity and utilisation are reviewed over time and the system is scaled accordingly to manage forecasted requirements

ISSUE: Responding to a data breach
RISK: UK GDPR non-compliance
MITIGATING ACTION: Low-level auditing software is run on all production systems to record potentially malicious actions that may take place. If Schoolcomms become aware of a security breach of users' Personal Data, Schoolcomms will notify affected users as required by applicable laws and may post a notice on the Services as required by applicable laws. Schoolcomms run regular vulnerability scans on its systems and network using a trusted third party

ISSUE: Post Brexit

RISK: UK GDPR non-compliance
MITIGATING ACTION: The Schoolcomms Products and Services only processes your personal information in the UK. Schoolcomms data is stored in Edinburgh and London

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: Schoolcomms Privacy Notice states that data subjects have the right of access to their personal information that Schoolcomms process and details about that processing

This can usually be accessed directly within the Schoolcomms Products and Services (self-service). However, should this not be possible, schools can raise a Data Subject Access Request (DSAR) to receive this information in another format

ISSUE: Data Ownership
RISK: UK GDPR non-compliance
MITIGATING ACTION: The school remains the data controller for any data shared by the school to Schoolcomms. If data needs to be added, deleted or updated, this is done by the school using their management information system. This means that Schoolcomms use the data to carry out a specific function on behalf of the school, i.e. sending school messages to parents. Schoolcomms will never add, delete or update any of the school's data unless the school specifically requests Schoolcomms to do so
Schoolcomms is the data controller for the data that does not belong to the school, which includes the information that is entered when a person creates an account in the Schoolcomms services

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: Schoolcomms stores its data within Microsoft's Azure cloud infrastructure which is managed in compliance with multiple regulations, standards and best-practices, including ISO/IEC 27001, and is a Level 2 PCI-DSS certified organisation

The Schoolcomms service is geo-redundant, which means it runs in multiple locations at once. This means that a failure in one service location would not affect the running of the service. Only in the event of multiple failures in disparate locations may the service be affected

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

ISSUE: Security of Privacy
RISK: UK GDPR non-compliance
MITIGATING ACTION: Schoolcomms are a Level 2 PCI-DSS certified organisation and operate an ISO27001 compliant security programme to help protect school data at all times

ISO 27001: is one of the most widely recognized, internationally accepted independent security standards. Data centres used by Schoolcomms have earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centres that make up its shared Common Infrastructure

Schoolcomms is registration with the ICO under the parent name ParentPay Ltd (registration number Z7380292)

The school moving to a cloud-based solution will realise the following benefits:

- Scalability
- Reliability
- Resilience
- Delivery at a potentially lower cost
- Supports mobile access to data securely
- Good working practice

The views of senior leadership team and the Board of Governors will be obtained. Once reviewed the views of stakeholders will be considered

The view of YourIG has also been engaged to ensure Data Protection Law compliance

The lawful basis for processing personal data is contained in the school's Privacy Notice (Pupil and Workforce). The Legitimate basis includes the following:

- Childcare Act 2006 (Section 40 (2)(a)
- The Education Reform Act 1988
- Further and Higher Education Act 1992,
- Education Act 1994; 1998; 2002; 2005; 2011

- Health and Safety at Work Act
- Safeguarding Vulnerable Groups Act
- Working together to Safeguard Children Guidelines (DfE)

Schoolcomms will only process personal data that is necessary to run the service. Personal data is never shared with any other third-party
The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law

The cloud-based solution 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?

The school will continue to be compliant with its Data Protection Policy

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
	Possible	Severe	Medium
Data transfer; data could be compromised	Possible	Significant	Medium
Asset protection and resilience	Possible	Significant	Medium
	Probable	Significant	Medium
Data Breaches	Probable	Significant	Medium
Subject Access Request			
Data Retention			

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**
Data Transfer	Secure network, end to end encryption	Eliminated reduced accepted Reduced	Low medium high Medium	Yes/no Yes
Asset protection & resilience	Data Centre in UK. Accredited to ISO 27001 and Level 2 PCI-DSS certified	Reduced	Medium	Yes
Data Breaches	Schoolcomms ability to respond and deal with a data breach	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Data Retention	Implementing school data retention periods in the cloud	Reduced	Low	Yes

Item	Name/date	Notes
Measures approved by:	Richard May	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Richard May	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:

YourIG DPO raised the following queries

What controls are in place? For example, are password policies enforced to ensure any and all passwords meet a minimum level of strength and complexity and are changed regularly?

Is personal data stored in an anonymised format after a relevant period of time, to ensure that any sensitive details are not retained for any period longer than they are needed?

Is there monitoring in place for unusual activity, for example attempted access from unrecognised IP addresses, or failed log in attempts?

Are databases encrypted at rest using AES and 3DES encryption algorithms; and are there firewalls in place to maximise security?

What securities are in place when transferring data between the school and the cloud? Is data encrypted during transit?

Process of responding to a data breach which has been identified by Schoolcomms and how this is communicated to the school?

Confirmation that personal data is stored on UK servers. If elsewhere, have model contract clauses been used, etc?

DPO advice accepted or overruled:
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

This DPIA will kept under review by:	Alicia Mortimer	The DPO should also review ongoing compliance with DPIA