Llywodraeth Cymru
Welsh Government

Information security guidance for schools

Guidance

Guidance document no: 206/2016
Date of issue: August 2016
Replaces guidance document no: 186/2015

Information security 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
Operations 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

Mae'r ddogfen yma hefyd ar gael yn Gymraeg.
This document is also available in Welsh.

OGL © Crown copyright 2016 WG29506 Digital ISBN 978 1 4734 7354 6

Contents

1. Introduction 2
2. Information security 3
3. Personal data 4
4. Data classification 5
5. General advice 6
6. Hwb 7
7. Hwb+ 8
8. HwbCloud 9

Appendix A: Data protection definitions 14
Appendix B: HwbCloud controls summary 15

1. Introduction

Hwb is the Welsh Government's digital learning solution for schools.

The following diagram illustrates the different aspects of Hwb.

This document describes the controls available across the range of digital tools in Hwb and how these tools can be used to enable schools to maintain the security of the information they use.

The guidance provided is generic in nature but reflects a typical school's usage based on information from meetings with a range of stakeholders including teachers, support staff and local authorities.

2. Information security

The intention of information security is to preserve the following properties:

- Confidentiality – ensuring information remains secret
- Integrity – ensuring the accuracy of information
- Availability – ensuring information can be accessed when required

In addition to these key attributes, there will be scenarios in which other properties will be of importance for example: accountability, non-repudiation and reliability.

3. Personal data

Information about identifiable individuals is personal data, the Data Protection Act (DPA) defines the legal requirements applicable to the use of personal data.

The DPA definition of personal data is included at Appendix A.

The precautions that should be taken are applicable irrespective of media type. For example, each of the following can require security measures if they contain personal data:

- e-mails
- photos
- electronic documents
- hand written notes

The guidance in this document is limited to controls applicable to electronic formats of data, if information is printed out it still needs to be protected, procedures should be consistent with those applicable to electronic documents.

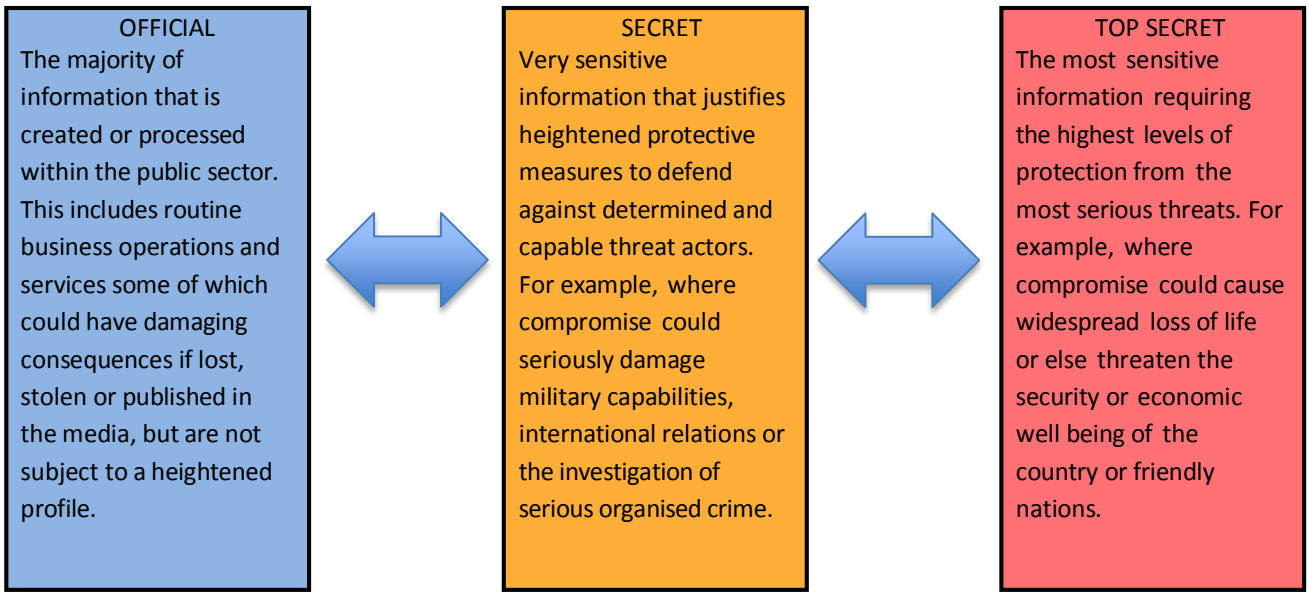
The Information Commissioner's Office (ICO) publishes guidance and codes of practice applicable to data protection and personal data on their website[1].

