

# Biddenham International School & Sports College

## STAFF CLOUD AND WEB SERVICES POLICY

### Introduction

Biddenham School provides Google Workspace for Education as our primary cloud storage provider. Only Google Workspace services provided under the @MyBiddenham.com domain are supported for use in school. Personal Google or other cloud service accounts (such as Microsoft Skydrive, Dropbox, Apple iCloud, or Amazon EC2) **should not** be used under any circumstances for school business or for communication with students. Only Cloud and Web services recommended and supported by the ICT Strategy Group should be used in school supported by the appropriate data sharing agreements.

You may decide within your department which curriculum resources it is appropriate to store on Google Workspace for Education (Google Drive/Shared Drives provided by school), however, you should be aware that data not stored on Biddenham servers is outside the control of the school and as such you assume certain risks with regard to recovery and accessibility of data.

Cloud Services have huge benefits for collaboration and sharing of information, but there are also risks that you should be aware of when using these services. The following is not to discourage your use of cloud services, but to allow you to make informed decisions on the most appropriate place to store Biddenham's data.

Basic data storage information:

| Biddenham Storage  | Cloud Storage (Google Drive)  |
|--|---|
| Multiple daily backups/versioning 7am/12pm.                        | Incremental Document versioning.  |
| ~ 12 month data retention period for all data on tape.             | A few weeks data retention if document has been deleted from the 'Bin'. |
| Availability is reliant on network access.                         | shared drive's trash within the last 25 days                            |
| Biddenham IT Services take responsibility for the storage of data. | Availability is reliant on Internet access                              |
| Biddenham controls access to all data.                             | You take responsibility for the storage of data.                        |
|  | Google ultimately has control of data.                                  |

### Definitions

Biddenham School defines **Cloud Services** as any storage solution which stores school data in a storage facility not hosted within Biddenham School.

**Information Assets** are defined as any digitally stored data (including, but not limited to, documents, images, and media) which has informational or financial value or which contains information covered by the Data Protection act. This may include, but is not limited to, detailed student, parent or personnel information; images or digital recordings of students; financial data; reports generated from SIMS; and data which by law has to be retained for a specific period of time.

Some guidelines to help you identify an Information Asset are:

- Does the information have a value to Biddenham School?
- Will it cost money or time to reacquire or duplicate?

- Could there be legal, reputational or financial repercussions if you could not produce it on request?
- Would it have an effect on operational efficiency if you could not access it easily?
- Would there be consequences of not having it?
- Is there a Data Protection risk associated with the information?
- Is there a risk arising from inappropriate disclosure?
- Would disclosure of the information break Data Protection requirements?

## **Appropriate Use**

All Biddenham School Information Assets are to be stored on server systems hosted by Biddenham School's IT Services Department. Information assets within these systems are resilient to failures and multiple backup copies are kept in multiple secure locations.

You may decide within your department that specific curriculum resources are appropriate to store on Google Drive\Shared Drives or the school network.

Biddenham IT Services must be consulted about the use of cloud storage and management of information assets if there is doubt on its appropriate or correct use.

It is the responsibility of each member of staff to ensure that you are meeting the requirements of this document.

Do not store online any information which could cause significant disruption to school services if inaccessible or lost for any period of time. If you do wish to store data of this type online, always ensure an up to date duplicate is kept on school servers.

Several Google Workspaces allow you to make data public. In some instances - for example Google Sites, and Blogger - information is public by default.

All Staff should support the safe and appropriate use of cloud and web services in lessons and should not encourage students to use services that are not suitable or could result in students leaking personal information online.

Any external Cloud or web based service that you would like the students to use needs to be vetted, terms of service read and a data agreement setup if the school is to sign up to the service (to comply with GDPR). To use a service you need to perform a 'Data Protection Impact Assessment' (a risk assessment) this will identify what the data usage is, benefit of using the service and potential risks to data (supporting information and guide will be held with the Data Protection Impact Assessment form).

Most online services have a minimum sign up age and this can vary from 13-18, under the GDPR and Data Protection Act 2018 only children aged 13 and above are able to provide their own consent for commercial internet services to process their personal data. So in some cases you would need written consent from the parent/carer of students under the age of 13 (this data would need to be recorded and stored). Web hosting and video websites where you publish data/media also tend to have a higher age limit and as such the only web publishing services you should be endorsing the use of are Google Sites and Blogger (both Google provided services).

Under no circumstances should you ask a student to sign up to services they are not allowed to use under the providers terms of service or GDPR. This means forward planning is needed for any future use of cloud or web services, it is unreasonable for you to find a new service and expect to start using it immediately.

If you choose to use a service that the school does not provide you are “asking” the student to sign up and submit data and by doing this enter into a relationship between them (the student) and the company and this should be expressed. They also have the right to refuse to use the service and need to adhere to the terms of service including age etc this needs to be declared and checked prior to asking the students to sign up.

This has to be considered every time we look at using external service and we would rather student only sign up to services managed by the school.

A Data Protection Impact Assessment is available on the Staff Homepage under IT Services.

A list of supported services with data sharing agreements is available from the DPO/IT Services or SLT.

## **Legislation and Information Assets**

There are many situations where data created by Biddenham staff requires stringent protection which must satisfy both school regulations and government legislation. When choosing where to store your data you need to take the following into consideration. Failure to do so may result in legal action against yourself and the school.

