Information governance guidance for schools

Audience

All staff, governors and learners in maintained schools including pupil referral units.

Overview

This document aims to provide advice and guidance for schools in relation to storage of information within the Hwb+ platform (which includes Microsoft Office 365).

Action required

None – for information only.

Further information

Enquiries about this document should be directed to:
Digital Learning Unit
Digital Learning Division
School Standards and Workforce Directorate
Welsh Government
Cathays Park
Cardiff
CF10 3NQ
Tel: 0845 010 3300 (English-medium enquiries)
0845 010 4400 (Welsh-medium enquiries)
e-mail: hwb@wales.gsi.gov.uk

Additional copies

This document can be accessed from the Welsh Government's website at www.gov.wales/educationandskills

 WG26231 Digital ISBN 978 1 4734 4464 5

Contents

Introduction

This document aims to provide advice and guidance for schools in relation to storage of information within the Hwb+ platform (which includes Microsoft Office 365).
The guidance will explain what sensitive information is, how it should be protected and will inform the reader about:

- the meaning of information governance;
- school and staff responsibilities in relation to Data Protection;
- data classification;
- information handling; and
- cloud storage.

Intended audience

- School staff;
- learners; and
- school governors.

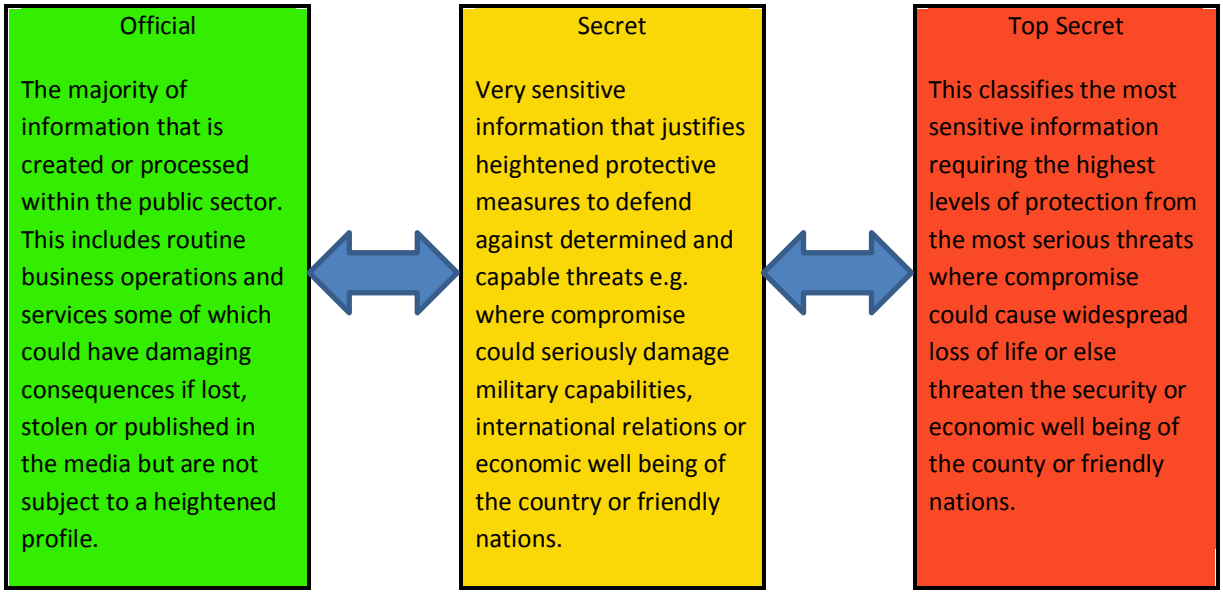
Elements of this document should be made available to everyone within and associated with the school as appropriate.

Information governance

Information governance is an approach to the way an organisation handles its information. It allows organisations and individuals to ensure that personal information is processed in accordance with legislation and enables the establishment to ensure that its information is effectively and efficiently processed.