[1] www.ico.org.uk

4. Data classification

The Government classification scheme changed in April 2014 from a protective marking scheme using five categories (PROTECT, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET) to the present scheme which has three categories (OFFICIAL, SECRET and TOP SECRET).

The new categories are defined as follows:



Information processed within the school environment will fall into the OFFICIAL category.

For OFFICIAL data the information security outcomes should:

- protect against deliberate compromise by automated or opportunistic attack; and
- aim to detect actual or attempted compromise and respond

Full details are available in the associated Cabinet Office documentation[2].

[2] https://www.gov.uk/government/publications/government-security-classifications

5. General advice

All users (school staff and learners) should follow basic general security rules; these are generally applicable to any IT system and include:

- never let anyone else use your Hwb account
- never use someone else's Hwb account
- be mindful when using your Hwb account in a public place - ensure that your usage cannot be observed, especially when entering your password
- don't use your Hwb account for purposes other than related to school business
- always check email recipient details are correct before sending
- always report concerns about inappropriate usage - local procedures should be followed as necessary
- avoid use of public, shared or personal devices / systems for sensitive or personal data.

The use of personal devices, often referred to as 'Bring Your Own Device' (BYOD), will almost certainly introduce risks to the information processed on them, this is each school's risk management decision. The ICO has published specific guidance with respect to BYOD and data protection .

Hwb is not currently configured to control or check the devices accessing Hwb, instead there is a reliance on users following the local policies that are applicable to them.

6. Hwb

Hwb is the centrally-funded, digital learning platform intended for providing access to a range of digital content and tools.

As well as providing access to the wider Hwb solution, it also provides a gateway to additional content services, examples of which are illustrated below:

Hwb has been designed primarily to store educational content that can be shared with any other Hwb user.

Although access to the Hwb platform is only available to registered Hwb users, it is not intended to store sensitive data. Where schools are required to handle sensitive data, this should be done via HwbCloud as outlined below.

7. Hwb+

Hwb+ is the virtual learning environment that has been designed and built to provide a safe online learning environment for teachers and learners and enables collaboration using digital resources.

Hwb+ is primarily intended to be used for day to day school teaching activity and where relevant general personal data can be included, similar to the way personal data would be used in the classroom.

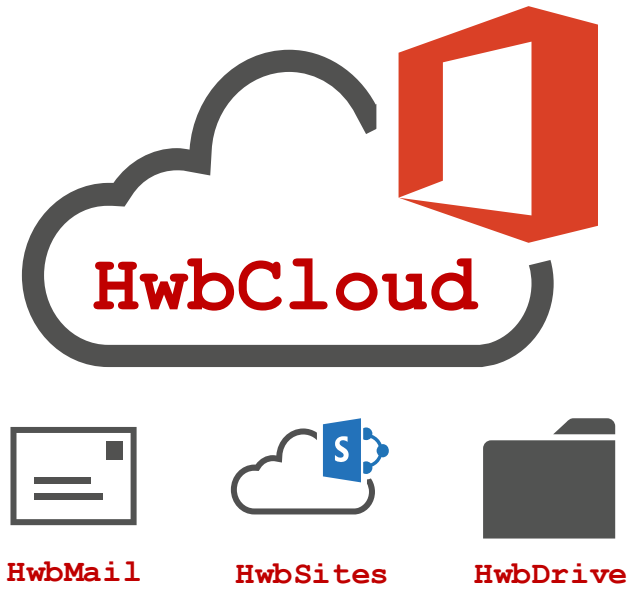
Although access to Hwb+ is only available to registered Hwb users, it is not intended to store sensitive data or for non-learning administrative activities. This should be done via HwbCloud as outlined below.

