Information Governance
Support Services
by Stockport Council

Securing Data Sharing in Schools

Ensuring Enhanced Security in Digital Collaboration

Data protection law requires schools and organisations to process personal data securely, with appropriate organisational and technical measures in place. The security measures must be “appropriate” to the nature, scope, context and purpose of the processing and the risks posed to the rights and freedoms of individuals.

Schools must also take into account the various security measures available and the costs of implementation when determining what measures are appropriate for their circumstances.

Responsibility for data that has been shared

Any organisations that schools share data with take on their own legal responsibilities for that data, including its security. However, schools should still take reasonable steps to ensure that the data they share will continue to be protected with adequate security by the recipient organisation and should;

- ensure that the recipient understands the nature and sensitivity of the information;
- take reasonable steps to be certain that security measures are in place, particularly to ensure that you have incorporated an agreed set of security standards into your data sharing agreement, where you have one; and
- resolve any difficulties before you share the personal data in cases where you and the recipient organisation have different standards of security, different IT systems and procedures, different protective marking systems etc.

Sharing Data Securely

In an era where data breaches are more common, ensuring secure and efficient data sharing is paramount for organisations. A preferred method of data sharing is to share data internally and externally by secure network links. For large files, transfer using a secure protocol is sometimes necessary, Google Drive, Google Workspace, Microsoft OneDrive and Microsoft SharePoint offer robust solutions for secure data sharing through direct links.

This document outlines the security benefits of each of the platforms and the steps to share data securely. These options also enable sharing of data with specific people to limit data being shared with the wrong recipients alongside password protected documents and files where required to further enhance secure sharing.

By leveraging the secure sharing capabilities of Google Drive, Google Workspace, Microsoft OneDrive and Microsoft SharePoint, schools and organisations can protect sensitive data while ensuring efficient collaboration. Each platform provides robust encryption, access control, and compliance features to safeguard information.

Following the outlined steps for each application will help ensure that data is shared securely.

When thinking about sharing data, as well as considering whether there is a benefit to the data sharing and whether it is necessary, you must consider your overall compliance with data protection legislation, including fairness and transparency. Before any data transfers are made, consider the following;

- Is the sharing necessary and proportionate to the issue you are addressing?
- What is the nature of the information, its sensitivity, confidentiality, or possible value? What is the size of the data being transferred?
- Is it fair to share data in this way? What damage or distress might be caused to individuals as a result of any loss or unmanaged sharing during transfer?
- What implications would any loss or unmanaged sharing have for the school?
- What is the minimum data you can share to achieve the aim? Could the objective be achieved without sharing any personal data, or by sharing the minimum personal data?

Limiting access to information shared

The data protection security principle goes beyond the way you store or transmit information. Every aspect of your processing of personal data is covered, not just cybersecurity. This means the security measures you put in place should seek to ensure that data can be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority you give them) additionally the Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 describes that public authorities must be able to trust their information. To do this,

- they must be able to establish when information was created and who it was created by;
- have in place policies and processes for information security that comply with relevant legislation, guidance and codes of practice;
- apply access and permission controls throughout the life of the information to prevent unauthorised or unlawful access;
- have appropriate technical and organisational measures to prevent accidental loss, destruction or damage, to their information.

Google and Microsoft both offer powerful sharing capabilities that allow users to collaborate and share files seamlessly. However, there might come a time when you need to stop sharing certain files to maintain privacy or control over your documents both Google and Microsoft provide features that allow you to limit access to shared data by a specific timeframe using expiration dates where enabled. Both platforms offer flexibility and control over how and when data can be accessed, ensuring that security and compliance is maintained according to specific needs.

Google

Google Drive

Security Benefits

Google Drive employs several layers of security to protect data:

- Encryption: Files are encrypted in transit and at rest using SSL (Secure Sockets Layer)/ Transport Layer Security (TLS) and 128-bit AES (Advanced Encryption Standard) keys.
- Access Control: Granular permissions can be set to determine who can view, comment, or edit the files.
- Two-Factor Authentication (2FA): Adds an additional layer of security to user accounts.

