STUART BATHURST CATHOLIC HIGH SCHOOL

Data Protection Impact Assessment (Compass+)

Data Protection Impact Assessment (Compass+)

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 or hosted solution called Compass+. Access to Compass+ is through a web browser. 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 recognizes that changes do occur and on this basis, good practice recommends that the school review its Data Protection Impact Assessment.

What is the aim of the project?

Compass+ is an online tool to help secondary, special schools and sixth forms to benchmark, manage, track and report on the school's careers programme.

Compass+ is powered by pupil-level data. It integrates with the school's Management Information System (MIS) data for effective and targeted careers programme planning and delivery. Compass+ provides a one-stop-shop platform for completing Compass evaluations, creating activity plans and managing engagement with employers and partners.

Compass+ will be able to:

- Quickly map out and assess the impact of the school's careers programme for the academic year
- Target relevant careers interventions to the students most in need
- Analyse data more effectively, draw powerful insights and improve student outcomes
- Encourage collaboration by allowing colleagues to contribute to the careers programme
- Receive intelligent provider recommendations for activities and start to build a strong network of careers partners

The personal student data in Compass+ is initially extracted from the school's Management Information System using the automated extraction software provided by the Data Integrator.

The school selects and approves the data fields, called "scopes", that Compass+ want to be transferred from the school's Management Information System to Compass+. The Data Integrator then extracts and caches the selected data. This data is then made available to Compass+.

An integration tool called the "Connector" fetches only the data required by Compass+ from the Data Integrator API. The Connector transforms the MIS data received into the necessary format and loads it into Compass+. Compass+ only receives the specific data scopes that our school has approved for use in Compass+.

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:

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 Compass+ the school aims to achieve the following:

1. Scalability
2. Reliability
3. Management
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Update of documents in real time (where applicable)
7. Good working practice, i.e. security of access

Compass+ is a web-based application which uses personal data to set up individual log ins. Compass+ cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated with reference to Compass+.

Stuart Bathurst Catholic High School is the data controller and Compass+ is the data processor.

The Privacy Notices (Pupil) for the school provides the lawful basis of why Stuart Bathurst Catholic High School collects data. The lawful basis in order to process personal data in line with the 'lawfulness, fairness and transparency principle is as follows:

6.1 (c) Processing is necessary for compliance with a legal obligation to which the controller is subject; e.g. health & safety and safeguarding;

6.1 (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

6.1 (f) Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third-party;

For the processing of special category data the lawful basis for collecting this information will be 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 will you collect, use, store and delete data?

The information collected by the school is retained on the school's computer systems and is shared on the Compass+ website/app. Compass+ set-up requires the school to provide an e-mail address to register the children and give access to Compass+.

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.

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, Management Information Systems and various third-party applications including Compass+.

However, concerning Compass+ only staff working at Stuart Bathurst Catholic High School can see the benchmark, manage, track and report on the school's careers programme respecting its pupils.

No information from Compass+ can be shared with other people without explicit consent Stuart Bathurst Catholic High School.

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

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

What is the nature of the data?

Pupil data relates to personal identifiers and contacts (forename and surname, admission number, UPN, date of birth, ethnicity, English as an Additional Language, Gender, SEN provision, Pupil Premium, free school meal status or other indicator of social deprivation, School Year, Form, attendance, responses to assessment questions, assessment output, and other fields which may be determined by the school).

The lawful basis for processing pupil's personal information in this way is public task.

Workforce data relates to personal identifiers and contacts (e mail address, forename and surname, job role, management level and place of work). No special category data is held on Compass+ respecting workforce data.

Stuart Bathurst Catholic High School as data controller decides exactly what data to include.

Special Category data?

In the context of the Compass+ secondary, special schools and sixth forms may process special category data as defined by GDPR Article 9. This could include ethnicity, race and health information.

How much data is collected and used and how often?

Personal data is collected for each pupil enrolled in Year 7 to Year 11.

