DPIA - Microsoft Office 365

Name of School	**The Acorn Federation**
Document Prepared by	**Teresa Bosley**
Reviewed by DPO	**Yes** GDPR in Schools
Date of DPO approval	**15/3/21**
Governor minute number	
Review Date	

Version History			
Version	**Date**	**Detail**	**Author**
1.0	30/06/2020	First draft	Heather Toomey
1.1	06/01/2021	New format.	Alex Steward

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 - Microsoft Office

Microsoft Office 365 allows staff and pupils to work together with real-time co-authoring, auto saving, and easy sharing across applications.

It is intended that the use of Microsoft Office 365 will improve learning outcomes due to the built-in accessibility features and Learning Tools that support reading, writing, math, and communication for all students and especially those with additional needs.

Most schools already have access to a range of applications via their Office 365 Educational Licence. This enables staff to use an array of applications, including:

Office apps
- Outlook – a secure email backed up to the cloud with generous storage limits.
- Word
- Excel
- PowerPoint
- OneNote - digital notes to be taken, reducing the need for paper notes which are easily lost.
- Publisher (PC only) – media tools
- Access (PC only) – data base management systems

Services
- Exchange
- OneDrive – central cloud storage of documents, reducing the need for e-mailing files.
- SharePoint
- Teams – video conferencing, live events and collaboration hub
- Sway - digital story telling
- Forms – streamlined communications, for curriculum based tasks or administrative ones.
- Stream – Video collation, sharing and editing

The school plans to use Microsoft Office for staff and pupils to meet face to face with their class, deliver lessons, facilitate data sharing, provide email functionality and access services which are of benefit to the smooth running and operation of the school.

As Microsoft Office is the leading platform in business, pupils will learn skills from an early age which will help then into adulthood.

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 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).

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 Microsoft, 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.
Potentially. The use of video whether for conferencing or as a stand-alone medium may be perceived by some as privacy intrusive. However, individuals are not compelled to allow images to be recorded.

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 with the provider is the name and email address of the person that is set up on the account.

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 should not be processed but 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 Microsoft 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:

Many schools have utilised a variety of systems to aid teaching and learning and to communicate effectively with stakeholders. As schools purchase increasing numbers of separate platforms which do not inter-connect or communicate, the numbers of imports/exports and the time for system administration increases. This leads to higher data processing levels than needed and puts personal information at greater risk.

Encouraging schools to utilise the functionality available via the Microsoft license they already possess and centralising the data sharing to one company, rather than using a host of different platforms, will lead to more secure and robust working practices and greater flexibility.

Using cloud drives will reduce the use of pen drives in schools and the need to e-mail documents. This will strengthen data protection and reduce the associated security risk of using removable storage media. Aligning platforms across schools will align support and training needs and make cross setting transitions easier.

The support communities for Office 365 is extensive and well established, providing many channels for accessing help. Both systems have extensive cross overs in functionality, support the teaching of 'digital citizenship' and teach skills which are crucial in the modern world. This is line with the government's digital strategy.

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

1.1 Identify the data subjects:

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

1.2 What personal data will be processed?

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

1.3 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.

1.4 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

1.5 Describe the nature, scope and context of the processing, including a functional description of the processing operations:

Personal data processed by Microsoft is restricted and data locations for UK customers are in Durham, London and Cardiff.
https://docs.microsoft.com/en-us/office365/enterprise/o365-data-locations

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.

Nature and Purpose of Processing: Microsoft Office will Process Personal Data on behalf of Customer for the purposes of providing the Services in accordance with the Agreement.

Duration of Processing: The term of the Agreement plus the period until Microsoft Office deletes all Personal Data processed on behalf of Controller in accordance with the Agreement. Categories of Data Subjects: Individuals about whom Personal Data is provided to Microsoft Office via the Services by (or at the direction of) Customer or Customer's end users, which may include without limitation Customer's employees, contractors and end users.

Type of Personal Data: Personal Data provided to Microsoft Office via the Services by (or at the direction of) Customer or Customer's end users, including but 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

Cloud Recordings (optional): videos, audio recordings and presentations, Text file of all in meeting chats, Audio transcript file, IM Chat Logs

Group policy deployed across the Microsoft tenancy can restrict or enable access and offer centralised management to improve security and privacy.

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

The internet
School IT staff
Teaching and admin staff

Internal/external Microphones / headsets Laptops, desktops, tablets, phones. Some will be school property, others will be privately owned devices Stakeholder home Wi-Fi and internet providers

1.7 Set out the periods for retention of the personal data:

Microsoft Office retains information which has been backed up to their servers via their cloud backup solution. This is for the purposes of delivering their services. Microsoft Office holds limited account holder data until the account is terminated. (Name, email address, company name) Microsoft has further information on data retention here.

