# 

**DPIA – IT Provider**

|  |  |
| --- | --- |
| **Name of School** |  |
| **Reviewed by DPO** | **Y/N** *(signature of DPO here)* |
| **Date of DPO approval** |  |
| **Governor minute number** |  |
| **Review Date** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version History** | | | |
| **Version** | **Date** | **Detail** | **Author** |
| 1.0 | 30/01/2021 | First draft | Heather Toomey |

Schools are responsible for ensuring that Data Protection measures are in place to mitigate risk and appropriate acceptable user policies are signed by all those with access to the system.



Introduction

The school currently has its personal data stored [locally via a dedicated servers held on site / held in the cloud].

The school plans to use [IT Provider] to facilitate: *(delete as applicable)*

1. The monitoring and maintenance of services
2. Backup services
3. Email provisioning
4. On-site technical support
5. Provision access to services which are of benefit to the smooth running and operation of the school.

* Administration Access to any system, including the server, will be approved by the headteacher and [IT service provider] will be added to the log of administrators.
* The Headteacher will have access to administrative logins at all times. Administrative access provided to [insert service provider] is facilitated only whilst services are being provided to the school under contract and staff working with/for [IT service provider] will ensure they remain compliant with the computer misuse act 1990 and the data protection act 2018.
* The Headteacher will ensure access to the provider is removed if they cease to provide services to the school.
* [IT service provider] will be limited to data processing functions linked to backup and restoration functions or those required as part of disaster / incident recovery.
* Prior approval by [senior school staff / IT Lead] will be sought before any data processing not covered under the terms of the contract takes place.
* The network is only accessible via user specific passwords and usernames. Sensitive data is secured by role specific access restrictions.
* Information will be held securely [detail encryption methods] and include appropriate technical controls.

**Backup and Restoration Provision**

[IT Service provider] is contracted to provide backup/restoration services to the school.

The backup is [site based/remote cloud based].

Backup services require the processing of all data held by the school, including sensitive data. The loss of such data would give rise to a high risk and significant data breach.

Backup schedules are included in the Service Level Agreement.

**Email Provision**

[IT Support provider] provides email services to the school and provisions email accounts. Staff are aware that email communications with sensitive or personal information must be encrypted.

Email monitoring is undertaken for security purposes only and includes scanning for malware and spam, as per the service contract. The viewing or processing of emails by the provider, except for backup purposes, is strictly forbidden, unless authorised as part of an authorised investigation.

**Cloud Computing**

[Insert school name] has chosen cloud computing as a method for delivering information technology services. Resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server on-site at the school.

The school utilises a cloud based solution with the aim of:

1. Scalability and a more flexible storage solution

2. Reliability and resilience

4. Lower infrastructure cost

5. Increased support and security for mobile working/access

6. The ability to update data in real time

7. Improved working practices and security

The school recognises that moving to a cloud service provider has a number of implications. The data protection impacts of the cloud system the school has chosen is contained within a separate DPIA.

**Screening questions**

**Will the project involve the collection of new information about individuals? If yes, please detail the information to be collected.**

Yes, data will be shared with the [IT provider] to allow users to have accounts. This data will be limited to the minimum necessary for accounts to be set up (usually first and last name and email address).

[IT provider] will have access and process to data as part of a backup agreement and as part of any necessary restoration.

The school uses the internal network to undertake the following processes:

1. Collecting data
2. Recording and organising data
3. Structuring and retaining (storing) data
4. Retrieving information
5. Deletion

Whilst not all data on school systems is defined as personal data, the school recognises that personal data, including data which is classed as sensitive, forms part of the information processed and stored by the school.

**Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? If yes, please detail which organisations will be provided with access.**

Yes. The school will be sharing data with [IT provider] who will be data processor.

**Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. If yes, please detail the new technology, below.**

No

**Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them? If yes, please describe the impact, below.**

No.

**Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private. If yes, please describe the information to be collected, below.**

The information indirectly relates to children who are identified under the GDPR as requiring extra safeguards to protect their data.

However, the only information that is shared routinely with the provider is the name and email address of the person that is set up on the account.

Additional data is accessible through the need to provide administrative access.

The confidentiality of data is protected by signed confidentiality agreements, service level agreements and service contracts.

**What is the lawful basis of the processing?**

The lawful basis for processing this information is that it is necessary for a task in the public interest.

Special category data would only be processed as part of a system recovery / restoration.

If any special category data is processed, then it is justified as necessary for substantial public interest.

**Note regarding Consultation**

The school will consult with the DPO regarding this change in sharing of data. As the school already shares data with IT support services and relies on public interest to do so, there is no need for any external consultation.