Steps to Share Data Securely

1. Select the file or folder you wish to share.
2. Click the Share button.
3. Enter the email addresses of the people you want to share with or generate a shareable link.
4. Set the access permissions (Viewer, Commenter, Editor).
5. Click Send or Copy Link to distribute the link.

Google Workspace

Security Benefits

Google Workspace integrates tightly with Google Drive, providing enhanced security:

- Encryption: Uses 128-bit AES keys for data at rest and SSL (Secure Sockets Layer)/ Transport Layer Security (TLS) for data in transit.
- Compliance: Meets various compliance standards including UK GDPR, ISO 27001.
- Endpoint Management: Allows admins to manage devices accessing the data.

Steps to Share Data Securely

1. Open Google Drive within Google Workspace.
2. Select the file or folder to share.
3. Click the Share button.
4. Enter the email addresses or generate a shareable link.
5. Set the desired permissions (Viewer, Commenter, Editor).
6. Click Send or Copy Link to distribute the link.

Google – Stop sharing

To stop sharing your files in Google Drive, follow these steps:

1. Open Google Drive and navigate to the file or folder you wish to stop sharing.

2. Right-click on the file or folder and select "Share."
3. In the "Share with people and groups" window, you will see a list of people who have access.
4. To remove someone, click on the drop-down menu next to their name and select "Remove."
5. If you want to stop sharing the link, click on the "Get link" section and change the access to "Restricted."
6. Click "Done" to save your changes.

This will revoke access to the shared file or folder, ensuring that recipients can no longer view or edit the content.

Google Expiration Dates

Use the "Expiration" feature in Google Drive to set an expiry date for files shared with others. This feature is also available for Google Workspace accounts. Once the expiration date is reached, the recipient will no longer have access to the file.

Microsoft

Microsoft OneDrive

Security Benefits

OneDrive offers comprehensive security features:

- Encryption: Data is encrypted in transit using Transport Layer Security (TLS) and at rest using BitLocker and per-file encryption.
- Access Control: Permissions can be set to manage who can view or edit files.
- Advanced Threat Protection: Monitors and protects against malware and phishing.

Steps to Share Data Securely

1. Select the file or folder you wish to share.
2. Click the Share button.
3. Enter the email addresses of the recipients or generate a shareable link.
4. Set access permissions (View, Edit).
5. Click Send or Copy Link to distribute the link.

Microsoft SharePoint

Security Benefits

SharePoint offers enterprise-level security:

- Encryption: Data is encrypted at rest and in transit using TLS (Transport Layer Security) and BitLocker.
- Access Control: Allows detailed permission settings for users and groups.
- Compliance Features: Supports UK GDPR, ISO 27001, and other compliance standards.

Steps to Share Data Securely

1. Navigate to the file or folder you wish to share in SharePoint.
2. Click the Share button.
3. Enter the email addresses of the recipients or generate a shareable link.
4. Set the appropriate permissions (View, Edit).
5. Click Send or Copy Link to distribute the link.

Microsoft - Stop sharing

To stop sharing your files in Microsoft 365, follow these steps:

1. Open OneDrive or SharePoint Online.
2. Navigate to the file or folder you wish to stop sharing.
3. Click on the shared icon next to the file name.
4. In the Manage Access pane, you will see a list of people who have access. Click the “Stop sharing” option next to the link or individual you want to remove.
5. Confirm your action to stop sharing the file or folder.

This will immediately revoke access to the shared file or folder, ensuring that the recipients can no longer view or edit the content.

Microsoft Expiration Dates

Use SharePoint Online and OneDrive to set expiration dates for sharing links. This feature allows you to specify a date when the shared link will expire, thereby restricting access to the data after the set timeframe.

Further Guidance and information

For further information about this guidance, data protection, information security and governance please contact: igschoolsupport@stockport.gov.uk.

Information Governance
Support Services
by Stockport Council