- Those working with student or personnel data should be aware that you have legal obligations to protect and retain personal information. The Data Protection Act requires you to:
  1. Keep data secure.
  2. Ensure it is relevant and up to date.
  3. Only hold as much as you need and only for as long as you need it.
  4. Allow the subject of the information to see it on request.
- You must ensure that data retention and deletion policies are followed and that data can be produced on request in order to fulfil requirements of the Data Protection Act 1998.
- If there is any doubt regarding the classification of data you must seek advice from the IT Services Department.
- All data generated in carrying out your duties belongs to Biddenham School.
- The Freedom of Information Act gives students the right to see not only their personal information which is held by an academic institution but also their educational records. If a request by a student is made the relevant information must be supplied within 20 working days.

## **Limitations of Use**

This Code of Practice is specific to school Information Assets only and does not pertain to any personal data.

## **Your Google Workspace Account**

Your Biddenham Google Workspace account may be closed or suspended or related services restricted at the discretion of the Network Manager under the following circumstances: your employment at the school has ended; you are taking a leave of absence; as part of an ongoing or potential disciplinary procedure; or where the Cloud Services Code of Practice is thought to have been breached. An appeal of this decision can be made to the headteacher.

Under certain circumstances access to services may be restricted by Google without involvement of Biddenham. For example, if you create a blog on Blogger.com and breach the terms of service of the site by, for example, sharing copyrighted music, your access to Blogger.com may be restricted permanently. In circumstances such as this there is little action that we can take and your blog would be considered lost with continued access to Blogger at the discretion of Google.

You only have full control over a file stored in Google Drive if you are set as an Owner. Files for which you are not the owner can be edited and deleted without your permission and will be unrecoverable.

Once your Google Workspace account has been deleted all data held associated with it (including Google Drive files, Blogs, Calendar data, Emails etc.), and **any shared content of which you are the owner** will be permanently deleted within five days. Biddenham IT Services takes no responsibility for any data lost as a result of closing an account. It is your responsibility to ensure this data is backed up. There is no possibility to recover deleted data after the five day period.

#### Student Contact with outside Services\Contacts

Students by default are blocked from receiving external communication with all outside agents. We then have a bypass rule to allow an approved list of businesses\services and educational establishments (no lone non professional businesses\services and educational email is to be included\approved). This implementation means that students could not have contact with persons external to the school without first vetting the businesses\services and educational establishment to see if it is legitimate and that the businesses\services and educational establishment has an acceptable reputation or leadership structure in the event of misconduct.

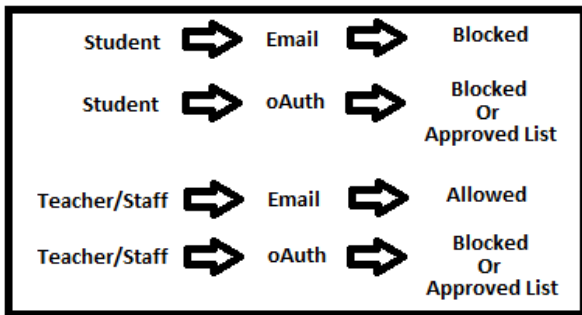
#### Google Authentication (oauth)

Signing into services using your Google Workspace account is disabled by default for external services. This is to limit the giving out of personal information when signing up to external services such as date of birth or any other questions that may be automatically completed/requested on sign up. As more and more websites have started to use oauth (i.e. signing in with Google account) the list of sites the staff/students have the ability to access with "one click" has also increased with a number of the sites holding no educational merit. Additionally to this the services are now integrating into Google Service allowing the transfer of data into/out of Google Drive and Classrooms. To protect this data all new signups are blocked for both staff and students alike and all unknown services have had their permissions revoked. If staff would like to access a new service they will need to sign up manually with email and password to test the service. Once tested the services can be allowed by IT Support or in the event that we feel the data access is deemed inappropriate or that it requires too much access but the service however has merit and could/will be a valued educational tool the staff member can start the Data protection impact assessment.

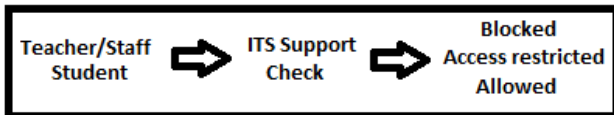
The data flows are shown below for the DPIA and will follow the existing practice.

\*This will mean staff still have the flexibility to look at new teaching tools without the risk to any Google services.

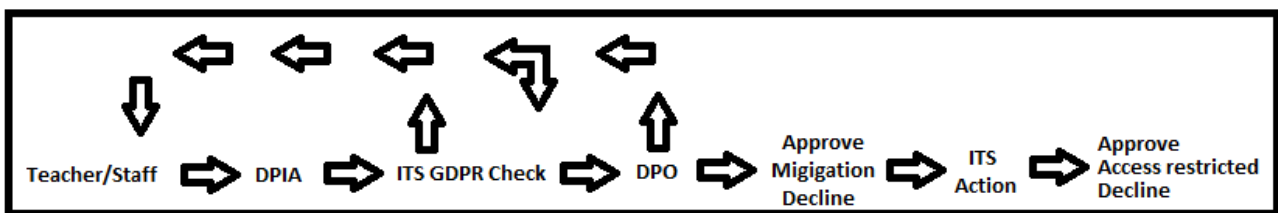
### Default Access



### Access Request



### DPIA Approval Process



## More Information

ICO: <https://ico.org.uk/>

Data Protection Act 2018: <https://www.gov.uk/government/collections/data-protection-act-2018>

Freedom of Information Act: [www.legislation.gov.uk/ukpga/2000/36/contents](http://www.legislation.gov.uk/ukpga/2000/36/contents)

For more information, email: [helpdesk@biddenham.beds.sch.uk](mailto:helpdesk@biddenham.beds.sch.uk)

Date of Next Review: **May 2024**