8. HwbCloud

HwbCloud is the most appropriate tool, for the exchange and storage of management information and documents, including information about staff and learners.

The functionality in HwbCloud is provided by Microsoft Office 365 and therefore benefits from the controls that have been incorporated into the service by Microsoft.

The following diagram illustrates the services currently available in HwbCloud.



8.1 Office 365

Microsoft's Office 365 solution is based on a core set of controls that make it suitable for processing both OFFICIAL and personal data, this has been formally recognised by:

- certification to international information security standards
- Pan-Government Accreditation
- on-going independent audits

Office 365 offers multiple options for users to store and share information. The choices available range from highly flexible and convenient options, through to secure options that use encryption to provide assurance that data will remain confidential.

The Welsh Government have reviewed the security options available in Office 365 and configured HwbCloud with the intention of providing a secure environment that caters for the typical usage scenarios in schools.

Note: The effectiveness of controls in HwbCloud is completely reliant on appropriate local policies and procedures, all users of HwbCloud need to be aware of these and understand the implications of not adhering to secure working practices.

8.2 HwbCloud Security

While the majority of users will not need to access or exchange sensitive information, it is recognised that some users will regularly access more sensitive information that justifies a greater level of protection; therefore, different levels of control are available.

In this document the controls are referred to as standard and enhanced – all users of Hwb will benefit from the standard controls, whereas the use of the enhanced controls will necessitate a specific configuration decision and may require users to select appropriate options when storing or sending information.

For personal data the decision about when to use enhanced controls lies with the data controller; at schools this will normally be the headteacher. As highlighted earlier in this document there is advice on the ICO website to assist headteachers decide what level of control is necessary.

The following sections provide guidance on how the different applications within Hwb365 can be used to handle personal data securely.

The following table illustrates typical use scenarios, there are likely to be legitimate reasons to deviate from this model depending on a school's specific circumstances; any such deviation is a local risk management decision.

Note: This table must be used in conjunction with the control selection flowchart applicable to each aspect of HwbCloud.

Scenarios	**HwbCloud Standard Controls**	**HwbCloud Enhanced Controls**
General school information including attainment data from SIMS, which does not include sensitive information.	☺	☺
Learner information from MIS, for example for use on school trips. Where sensitive medical information is included enhanced security should be considered. SEN data can often include sensitive information; a local decision should be made based on the context and content of the data to determine whether enhanced controls are justified.	😐	☺
Child safety investigations tend to be sensitive in nature and require confidentiality; this will normally necessitate enhanced controls.	☹	☺

A summary of the controls is included at Appendix B.

8.2.1 HwbMail

HwbMail is the e-mail system provided for all users of Hwb. It is a standards based e-mail system that benefits from a number of configuration options that can provide robust security.

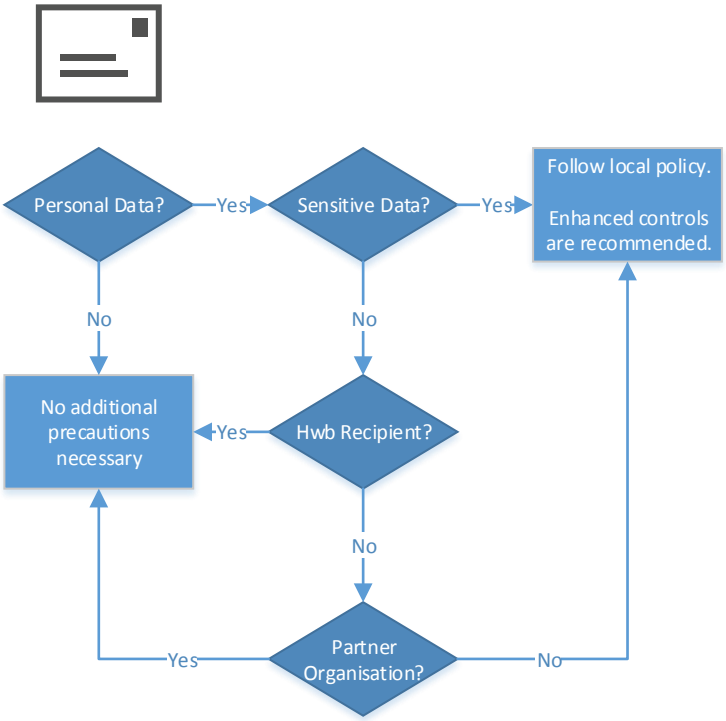
The default configuration of HwbMail provides a secure way of sending e-mail between HwbMail users as well as some partner organisations; the current list of verified partner organisations can be found on Hwb.

