

Data Protection Impact Assessment (GroupcallXporter)

[Old Park School](#) operates a cloud-based system. As such [Old Park 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.

[Old Park School](#) recognises that moving to a cloud service provider has a number of implications. [Old Park 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 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.

[Old Park School](#) aims to undertake 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	3
Step 2: Describe the processing	6
Step 3: Consultation process	13
Step 4: Assess necessity and proportionality.....	14
Step 5: Identify and assess risks	15
Step 6: Identify measures to reduce risk	16
Step 7: Sign off and record outcomes.....	17

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? – To help deliver a cost-effective solution to meet the needs of the business.

GroupcallXporter enables accessibility to personal data from the school's Management Information System to deliver a variety of apps and services on behalf of the school. As such GroupcallXporter ensures information security and enables the school to manage what access is given to personal data hosted on the school's Management Information System. As the data controller it is important that [Old Park School](#) controls exactly what data is shared with each application.

GroupcallXporter is a provider of online platforms and Application Program Interfaces (API)* which are simple, smart, and secure and gives schools more control and visibility of their own data and provides additional tools.

*An Application Program Interface (**API**) is a set of routines, protocols, and tools for building software applications. An **API** specifies how software components should interact.

GroupcallXporter and Third Party Apps/Vendors

GroupcallXporter'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.

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

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

clarity, GroupcallXporter does not extract data that is not approved by the schools for the vendors they are using.

[Old Park School](#) can reduce the requested GroupcallXporter permissions upon the integration taking place, and GroupcallXporter can assist schools with this. [Old Park 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 GroupcallXporter for the vendors to provide the agreed service).

[Old Park School](#) will undertake the following processes:

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

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

1. Scalability
2. Reliability
3. Resilience
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Update of documents in real time
7. Good working practice, i.e. secure access to sensitive files

GroupcallXporter provides the school with the tools to securely share data stored in the Management Information System (MIS) with third party applications (apps).

Through GroupcallXporter, schools can better manage suppliers and control exactly what data is shared with each application. The school uses apps powered by GroupcallXporter and has its own dedicated account.

GroupcallXporter connects Compass+ to the school's MIS.

It then transfers the personal information from the school's MIS to [Compass+](#).

Compass|+ is then kept up-to-date, as every time a school makes changes on their MIS, it will automatically change in [Compass+](#) after the overnight sync.

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 and workforce data in the cloud.

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 and Workforce) for the school provides the legitimate basis of why the school collects data.

How will you collect, use, store and delete data? – The information collected by the school is retained on the school's computer systems and in paper files. 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. Workforce information is collected through application forms, CVs or resumes; information obtained from identity documents, forms completed at the start of employment, correspondence, interviews, meetings and assessments.

Will you be sharing data with anyone? – [Old Park 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, Management Information System and various third-party Information Society Services applications.

[Old Park School](#) routinely shares workforce information internally with people responsible for HR and recruitment (including payroll), senior staff, with the Local Authority, and the Department for Education.

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? – GroupcallXporter will have access to the school's Management Information System. The school's MIS contains pupil data relating to personal identifiers and contacts (such as name, unique pupil number, contact details and address). Characteristics (such as ethnicity, language, nationality, gender, religion, data of birth, DPIA (GroupcallXporter)
20241014
v1.3

country of birth, free school meal eligibility). Special education needs, safeguarding information, medical and administration (doctor's information, child health, dental health, allergies, medication and dietary requirements). Attendance information, assessment, attainment and behavioral information. The school also obtains data on parents/guardians/carers including their name, address, telephone number and e-mail address.

The school's MIS may also contain workforce data relates to personal information (such as name, address and contact details, employee or teacher number, bank details, national insurance number, marital status, next of kin, dependents and emergency contacts). Special categories of data (such as gender, age, ethnic group). Contract information (such as start dates, terms and conditions of employment, hours worked, post, roles and salary information, pensions, nationality and entitlement to work in the UK). Work absence information, information about criminal records, details of any disciplinary or grievance procedures. Assessments of performance (such as appraisals, performance reviews, ratings, performance improvement plans and related correspondence). Information about medical or health conditions.

Data used by GroupcallXporter will include personal information. This may include information such as the pupil's first and last name, e-mail address and what school they're attached to. Providing this data will enable schools to access GroupcallXporter and for GroupcallXporter to access the school's Management Information System.

Special Category data? – Some of the personal data collected falls under the UK GDPR special category data. This includes race; ethnic origin; religion; biometrics; and health. These may be contained in the Single Central Record, the school's MIS, child safeguarding files, SEN reports, etc.

GroupcallXporter may collect data, for example, for the provision of a free school meal service which may include special category data relating to health and religion.

How much data is collected and used and how often? – Personal data is collected for all pupils. Additionally personal data is also held respecting the school's workforce, Board of Governors, Volunteers, and Contractors. Data relating to sports coaches and other

educational specialist is contained within the Single Central Record to ensure health and safety and safeguarding within the school.

GroupcallXporter will have access to the school's Management Information System. It will only process personal data to deliver the functionality required by the school.

How long will you keep the data for? – Consider the data retention period as outlined in the IRMS Information Management Toolkit for Schools

Scope of data obtained? – How many individuals are affected (pupils, workforce, governors, and volunteers)? And what is the geographical area covered? Year 1 to Year 14 pupils [149], workforce [157], Board of Governors [10], and Volunteers (1), and any other, i.e. contractors, education specialists [15].

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)?