Parents and pupils will be informed via relevant Privacy Notices.

**General Project Description**

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties:

|  |
| --- |
| **General Support and Maintenance**  The school utilises a variety of systems to aid teaching and learning and to communicate effectively with stakeholders.  The schools also purchases separate platforms which do not inter-connect and require imports/exports. These services require system administration and maintenance, which [IT support provider] is contracted to undertake.  **Email Hosting**  [IT Support provider] provides email services to the school and provisions email accounts. Staff are aware that email communications with sensitive or personal information must be encrypted.  Email provision includes scanning for malware and spam and monitoring is undertaken for security purposes only, as per the service contract.  **Cloud Services**  In line with the governments [cloud first strategy](https://www.gov.uk/guidance/government-cloud-first-policy) the school has transitioned from an on-site server to a cloud hosted server. Using cloud servers reduces the use of portable drives in schools, removes the need to e-mail documents internally, allows for real-time editing and strengthens data protection.  This is line with the government’s digital strategy.  **Backup Services**  [IT Support provider] provides the school with backup services.  Backups are held [on-site / off-site/in the cloud]  Backups are protected by encryption and secured against unauthorised access [add details].  [IT support provider] is registered with the ICO, registration number ZXXXXXXXXX as a data processor under the data protection act 2018. |

Will the project/system involve the processing of personal data or special category (sensitive) personal data?

YES

1. **Systematic Description of the Envisaged Processing Operations**
   1. Identify the data subjects:

|  |
| --- |
| Students  Parents  Staff  Governors  Stakeholders, such as PTA members who may be provided with a school email / account. |

* 1. What personal data will be processed?

|  |
| --- |
| Potentially all categories of personal data specified in all school Privacy Notices will be processed. |

* 1. What special category (sensitive) data or criminal convictions data will be processed?

|  |
| --- |
| See 1.2 This includes all special category data which the school processes, as detailed in our Privacy Notices. |

* 1. What are the purposes and lawful grounds for processing the personal data identified above?

|  |  |  |
| --- | --- | --- |
| Personal Data | Purpose | Lawful basis |
| See 1.2 | Additional data may be stored / shared for the purpose of collaboration and records of minutes etc. | Public Task Duty |

* 1. Describe the nature, scope and context of the processing, including a functional description of the processing operations:

|  |
| --- |
| The IT provider will only process Personal Data on behalf of the school for the purposes of providing the Services in accordance with the Service Level Agreement / contract.  Staff, pupils and governors are able to have user accounts which provide access to an array of applications and services. The settings within Active Directory and in relation to settings within the applications offer the ability to restrict what is seen / shared.  Group policy deployed across the network which can restrict or enable access and offer centralised management to improve security and privacy.  Duration of Processing: The term from the school entering into an agreement until the contract is ceased, plus the period legally required under retention guidelines.  Type of Personal Data, include but are not limited to the following:  User Profile: First Name, Last Name, Phone (optional), Email, Password (if SSO is not used), Profile Picture (optional), Department (optional)  Metadata: Topic, Description (optional), participant IP addresses, device/hardware information  Recordings: videos, audio recordings and presentations, Text file of all in meeting chats, Audio transcript file, IM Chat Logs  Backup and restoration of user files, which may include sensitive personal data.  Data is stored [detail storage locations and state if cloud services are provided] |

* 1. Describe the assets on which the personal data relies (hardware, software, people, paper, networks, transmission channels)

|  |
| --- |
| The internet – routers, access points and service provision.  School IT, teaching and support staff.  Laptops, desktops, tablets, phones. Some will be school property, others may be privately owned devices.  Stakeholder home Wi-Fi and internet provision. |

* 1. Set out the periods for retention of the personal data:

|  |
| --- |
| [IT service provider] retains information which has been backed up to their servers via their cloud backup solution. This is for the purposes of delivering their services.  The provider holds limited account holder data until the account is terminated. (Name, email address, school name)  Retention of account information is 6 years plus the current year. |

* 1. Set out details of any data sharing with third parties, including sub-processors:

|  |
| --- |
| Identify any sub processors, including third party services which form part of the provision. |

* 1. Set out details of any data sharing outside the EEA or with any international organisations:

|  |
| --- |
| Detail cloud storage outside the EEA, including AWS, Microsoft and GSuite |

1. **Necessity and Proportionality Assessment**
   1. If legitimate interest is identified as the lawful basis, set out details below:

**Not applicable.**

* 1. Identify any personal data processed in a manner which is not necessary for the identified purpose:

|  |
| --- |
| We will not process any data which is not already covered by school privacy notices. It is envisaged that no new data will be processed by this project. |