The list of partner organisations that are configured to receive secure e-mail from Hwb is established in conjunction with local authorities and regional education consortia.

Note: Until a partner organisation has been verified it should be assumed that e-mails will not be secure and enhanced controls considered.

HwbMail has additional options for encrypting sensitive e-mail, further guidance should be sought from your headteacher or local authority information security officer as required.

The following flowchart provides a graphical representation of the recommended decision process for deciding the appropriate encryption method for e-mails containing personal data, a similar process can be applied to other sensitive data.



8.2.2 HwbSites

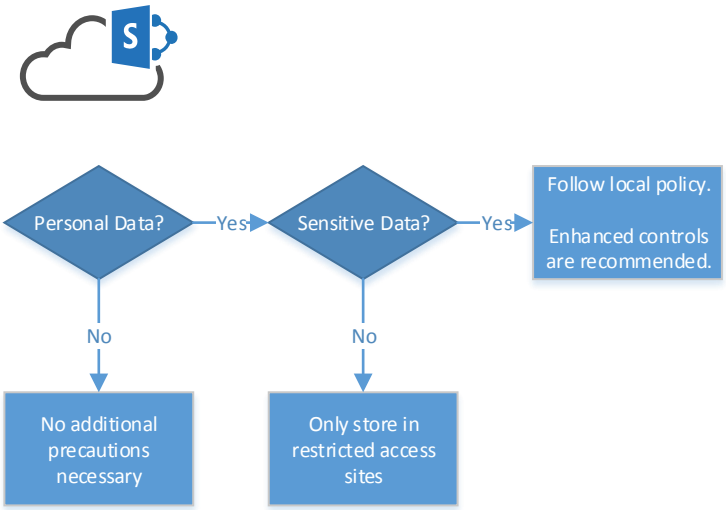
HwbSites are online workspaces intended to facilitate sharing of information between formally defined groups of users.

Due to the collaborative nature of HwbSites care should be taken when storing sensitive data in these areas. Specific sites for securely collaborating with sensitive data can be created to help ensure:

- access is constrained to those with a need to know the information
- enhanced protection for documents to reduce the risk of accidental release of information.

Note: The enhanced level of protection for documents will necessitate the use of the desktop version of Microsoft Office for creating and editing documents.

For staff with regular access to the most sensitive data additional authentication controls are available and should be considered (to help prevent password based attacks).



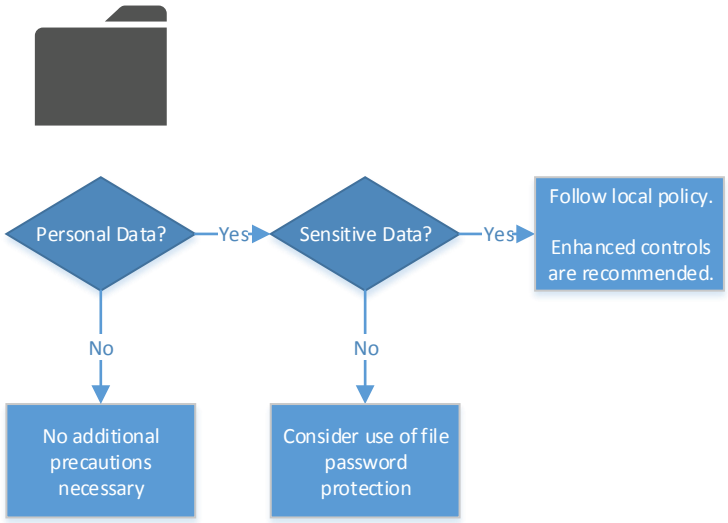
8.2.3 HwbDrive

HwbDrive is the personal online file storage area for Hwb users.