Data classification

The government classification scheme changed in April 2014 from the old protection marking scheme of five categories (Protect, Restricted, Confidential, Secret, Top Secret) to the new scheme which has three categories (Official, Secret, Top Secret) The new categories are defined as follows:



As can be seen above, information processed within the school environment will fall into the “Official” category. A limited subset of official information could have more damaging consequences if lost or stolen and should be marked as “Official – Sensitive”. This subset of data should have enhanced controls because it needs to be better protected due to the higher impact of unauthorised access. Enhanced controls could include password protecting or encrypting the relevant files as appropriate.

What is personal or sensitive information?

Personal information is defined by the Data Protection Act 1998 as:
“data which relate to a living individual who can be identified or from those data and other information which is in the possession of, or is likely to be in the possession of the data controller and includes any expression of opinion about the individual and

any indication of the intentions of the data controller or any other person in respect of the individual"

Sensitive information is defined as:

"consisting of information as to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, the commission or alleged commission of any offence or any proceedings related to any such offence or alleged offence …"

Hwb+ and Microsoft Office 365

Hwb+, the all-Wales learning platform, was launched on 12 December 2012 and has the capability to provide an individual and customisable learning platform for every school in Wales. Since its launch, the platform has been further complemented by an extensive suite of digital content resources and a wide range of e-Safety support materials and tools which have been made available through Hwb, the National Digital Content Repository.
Hwb+ has been developed using Microsoft's technology stack which underpins all of the platforms' key functionality. This approach has ensured that the platform is fully scalable and suitably robust to fully meet the needs of a national platform deployment.

This Welsh Government centrally-funded initiative provides a wide range of financial and pedagogical benefits consistently across all schools in Wales. The potential for local cost savings are significant when you consider that locally delivered services such as e-mail and storage are now available through Hwb+.

One of the major benefits of the Hwb+ platform is the integration of online tools; most notably Microsoft Office 365. Providing online tools via the national Hwb+ platform allows for a consistent approach across all schools and ensures that there is not a proliferation of different systems and protocols in place.

Microsoft Office 365 provides a suite of free web applications including Microsoft Word, Excel, PowerPoint and OneNote. Microsoft Office 365 also provides every Hwb+ user with an individual e-mail address and access to a large online storage area known as OneDrive. OneDrive will allow users to store all of their digital content in one place which will reduce the complexities of having their digital content stored in a range of locations.

It is important to note that Hwb+ and Microsoft Office 365 have not been designed to store sensitive information. Sensitive information should be stored with appropriate protection in place.

Care when using Hwb+ and Microsoft Office 365

All users (school staff and learners) should be reminded to follow basic general security rules. These include:

- never let anyone use your account to access Hwb+ or Microsoft Office 365;
- never use someone else's account to access Hwb+ or Microsoft Office 365;
- be mindful when accessing Hwb+ or Microsoft Office 365 in a public place;
- ensure that your usage cannot be observed, especially when entering your password;
- don't be tempted to use Hwb+ or Microsoft Office 365 for purposes other than related to school business; and
- always report concerns about inappropriate usage. Local procedures should be followed as necessary.

Managing information within Hwb+ and Microsoft Office 365

Users should be aware of all personal information stored within the systems. The following table can be used to help users decide whether information could or should be stored within Hwb+ and / or Microsoft Office 365:

Control	Suitability	Examples
Would I be happy for this information to be openly shared on the Internet?	Store within Hwb+ or Microsoft Office 365.	Learning resources; General e-mail exchanges not including any student details; Public events; Lesson plans.
Would I be happy for this to be shared in the classroom?	Consideration should be given before storing within Hwb+ or Microsoft Office 365.	E-mail exchanges containing classroom activity; Information on class trips.
Would I expect this information to be kept private?	Do not store on Hwb+ or Microsoft Office 365. Only systems with appropriate security should be used.	Sensitive information about learners or staff; Special educational needs information.