1. **Assessment of Risks to the Rights and Freedoms of the Data Subjects**

Consider and describe the risks to the rights and freedoms of the data subjects in the following areas:

* 1. Lawfulness of processing

|  |
| --- |
| Names, year groups, unique identifiers, school details and contact information is being processed for the purposes of creating new accounts. The existing lawful basis for each type of processing currently being done on School network shares will also apply to the same activity on cloud systems. The school has identified Public Task as a lawful basis for the act of processing data this data. |

* 1. Fairness and transparency of processing

|  |
| --- |
| The schools Privacy Notice will be updated with reference to the use of the new IT supplier. |

* 1. Data minimisation

|  |
| --- |
| Low risk – Only basic personal details will be processed when setting up new accounts and these will be managed by the school. |

* 1. Maintaining accurate and up to date data

|  |
| --- |
| On site server - Medium risk that data will not be updated due to being stored in multiple locations. Account accuracy is dependent on manual updates which could lead to errors or a lag in updating.  Cloud server – Low risk that data will not be updated as live-access is available and users are provisioned via an MIS connection exists.  Cloud services allow staff and pupils to work together with real-time co-authoring, auto saving, and easy sharing across applications. |

* 1. Ability for data subjects to opt out or object to processing

|  |
| --- |
| We accept that it will not be possible for data subjects to opt out of having their basic data processed, but consent for relevant processes in maintained by the school office. |

* 1. Ability to respond to subject access requests

|  |
| --- |
| Local storage  Low risk that ICT admin staff will not be able to locate all relevant personal information stored on school systems to be able to respond to an SAR.  Cloud storage  Moderate risk that ICT admin staff will not be able to locate all relevant personal information stored on school systems to be able to respond to an SAR. |

* 1. Rights of the data subjects

|  |
| --- |
| Right to be informed: School to add [IT service provider] to list of processors and inform parents this will be used via privacy notice  Right to access: School will update information audits and data maps accordingly to facilitate data retrieval in the event of an access request. The provider will assist with a SAR where a valid request is received.  There will be no automated profiling  The right to data portability is limited to applications and services owned and serviced by the school and does not require consent or contract with the provider.  Right to restrict processing: can be achieved by the school having administrative rights to amend login details and restrict IT provider access.  Low risk of difficulty complying with Right to Rectification and Right to Erasure where documents may be stored in multiple locations.  [IT support provider] shall, to the extent permitted by Applicable Data Protection Law, promptly notify the school upon receipt of a request by a Data Subject to access, rectify, restrict, erase, transfer, or cease Processing, withdrawal of consent to Processing, and/or objection to being subject to Processing that constitutes automated decision-making (such requests individually and collectively “Data Subject Request(s)”).  If the provider receives a Data Subject Request in relation to Customer’s data, the provider will advise the Data Subject to submit their request to the school and the school will be responsible for responding to such request, including, where necessary, by using the functionality of the Services.  The provider shall, at the request of the school, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organisational measures to assist the school in complying with any obligation under Applicable Data Protection Law to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, provided that (i) the school is itself unable to respond without the provider’s assistance and (ii) the provider is able to do so in accordance with all applicable laws, rules, and regulations. The school shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by the IT support provider.  The provider will ensure that the following processes are applied:   * **Discovery**. The process of determining what data is needed to complete a SAR. * **Access**. Retrieval and potential transmission to the data subject of discovered information. * **Rectify**. Implement changes or other requested personal data changes. * **Restrict**. Changing the access or processing of persona data by restricting access to the provider or removing data from any provider owned systems. * **Export**. Providing a "structured, commonly used, machine-readable format" of personal data to the data subject, as provided by the GDPR's "right of data portability." * **Delete**. Permanent removal of personal data from provider systems. |

* 1. Transfers to third parties

|  |
| --- |
| Identify any sub processors, including third party email services and backup providers.  *Data should only be transferred to third parties essential for the provision of services.* |

* 1. Transfers outside the EEA or to international organisations

|  |
| --- |
| UK storage No transfers take place.  Cloud storage outside the EEA - Medium risk as personal data is stored outside the EEA.  Detail the level of security and ensure it has been independently audited for GDPR compliance. Include any information relating to TLS / SSL / Encryption. |

* 1. Retention and deletion

|  |
| --- |
| Medium risk that the school will struggle to identify and delete all personal information held at the end of its retention period.  Staff will be advised to ensure electronic data is collated and filed appropriately to enable regular reviews in line with retention policy. |