The absence of the need for multiple users to have access to a document enables password protection of individual files, which can be an effective way of ensuring only the originator can access the contents.

For highly sensitive data, individual file password protection is the most suitable control to provide assurance of confidentiality. In such situations advice should be sought about password complexity, length and distribution.

Note: Password protection is currently only available in desktop versions of Microsoft Office.



Appendix A: Data protection definitions

Personal data is defined by the Data Protection Act 1998 (DPA) as:

> ‘Data which relate to a living individual who can be identified:
>
> a) from those data, or;
>
> b) from those data and other information which is in the possession of, or is likely to come into 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 personal data is defined by the DPA as:

> ‘Consisting of information as to:
>
> a) racial or ethnic origin of the data subject
>
> b) his political opinions
>
> c) his religious beliefs or other beliefs of a similar nature
>
> d) whether he is a member of a trade union
>
> e) his physical or mental health or condition
>
> f) his sexual life
>
> g) the commission or alleged commission of any offence
>
> h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.’

Appendix B: HwbCloud controls summary

This appendix summarises the controls available in HwbCloud.

B1 HwbMail

B1.1 Enforced STARTTLS

Enforced STARTTLS is configured by the HwbCloud admin team and provides encryption of e-mail in transit through the use of TLS for e-mail sent between HwbCloud and verified partner organisations.

There is no user action necessary, it happens transparently according to pre-defined rules.

E-mails between HwbMail accounts will be encrypted using TLS as part of Microsoft's default Office 365 configuration.

B1.2 S/MIME

S/MIME can provide encryption of e-mails both in transit and at rest.

This is an option that is available to any Hwb user and can be configured locally and does not require the HwbCloud admin team to make any changes to HwbCloud.

Users with S/MIME setup must choose to encrypt e-mails in Outlook (otherwise the e-mail will be sent normally).

B1.3 HwbMessage Encryption

Hwb Message Encryption provides a way of sending e-mails so that the recipient access the contents via a secure portal. It provides encryption of e-mail in transit and because the e-mail does not leave the portal it is not stored on the recipient's device in the same way as a normal e-mail. E-mails are not encrypted in the sender's sent items folder.

Hwb Message Encryption has been configured to work automatically if a user includes the key words 'secure mail' or 'post diogel' in the subject line of an e-mail.

B2 HwbSites

The Hwb team have defined the following levels for combining enhanced controls for HwbSites. MFA and IRM are described in the following sections.

It is anticipated that Level 3 will be used for the majority of HwbSites, with Levels 1 & 2 being suitable for personal data depending on the sensitivity of the information.

Level	MFA	IRM	Sharing	Expected Number of Users
1	Yes	Yes	No	Few
2	Yes	No	No	Few
3	No	No	No	Many
4	No	No	Yes	Few

B2.1 Multi-Factor Authentication (MFA)

MFA in HwbCloud has been configured so that users can be required to use a code from the Azure Authenticator app in addition to their username and password.

The Azure Authenticator app is installed on a smartphone and will help to prevent password-based attacks, such as password guessing or observation during entry.

For MFA to be effective there is an assumption that staff with access to sensitive data will not share their phone with others or leave it unattended and unlocked.

Note: While MFA in Office 365 has other options the Hwb team have assessed the Azure Authenticator app as being the only appropriate option for HwbCloud.

B2.2 Information Rights Management (IRM)

In HwbCloud IRM is a form of digital rights management that has been created by Microsoft to provide additional control for document access rights, that 'travel' with the document.

In HwbCloud the use of IRM is currently constrained to supplementing the existing network access controls.

A HwbCloud document that has had IRM applied will require a user to provide credentials for access to the document, even when they are accessing it outside the online environment.

B3 HwbDrive

B3.1 Multi-Factor Authentication (MFA)

HwbDrive can benefit from MFA in the same way as HwbSites, see the relevant section for more information.

B3.2 Document level Password Protection

Microsoft Office's native password protection can be used to protect documents containing sensitive data.