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

Services for internal Sales, Support, PR, Billing, Infrastructure.

1.9 Set out details of any data sharing outside the EEA or with any international organisations:

The Microsoft Office service is based in the United States, with additional server centres, technical and billing support in the UK and Ireland, and payment management and fraud detection systems in Europe.

2. Necessity and Proportionality Assessment

2.1 If legitimate interest is identified as the lawful basis, set out details below:
Not applicable.

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

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

3. 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:

3.1 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 Microsoft Office. The school has identified Public Task as a lawful basis for the act of processing data on Microsoft Office.

3.2 Fairness and transparency of processing

Moderate risk that staff use Microsoft Office for a new data processing 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. DPO advises that Microsoft Office is added to privacy notices.

3.3 Data minimisation

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

3.4 Maintaining accurate and up to date data

Low risk that the details will change and accounts may need to be updated. This will depend on whether a live MIS connection exists.

3.5 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 on Microsoft Office, but have ensured where possible, additional processing has been opted out. Privacy Policy: https://privacy.microsoft.com/en-GB/privacystatement#mainnoticetoendusersmodule

3.6 Ability to respond to subject access requests

Moderate risk that ICT admin staff will not be able to locate all relevant personal information stored on Microsoft Office to be able to respond to an SAR. Microsoft provides further information here

3.7 Rights of the data subjects

Right to be informed: School to add Microsoft Office 365 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. Microsoft will assist with a SAR where a valid request is received. No automated profiling Right to data portability is limited to applications and services owned and serviced by Microsoft and is not via consent or contract. Right to restrict processing: can be achieved by not utilising Microsoft Office where data is inaccurate. School have administrative rights to amend login details where these may be incorrect. Low risk of difficulty complying with Right to Rectification and Right to Erasure where documents may be stored in multiple locations. Microsoft shall, to the extent permitted by Applicable Data Protection Law, promptly notify Customer 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 Microsoft receives a Data Subject Request in relation to Customer’s data, Microsoft 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..

Microsoft shall, at the request of the Customer, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Microsoft ODPA any Customer obligation under Applicable Data Protection Law to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, provided that (i) Customer is itself unable to respond without Microsoft Office assistance and (ii) Microsoft Office is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Microsoft Office.
Microsoft 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, or removing data from the Microsoft cloud.
- **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 the Microsoft cloud.

3.8 Transfers to third parties

Low risk that staff might accidentally share personal data with another individual or organisation. Training on sharing functionality and security settings in O365 will be provided.
Microsoft does not use sub processors.

3.9 Transfers outside the EEA or to international organisations

Medium risk as personal data is stored outside the EEA. However, Microsoft Office is certified under the EU-US Privacy shield.
https://docs.microsoft.com/en-GB/azure/security/fundamentals/physical-security

Microsoft used enterprise level security and has been independently audited for GDPR compliance.

3.10 Retention and deletion

Medium risk that the school will struggle to identify and delete all personal information held on Microsoft Office at the end of its retention period. This will be reviewed no later than 6 months notwithstanding the requirement to review this DPIA when schools return to normal processing.

3.11 Data security

Low risk that a user might share personal data with the wrong person in error. A guides to Office 365 are available here Microsoft Office Data Processing Agreement: 6.2 Microsoft Office shall implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate: 6.2.1 the pseudonymisation and encryption of personal data; 6.2.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; 6.2.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and 6.2.4 a process for regularly testing, assessing and evaluating the effectiveness of security measures.

3.12 Further risks

Medium risk that personal information may be shared inappropriately with colleagues. This could happen inadvertently if videos or files are uploaded without restricted access settings. Low risk that a data breach occurs because staff are not sufficiently trained and familiar with Microsoft Office to be able to correctly configure all features for optimum privacy.

4. Measures Envisaged to Address the Risks

4.1 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 also apply to the same activity on Microsoft Office. The school has identified Public Task as a lawful basis for the act of processing data on Microsoft Office.	HT to control who has system access and decide on user levels with appropriate security settings to minimise data collection/processing, and restrict what facilities are available. Guidance on data sharing practices within Office 365 will be provided. If your organization or users engage with Microsoft to receive, support related to Microsoft products and services some of this data may contain personal data. For more information, see Microsoft Support and Professional Services Data Subject Requests for the GDPR.	Lowers risk

3.2	Low risk that users utilise Microsoft Office for a new data processing 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 training, terms of use and expectations.	Lowers risk
3.3	Low risk that user details will change and need to be changed in the hosting account.	Microsoft Office hold limited personal data for account holder – If details change the account will need to be modified. Identify the system administrator and the process for ensuring details are updated.	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 on Microsoft Office, but have ensured where possible, additional processing has been opted out. Privacy https://privacy.microsoft.com/en-gb/privacystatement Host will invite attendees to Microsoft Office meetings via email. Email provider will have a trail of all invites sent out and can request Microsoft Office delete and stored meta data. Meeting Metadata: Topic, Description (optional), participant IP addresses, device/hardware information To make a request, please contact our Privacy Team 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	Moderate risk that users will not have their access revoked when they leave school / their contract ends.	There will be a process in place for administration staff to inform the system administrator and request the deletion of the account. Microsoft will permanently delete accounts once they have been deleted by the user.	Lowers risk