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

What is the nature of your relationship with the individuals? – [Old Park 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) [Old Park 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? – Access to the files will be controlled by username and password. GroupcallXporter is hosting the data and has the ability to access data on instruction of [Old Park School](#) who is the data controller for the provision of supporting the service delivery.

The data processor (GroupcallXporter) will be able to upload personal data from the school's Management Information System for the data to be stored remotely by the service

provider. Changes made to personal data held within the school's Management Information System will be updated automatically after the overnight sync.

Do they include children or other vulnerable groups? – Data used by GroupcallXporter will include personal information such as a pupil's first and last name, e-mail address and what school they're attend.

GroupcallXporter may collect data, for example, for the provision of a free school meal service which may include special category data relating to health and religion. It is very much dependent on how the school uses GroupcallXporter.

Are there prior concerns over this type of processing or security flaws? – All data is encrypted and data is stored AES encrypted at rest. Groupcall are ISO27001 certified.

[Old Park School](#) recognises that moving to a cloud-based solution raises a number of UK 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 users of GroupcallXporter have their own accounts
- **ISSUE:** Transfer of data between the school and the cloud
RISK: Risk of compromise and unlawful access when personal data is transferred
MITIGATING ACTION: GroupcallXporter are committed to making sure school data is secure. This includes Secure Socket Layers for encrypted transfer, encryption of data at rest, field-level encryption for identifiable data and password protection for all end users
- **ISSUE:** Understanding the cloud-based solution chosen where data processing/storage premises are shared?
RISK: The potential of information leakage
MITIGATING ACTION: Using GroupcallXporter personal data is typically transmitted directly from the school's Xporter installation securely to the recipient service and doesn't pass through Groupcall servers at all

- **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: GroupcallXporter operates within European data boundaries and utilises the Microsoft Azure cloud platform, which is certified for the storage of personal data
- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
RISK: UK GDPR non-compliance
MITIGATING ACTION: GroupcallXporter exist to help schools get the most out of their data, not to gain any understanding of it ourselves. GroupcallXporter will never inspect data or mine for information, or allow others to do so
- **ISSUE:** Implementing data retention effectively in the cloud
RISK: UK GDPR non-compliance
- **MITIGATING ACTION:** GroupcallXporter doesn't hold any additional personal data other than that already contained in the school's MIS
- **ISSUE:** Responding to a data breach
RISK: UK GDPR non-compliance
- **MITIGATING ACTION:** GroupcallXporter is compliant with UK GDPR data security handling and reporting
- **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: Data subjects may make data access requests and GroupcallXporter will ensure that its response to the data access request complies with the requirements of the UK GDPR. Data subjects have the right to complain to GroupcallXporter related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled

In fulfilling any Subject Access Requests or Right to be Forgotten, GroupcallXporter will automatically follow whatever actions the school choose to make within its MIS, typically

within 24 hours of those changes being made – or sooner if the school manually refresh data

- **ISSUE:** Third Party Access

RISK: UK GDPR Non Compliance

MITIGATING ACTION: No third party may access personal data held by GroupcallXporter without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which GroupcallXporter is committed, and which gives GroupcallXporter the right to audit compliance with the agreement

- **ISSUE:** Data Ownership

RISK: UK GDPR non-compliance

MITIGATING ACTION: The school remains the data controller. GroupcallXporter is the data processor

- **ISSUE:** Post Brexit

RISK: UK GDPR non-compliance

MITIGATING ACTION: The UK has an approved Adequacy Agreement with the EU and therefore post Brexit GroupcallXporter will continue to remain compliant with the provision of cloud storage held within the EU. This means that the school remains GDPR compliant when using GroupcallXporter

GroupcallXporter operates within European data boundaries and utilises the Microsoft Azure cloud platform, which is certified for the storage of personal data

The UK will transitionally recognise all EEA states, EU and EEA institutions, and Gibraltar as providing an adequate level of protection for personal data. This means that personal data can continue to flow freely from the UK to these destinations following the UK's exit from the EU

- **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: GroupcallXporter are committed to making sure school data is secure. This includes Secure Socket Layers for encrypted transfer, encryption of data at rest, field-level encryption for identifiable data and password protection for all end users

- **ISSUE:** UK GDPR Training

RISK: UK GDPR non-compliance

MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to GroupcallXporter. This may include online e learning

- **ISSUE:** Security of Privacy

RISK: UK GDPR non-compliance

MITIGATING ACTION: All data is encrypted and data is stored AES encrypted at rest. Groupcall are ISO27001 certified.

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

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:

- Scalability
- Reliability
- Resilience
- Delivery at a potentially lower cost

- Supports mobile access to data securely
- Update of documents in real time
- Good working practice, i.e. secure access to sensitive files

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 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)

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

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
Post Brexit (GDPR non-compliance)	Possible	Significant	Medium
Subject Access Request	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
Data Transfer	Secure network, end to end encryption	Reduced	Low medium high	Yes/no
Asset protection & resilience	Data Centre in EU, ISO 27001 registered	Reduced	Medium	Yes
Data Breaches	Documented in contract and owned by school	Reduced	Low	Yes
Post Brexit	Servers are the EU based	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Miss Tina Partridge	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Miss Tina Partridge	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:		
DPO advice accepted or overruled by: Accepted by Tina Partridge If overruled, you must explain your reasons		
Comments:		
Consultation responses reviewed by: Retrospective If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will be kept under review by:	Tina Partridge	The DPO should also review ongoing compliance with DPIA