* 1. Data security

|  |
| --- |
| Low risk that a IT service provider might share personal data with a third party.  Low risk that backup data may be incomplete, too old, left at risk of exposure or corrupted. (Data breach)  Medium risk that data may be corrupted during installations / maintenance.  Low/Medium risk that IT backup provision may not facilitate data recovery in the event of an incident.  Low/Medium risk that email accounts are compromised and communication flows and data are affected. Low risk to personal data.  Medium risk of unauthorised access to data or inappropriate use of administrative access. |

* 1. Further risks

|  |
| --- |
| Medium risk that personal information may be shared inappropriately. This could happen if third party sub-processors are used.  Low risk that a data breach occurs because IT staff are not sufficiently trained to be able to correctly configure technical controls and privacy features. |

1. **Measures Envisaged to Address the Risks**
   1. Complete the following table using the risks identified above:

|  |  |  |  |
| --- | --- | --- | --- |
| Identified risk in paragraph 3 above | Risk | Controls to be implemented | Proposed Mitigation |
| 3.1 | The existing lawful basis for each type of processing currently being done on Schools network shares will apply.  The school has identified Public Task as a lawful basis for the act of processing this data. | HT to control admin system access and decide on user levels.  Contracts to cover appropriate security settings, data collection/processing, and restrict access, if necessary.  The service level agreement will be reviewed and a signed contract, covering confidentiality will be put in place. | Lowers risk |
| 3.2 | Low risk that the provider carries out an activity that has not been screened for GDPR issues, and that is not added to the Record Of Processing Activities, and not covered by privacy notices. | HT to ensure that new services and applications are centrally rolled out to include terms of use and expectations.  IT supplier to only commencement installations and processing activities under contract or by direct instruction from senior management.  Written authorisation will be provided when new services are implemented and change management will ensure staff have appropriate awareness and training. | Lowers risk |
| 3.3 | Low risk that user details will change and need to be changed in the hosting account. | Ensure there is a protocol for advising the IT provider of new starters / leavers and an account authorisation process is in place to cover access rights and levels. | Lowers risk |
| 3.4 | Unable to allow data subjects the right to object to processing. | We accept that it will not be possible for data subjects to opt out of having their basic meta data processed  **The school will ensure that individuals (staff) are aware of their rights under data protection legislation, including the right to object where the lawful basis is a public task duty.** | Lowers risk |
| 3.5 | Low risk that the school will not have their access to their own systems. | There will be a process in place to record system administrators.  At least two school staff should have administrative access to ensure IT providers cannot block access to services and that access can be revoked if problems arise. | Eliminates risk |
| 3.6 | Moderate risk that ICT admin staff will not be able to retrieve data in the event of an incident. | There will be a contract / SLA which encompasses backup obligations and which also details the provider’s responsibility for restoration.  Restoration information should include response timescales, roles/responsibilities and liability clauses. | Lowers risk |
| 3.7 | Low risk that the provider might accidentally share personal data with another individual or organisation. | Data protection obligations will be incorporated into contracts and confidentiality agreements and will be shared and signed, as appropriate.  Providers will be furnished with relevant policies and will sign their acceptance of these. | Lowers risk |
| 3.8 | Medium risk that we will have an issue with data transfers outside the EEA. | Standard Contract Clauses. Only if the school has service of backup cloud provision outside the EEA | Lowers risk. |
| 3.9 | Low risk that a data breach occurs because ICT admin staff are not sufficiently trained and familiar with systems to be able to correctly configure systems securely. | IT providers are expected to investigate all settings available to make sure access is restricted as much as possible.  Check providers are Cyber Essentials / ISO 27001 or similarly accredited.  Follow audit procurement guidelines. | Lowers risk. |

1. **Compliance with Guidance/Codes of Conduct**
   1. Identify any applicable guidance and/or codes of conduct issued by the Government, the ICO, the Commission or any relevant association or body:

|  |
| --- |
| NA |

* 1. Where applicable, set out details of compliance with any relevant guidance and/or code of conduct:

|  |
| --- |
| **SCCs**  Cloud services provided outside the EEA should benefit from compliance with the Standard Contractual Clauses (also known as [EU Model Clauses](https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-eu-model-clauses?view=o365-worldwide)).  If necessary, append the SCCs to this DPIA. |

1. **Involvement of Data Subjects**
   1. Where appropriate, seek the views of the data subjects or their representatives on the intended processing and set out the findings below:

|  |
| --- |
| Not appropriate to seek data subject views as the processing enables the school to carry out their duties as an authority under the lawful basis of public task. |