Please refer to Appendix A for further details on what information should and shouldn't be stored within Hwb+ and Microsoft Office 365.

Consideration should also be given to the device (and network) used to access. Remember the use of a family or public device to connect to Microsoft Office 365 could potentially give others access to information.

School Data Protection responsibilities

Each school has responsibility for the personal data which it collects. The Data Protection Act 1998 terms this role as "the Data Controller". The Data Controller has to ensure that the eight principles of the Act are followed. The underlying principle of the act and this guidance is that schools should do everything in their power to ensure the safeguarding of personal and sensitive information.
The Governing Body and the headteacher are responsible for compliance with legislative requirements relating to the use of information and ICT security and disseminating policy. The headteacher is also responsible for ensuring that users of systems and data are familiar with relevant aspects of the policies pertinent to data protection.

The eight Data Protection Principles can be found at Appendix B.

School staff responsibilities

School staff must ensure that all relevant policy guidance is read and understood. All staff with access to Hwb+ and Microsoft Office 365 must ensure that no sensitive information is put at risk of unauthorised access. Please refer to Appendix A, which will help to ensure that staff data usage does not put an organisation's personal data at risk.

Information handling

The Government has published local Government Data Handling Guidelines which instruct and inform on the best ways to ensure that data is used and protected efficiently and effectively.
The guidelines can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370725/PSN_local_public_services_data_handling_guidelines.pdf

Also the 360 degree safe Cymru self review tool from the South West Grid for Learning can help to inform schools about current levels of security. The 360 degree

safe Cymru Self Review Tool can be accessed via the Hwb website: http://hwb.wales.gov.uk. There are a range of template policies to support schools within the 360 degree safe Cymru tool.

Incident handling

An important part of information governance concerns the ability to recover from incidents. A suitable procedure should be in place to allow staff and learners to report incidents or suspected incidents.
The procedure should be documented and should describe a course of action which is to be followed. An example of a suitable procedure or data breach management plan is contained within the Acceptable Use Template document available through the e-Safety zone on Hwb.

http://hwb.wales.gov.uk/Resources/#resource/de0f0869-7cb9-4688-bce2-8b1945e905e7

Policy acceptance

A template acceptance / signature sheet is included at Appendix C. The template can be incorporated into existing acceptable use policies to highlight that staff understand their obligations in relation to information governance.

Poster overviews

Appendices D and E provide high level advice for teachers and learners to assist in ensuring that their use of personal or sensitive information adheres to school policy.

Appendix A: Information checklist

Recommendations on information that can be stored on the various platforms

Information Type	Storage Type		
	Within School	Hwb+	Office 365
Management Information Data			
Sensitive or personal information held within the schools MIS system	✓	✗	✗
Learner Details			
Date of birth	✓	✗	✗
Age	✓	✓	✓
Gender	✓	✓	✓
Year	✓	✓	✓
Class	✓	✓	✓
Year	✓	✓	✓
Admission Number	✓	✓	✓
Legal Surname	✓	✓	✓
Legal Forename	✓	✓	✓
Surname	✓	✓	✓
Forename	✓	✓	✓
Registration Group	✓	✓	✓
Subject	✓	✓	✓
Classroom management activities			
Sharing links to relevant, approved websites	✓	✓	✓
Sharing classroom documents	✓	✓	✓
Sharing appropriate images / videos of learner activities	✓	✓	✓

Sharing appropriate images / videos of learner work	✓	✓	✓
Hosting online discussions	✓	✓	✓
Setting, receiving and commenting on homework	✓	✓	✓
Collaborating with other teachers on planning and other documents	✓	✓	✓
Learners peer assessing	✓	✓	✓
Learners keeping a learning journal (e-portfollio)	✓	✓	✓
Teachers video-conferencing with other teachers / classes	✓	✓	✓

Appendix B: Data Protection Act (1998) Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

    a) at least one of the conditions in Schedule 2 is met, and

    b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

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

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

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

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. 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.