How long will you keep the data for?

Unless there is a specific legal requirement to keep the school's personal information, it will be retained for no longer than is necessary for the purposes for which the data was collected or for which it is to be further processed, i.e. further processing shall often include research. The school may wish to opt out of this

The school will consider the data retention period as outlined in the IRMS Information Management Toolkit for Schools and within the School's Data Retention Policy.

Compass+ will be used to benchmark, manage, track and report on the school's careers programme respecting its pupils.

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 to manage learning activities.

Through the Privacy Notice (Pupil) 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?

The school will be able to upload personal data from its management information system through a csv file which is uploaded to the website or through an Application Interface Program (AIP).

Stuart Bathurst Catholic High School can log into the school account and select to download report. The report will be e-mailed to the e-mail address associated with the school account.

Do they include children or other vulnerable groups?

Personal data will relate to pupils attending the school to Year 7 to Year 11. Appropriate password permissions will be in-situ to (1) access Compass+ at school; (2) access Compass+ remotely or; (3) access personal data by the cloud service provider.

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

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

- **ISSUE:** Compass+ will be storing personal data
  RISK: There is a risk of uncontrolled distribution of information to third parties.
  MITIGATING ACTION: Compass+ apply appropriate organisational and
  technical security measures to protect the school's personal information against unauthorised disclosure or processing

  Various security measures are used to protect the information that Compass+ collects, as appropriate to the type of information. These measures include encryption, firewalls, and access controls. Password controls are in place for user access, with variable permissions according to the user's role. All external data transmissions to and from Compass+ are encrypted using modern protocols and ciphers. All personal data is encrypted in transit and at rest.

  Compass+ only stores and processes the minimum personal data required to provide the Compass+ service

  All Careers & Enterprise Company staff having access to personal data hold a valid Disclosure and Barring Service certificate

  The school is responsible for granting and managing staff access to Compass+. Under Careers & Enterprise Company processes, the primary Administrator user of the school must be authorized by the Head Teacher or nominee. The primary Administrator user is then responsible for managing the authorization of other users in the school. Careers & Enterprise Company reminds school Administrator users of their obligations for ensuring that their users are appropriate, and from time to time may audit the user lists, highlighting apparent anomalies to schools.

- **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: Data is stored in the UK. This means that the UK GDPR privacy rules apply to the cloud-based service

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred
  MITIGATING ACTION: Personal data originating from the school will be transported and stored using modern and best practice encryption technologies. This includes Secure Socket Layers (SSL/TLS) for encrypted data transfer over the internet, encryption of all data at rest, field-level encryption for personally identifiable data and password protected identities for all end users

- **ISSUE:** Use of third-party sub processors?
  RISK: Non-compliance with the requirements under UK GDPR
  MITIGATING ACTION: Where necessary and in limited circumstances, Compass+ may share the schools personal information with third parties to the extent permitted by or required by law including to (a) meet Compass+ legal obligations; (b) provide reasonable voluntary cooperation with a relevant police or regulatory investigation or any ongoing or prospective legal proceedings; (c) in order to establish, exercise or defend Compass+ legal rights, including providing information to others for the purposes of fraud prevention and reducing credit risk

  In addition, Compass+ make use of expert third party service providers to help them provide relevant services, such as expert IT providers helping them with their IT systems, or professional auditors. These third-party service providers may use the school's personal information, in order to provide the agreed service to Compass+, or to the school on their behalf. Compass+ have contractual agreements in place with third party data providers and they ensure that they are fully compliant with data protection laws

  The school's personal information may be held by Compass+ in one or more customer relationship management (CRM) database(s), consolidating details of school dealings with Compass+ across various services, to ensure Compass+ have clear and accurate records about school use of their services/programmes, to better understand school requirements and how Compass+ might provide other services/programmes to the school.