3.6	Moderate risk that ICT admin staff will not be able to locate all relevant personal information stored on Microsoft Office to be able to respond to an SAR.	We have to request any information from Microsoft as we have no access to this. You can request a copy of the personal data. https://blogs.microsoft.com/datalaw/our-practices/	Lowers risk
3.7	Low risk of difficulty complying with Right to Rectification and Right to Erasure as only basic information is stored.	From Privacy policy - https://Microsoft Office.us/privacy Erasure**:** You can request that we erase some or all of your personal data from our systems. Microsoft Office DPA also includes: Following completion of the Services, at Customer's choice, Microsoft Office shall return or delete the Personal Data, except as required to be retained by law, rule or regulation that is binding upon Microsoft. If Customer and Microsoft Office have entered into Standard Contractual Clauses (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Microsoft Office to Customer only upon Customer's request.	Lowers risk
3.8	Low risk that staff might accidentally share personal data with another individual or organisation.	Sharing is only enabled within the tenancy and therefore, within the organisation – with those with the same @X. Derbyshire.sch.uk email address. When emailing externally users should use BCC for groups of individuals and keep address books updated.	Lowers risk
3.9	Medium risk that we will have an issue with data transfers outside the EEA.	Standard Contract Clauses. Only if Microsoft chose to back up in USA	Lowers risk.
3.10	Medium risk that the school will struggle to identify and delete all personal information held by Microsoft at the end of its retention period.	Ensure data maps, information audits and ROPA are kept updated. Ensure there is a regular review of data stored and have a documented process for reviewing the data staff backup to the cloud / save in OneDrive.	Lowers risk

3.11	Medium risk of issues if staff use Microsoft Office video conferencing facilities	Provide video conferencing guidance and include the need to secure meetings, restrict the roles of the attendees and are aware of data visible on their screens.	Lowers risk.
3.12	Low risk that a data breach occurs because ICT admin staff are not sufficiently trained and familiar with Microsoft Office to be able to correctly configure all features for optimum privacy.	Hosts will be given time to investigate all settings available to the host account and make sure it is restricted as much as possible. Training regarding how to use Microsoft Office will be undertaken by staff who will have access to the service.	Lowers risk.

5. Compliance with Guidance/Codes of Conduct

5.1 Identify any applicable guidance and/or codes of conduct issued by the Government, the ICO, the Commission or any relevant association or body:

NA

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

SCCs Customers of Microsoft business cloud services benefit from compliance with the Standard Contractual Clauses (also known as EU Model Clauses) under the Microsoft Online Services Terms, unless the customer has opted out of those clauses.

6. Involvement of Data Subjects

6.1 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.

6.2 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:

Microsoft Office will help the School fulfil its obligations, reduce the number of disparate platforms, thereby limiting data sharing and saving public funds.

7. DPIA Review

7.1 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 children's accounts are added to the system.

8. 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	13/03/21	TB
Consult with DCC GDPR team, DPO and Governors	May 2021	TB
Approval of the final version of this DPIA by DPO	15/3/21	TB
Update information asset register/map	June 2021	TW / ML
Amend Privacy Notice(s)	June 2021	TW / ML
Amend relevant policies e.g. Information Security Policy, IT Policy and Acceptable User Agreement, Safeguarding and Child Protection Policy	September 2021	TB
Establish regular review of this DPIA and the function of the software	May 2021	TB

Appendix A: Evidence of due diligence of supplier/s

The Terms and Conditions and Privacy Policies of the following have been checked:
Microsoft
https://privacy.microsoft.com/en-gb/privacystatement
ICO Registration Number: Z6296785

For Microsoft products provided by your K-12 school, including Microsoft 365 Education, Microsoft will:

- not collect or use student personal data beyond that needed for authorised educational or school purposes;
- not sell or rent student personal data;
- not use or share student personal data for advertising or similar commercial purposes, such as behavioural targeting of advertisements to students;
- not build a personal profile of a student, other than for supporting authorised educational or school purposes or as authorised by the parent, guardian or student of appropriate age; and
- require that our vendors with whom student personal data is shared to deliver the educational service, if any, are obligated to implement these same commitments for student personal data.

Terms and Conditions: https://www.microsoft.com/en-gb/servicesagreement/

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. and by urgent message to users
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	Potentially
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?	Interaction with school MIS. School will check email addresses 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