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

Appendix C: User acceptance template

It is recommended that this user acceptance statement is included in your existing acceptable use policies.

This document can be used to evidence the fact that members of staff have read and understood the Information Governance Guidance for Schools. It also acknowledges that the member of staff will endeavour to ensure that personal information is protected and will not be stored within Hwb+, including Microsoft Office 365, unless approval is received from the head teacher or deputy head teacher.

_____

I confirm that I have read and understand the Information Governance Guidance for Schools.

Name: _____

Role: _____

Signature: _____

Appendix D: Overview for teachers

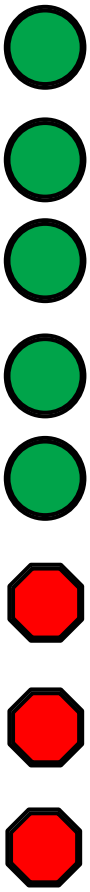
	
GO **Follow these good practices**	**STOP** **School Policy MUST be followed**

When using Office 365 teachers need to understand that any information stored is not held on their local device. All information is held within “the cloud”.

Teachers need to ensure that their use of personal or sensitive information adheres to school policy. The usage should not put any of the information at risk of unauthorised access.

Teachers must ensure that the following advice is followed:

- **Guidance regarding protection of school information must be adhered to**
- **Usage of Hwb+ and Office 365 should only be work-related and that usage must never put personal or sensitive information at risk**
- **Strong passwords should be used especially when the system being accessed contains personal or sensitive information. The passwords should not be shared with anyone. Passwords should never be saved within the device being used for access**
- **Keep in mind that teachers have a responsibility for the data in their possession and to the learners, parents or colleagues the information is about**
- **Users must never circulate, publish or store inappropriate content within Hwb+ or Microsoft Office 365**



Treat the school information as though it was your own personal or financial information

Incidents or suspected incidents should be reported to the head teacher or deputy head teacher of the school

Personal or sensitive information should be encrypted when it is being transported on any portable media e.g. laptop, pen drive, etc.

Install Anti-Virus Software on your phone, tablet or laptop

Mobile devices should be protected as though they were cash e.g. should not be left unprotected and in plain view in a vehicle, office, café, shop, etc.

Sensitive information should not be sent using e-mail unless held within a protected attachment

Sensitive information should not be stored within systems which have not been designed for the purpose

Information which you believe should only be discussed in private should not be sent via e-mail or stored within Hwb+ or Microsoft Office 365

It should be noted that usage of Hwb+ and the related use of Microsoft Office 365 cannot be considered personal. All usage is logged and monitored.

Appendix E: Overview for learners

	
GO **Follow these good practices**	**Stop** **School Policy MUST be followed**

When using Office 365 leaners need to understand that any information stored is not held on their local device. All information is held within “the cloud”.

Learners need to ensure that their use of personal or sensitive information adheres to school policy.

Learners should ensure that the following the dos and don’ts are followed:

- **Ensure passwords are strong and difficult to guess. A strong password is at least 8 characters long and includes an upper and lower case letter, a number and a special character. Hwb+ logins allow for easier to remember passwords for Primary age learners.**
- **Always make sure that you know who you are communicating with**
- **Make sure that what you are doing wouldn’t offend or hurt anyone**
- **Password protect and/or lock your phone, tablet or computer. Make sure that it is locked when you are not using it. Install Anti-Virus Software on your phone, tablet or laptop**
- **Tell your teacher if you have any concerns when using Hwb+**
- **If you think someone may have discovered your password change the password immediately.**

Never share your password with anyone.

Don’t open files from strangers

Don’t follow links within e-mails unless you know the sender

Don’t supply personal information via a web page unless you are confident that the site is genuine – don’t be tricked!

Don’t store personal or sensitive information within Microsoft Office 365 or Hwb+

Don’t use Microsoft Office 365 to threaten, offend or harass other users

It should be noted that usage of Hwb+ and the related use of Microsoft Office 365 cannot be considered personal. All usage is logged and monitored.