  Compass+ may share personal information within its advisory boards, panels and stakeholders, as needed for reasonable management, analysis, planning and decision making, including in relation to taking decisions regarding its service/programme offering

- **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: As a service, Careers & Enterprise Company is UK GDPR compliant. The data processor remains accountable for the data within the system. For the services it manages, Compass+ applies its own security updates. Where security updates are applicable to the infrastructure, the servers hosting Compass+ will manage these.

- **ISSUE:** Data Retention
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The length of time that Compass+ hold the school's personal data varies depending on the type of information and its use. Compass+ will only keep the personal data for as long as it is necessary to provide the services and/or products that have been requested, for the execution of a contract or for such other essential purposes such as, complying with legal obligations, resolving disputes, investigating disciplinary matters and enforcing agreements.

  In terms of student data this will be deleted from Compass+ 3 years after the student leaves the school. This is in line with the recommendation of Gatsby Benchmark 3 for Careers Leaders to track the destinations of students for 3 years after they leave school: *"The school collects and maintains accurate data for each student around their education, training and employment destinations for at least three years after they leave. This information is shared with current students to support ongoing review and evaluation of the careers and enterprise programme."*

- **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 staff and other users whose data is held by Compass+ as the Data Controller may request a copy of any information held about them by writing to: Careers & Enterprise Company, 2-7 Clerkenwell Green, London EC1R 0DE or by by emailing DPO@careersandenterprise.co.uk

  Where a request is received from a pupil (or their legal guardian) whose details have been entered on Compass+ systems by the school Compass+ will in the first instance direct the request back to the school as the data controller. Compass+ will support the school where the school requests assistance with data subject access requests

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school as data controller maintains ownership of the data. Careers & Enterprise Company is the data processor. In terms of disclosure Compass+ will not release the information to any third party unless the request is subject to legal obligation without obtaining the express written authority of the school who provided the information

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: All Compass+ data is stored in a secure database, hosted on cloud-based servers in the UK and transported within the EEA for support purposes only.
- **ISSUE:** Lawful basis for processing personal data
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: School has included Compass+ in its Privacy Notice (Pupil) which identifies the lawful basis for processing personal data

- **ISSUE:** Responding to a Data Breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Careers & Enterprise Company is an ICO registered company, fully compliant with UK GDPR data security handling and reporting

  Careers & Enterprise Company perform regular penetration testing. They review all security concerns brought to their attention, and they take a proactive approach to emerging security issues. Careers & Enterprise Company strive to stay on top of the latest security developments both internally and by working with external security auditors and companies

- **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: School staff and other users whose data is held by Compass+ as the Data Controller may request a copy of any information held about them by writing to:

  Careers & Enterprise Company, 2-7 Clerkenwell Green, London EC1R 0DE or by emailing DPO@careersandenterprise.co.uk

  Where a request is received from a pupil (or their legal guardian) whose details have been entered on Compass+ systems by the school Compass+ will in the first instance direct the request back to the school as the data controller. Compass+ will support the school where the school requests assistance with data subject access requests.

- **ISSUE:** Data is not backed up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: All data backups are in line with the standards as set out by the company providing the cloud-based service.

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

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Careers & Enterprise Company is registered with the ICO. The ICO's registration number is ZA128193.

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

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.

The lawful basis for processing personal data is contained in the school's Privacy Notice (Pupil). 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.

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
Data Retention	Probable	Significant	Medium

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, appropriate security in place	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
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 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, 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 are in place to maximise security?

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

How and when is the data backed up?

Does Compass+ use third party sub processors? And if so, what controls are in place?

Process of responding to a data breach which has been identified by Compass+ 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?

Does Compass+ have any accreditations, i.e. ISO 27001, Cyber Essentials Plus?

The responses to these questions have been embedded within Step 2 Issues, Risks and Mitigating Actions.

DPO advice accepted or overruled by: If overruled, you must explain your reasons		
Comments: DPO Advice provided		
Consultation responses reviewed by: If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by:	Alicia Mortimer	The DPO should also review ongoing compliance with DPIA