* 1. If the views of the data subjects have not been sought, set out the rationale below, with reference to any commercial or public interests and the security of processing operations:

|  |
| --- |
| The provider will help the School fulfil its obligations, reduce the number of disparate platforms, thereby limiting data sharing and saving public funds. |

1. **DPIA Review** 
   1. This DPIA will be reviewed to assess if processing is performed in accordance with this DPIA annually.

|  |
| --- |
| This DPIA will be reviewed prior to any significant changes to the system and especially if there is a change in methodology or a security risk. |

1. **Integrate the PIA outcomes back into the project plan**

|  |  |  |
| --- | --- | --- |
| Action To be Taken | Date of completion | Responsibility for |
| Adapt and amend this Template DPIA to fit the requirements of the individual school |  |  |
| Consult with DCC GDPR team, DPO and Governors |  |  |
| Approval of the final version of this DPIA by DPO |  |  |
| Update information asset register/map |  |  |
| Amend Privacy Notice(s) |  |  |
| Amend relevant policies e.g. Information Security Policy, IT Policy and Acceptable User Agreement, Safeguarding and Child Protection Policy |  |  |
| Establish regular review of this DPIA and the function of the software |  |  |

**Appendix A: Evidence of due diligence of supplier/s**

The Terms and Conditions, Privacy Policies, Service Level Agreement and Contract of the supplier should be checked and, where necessary, appended.

**Appendix B: Linking the DPIA to the Data Protection Principles**

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the GDPR or other relevant legislation, for example the Human Rights Act.

**Principle 1**

**Lawfulness, fairness and transparency of data processing**

There must be lawful basis for processing the personal data as follows;

**(a) Consent:**the individual has given clear consent for you to process their personal data for a specific purpose.

**(b) Contract:**the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

**(c) Legal obligation:**the processing is necessary for you to comply with the law (not including contractual obligations).

**(d) Vital interests:**the processing is necessary to protect someone’s life.

**(e) Public task:**the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

**(f) Legitimate interests:**the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.

|  |  |
| --- | --- |
| Have you identified the purpose of the project and which lawful basis applies? | E |
| Is the processing of the data necessary in terms of GDPR? | Yes |
| How will you tell individuals about the use of their personal data? | P.N. |
| Do you need to amend your privacy notices? | Yes |
| If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn? | n/a |
| If special categories of personal data have been identified have the requirements of GDPR been met? | Yes |
| As the School is subject to the Human Rights Act, you also will, where privacy risk are especially high, need to consider: | |
| Will your actions interfere with the right to privacy under Article 8 | No |
| Have you identified the social need and aims of the project? | Yes |
| Are your actions a proportionate response to the social need? | Yes |

**Principle 2**

**Personal data shall be obtained only for one or more specified explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.**

|  |  |
| --- | --- |
| Does your project plan cover all of the purposes for processing personal data? | Yes |
| Have you identified potential new purposes as the scope of the project expands? | Yes |
| Does your Privacy Notice cover all potential uses? | Yes |

**Principle 3**

**Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.**

|  |  |
| --- | --- |
| Is the quality of the information good enough for the purposes it is used? | Yes |
| Which personal data could you not use, without compromising the needs of the project? | None |

**Principle 4**

**Personal data shall be accurate and, where necessary, kept up to date.**

|  |  |
| --- | --- |
| If you are procuring new software does it allow you to amend data when necessary? | Yes |
| How are you ensuring that personal data obtained from individuals or other organisations is accurate? | School will check data wherever reasonably practicable to do so. |

**Principle 5**

**Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.**

|  |  |
| --- | --- |
| What retention periods are suitable for the personal data you will be processing? | As per school policy |
| Are you procuring software that will allow you to delete information in line with your retention periods? | Yes |

**Principle 6**

**Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**

|  |  |
| --- | --- |
| Do any new systems provide protection against the security risks you have identified? | Yes |
| What training and instructions are necessary to ensure that staff know how to operate a new system securely? | None |

**Rights of Data Subjects and Privacy by Design**

|  |  |
| --- | --- |
| Will the systems you are putting in place allow you to respond to subject access requests more easily? | Not investigated |
| Will the system allow compliance with individual rights under GDPR, in particular the right to be informed, the right to rectification and the right to ensure (right to be forgotten). | Not investigated |
| If the project involves marketing, have you got a procedure for individuals to opt in to their information being used for that purpose? | n/a |

**Transferring data outside European Economic Area**

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data**.**

|  |  |
| --- | --- |
| Will the project require you to transfer data outside of the EEA? | Possibly |
| If you will be making transfers, how will you ensure that the data is adequately protected? | SCCs |