Support for schools

Office 365 hints and tips

Solihull METROPOLITAN BOROUGH COUNCIL

Using encrypted/secure email

We all deal with sensitive information and issues sometimes. And we all have ethical and legal responsibilities to handle information safely.

Anyone can now send encrypted/secure emails using their Solgrid Office 365 account. Although this is an unusual thing for most Solgrid users to do, it makes sharing sensitive information safer *when* it is needed. These notes explain how it works and how to use it. Remember –

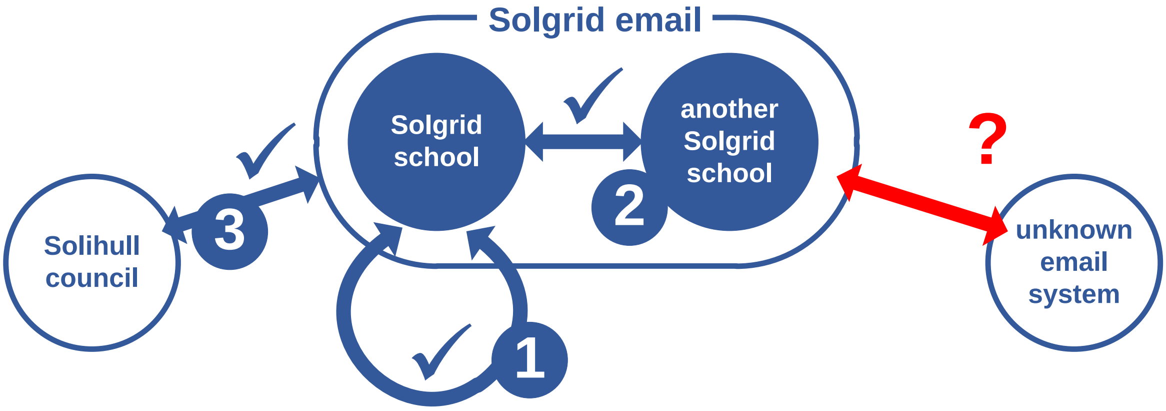
- ***No* email system will protect the information (and you) if you simply send it to the wrong person; and**
- **Encryption will not work if you don’t do it the right way.**

Please spend a few minutes reading this. It will save you time when you start to use encrypted email and help stop you make *some* mistakes.

Solgrid email security

We know that, if used properly, **any** Solgrid email is appropriately secure when:

- sending an email between two users in the same school (1);
- sending from one Solgrid school to another (2); and
- sending emails from any Solgrid school to and from Solihull council (3).



We know: that the **servers** used are secure enough; that the **connections between the servers** are secure enough; and that the access to the servers is secure enough - so you do not need to encrypt any emails between these users.

But we – and you – do not know how secure other email systems are.

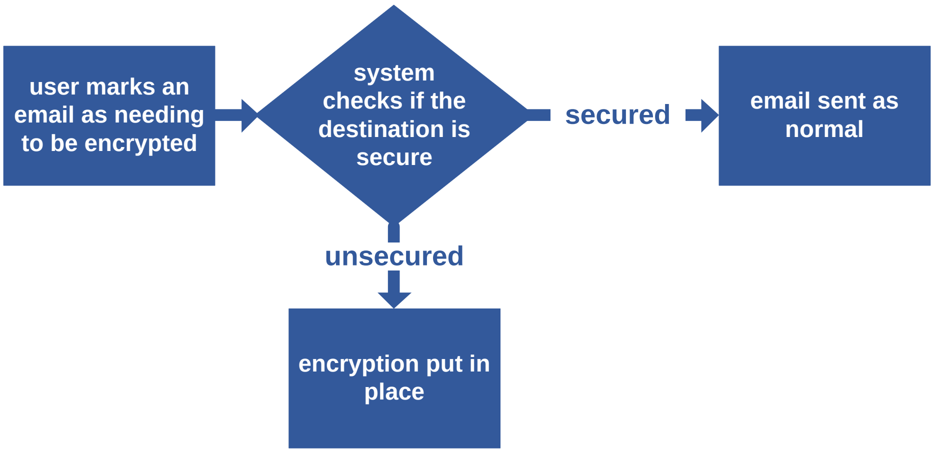
Email encryption

Email encryption stops sensitive emails being sent out to unknown email systems where we – and you – can't be sure how securely the email is being sent, stored or accessed.

The Solgrid email system holds the sensitive email and sends a notification to the *unsecure* recipient. The unsecure recipient can access the sensitive email (while it's still on our Office 365 email system) with a username/password or special passcode that they can be sent. They can reply to the email and so on but using our, secure, Solgrid email system.

This is much more secure – keeping *your* data safe – but, inevitably, harder for the unsecure email recipient to use. So, the Solgrid Office 365 system has been set up to only encrypt email when it has to be encrypted.

Solgrid email encryption


user marks an email as needing to be encrypted
system checks if the destination is secure
secured
email sent as normal
unsecured
encryption put in place

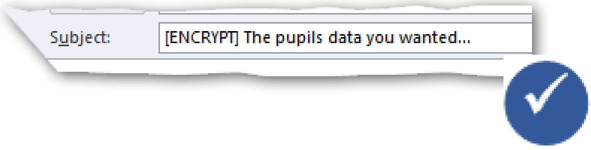
Marking an email as needing to be encrypted

You have to mark an email as being sensitive. There are two ways of doing this. Solgrid Office 365 can be accessed in different ways so you need to use the best way for you. There are separate notes about *when* to use secure email

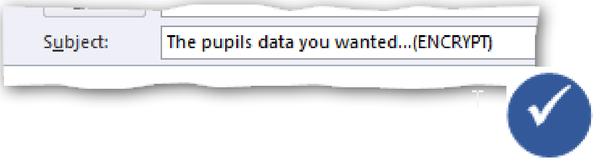
Putting an identifier in the subject line of the email

You can put **[ENCRYPT]** or **(ENCRYPT)** or **{ENCRYPT}** in the **subject** line of the email.

- It can go anywhere – with your actual subject in front or after it,
- It must be in block capitals.
- It must be enclosed in brackets, parentheses or curly brackets *that match*.



Subject: [ENCRYPT] The pupils data you wanted...



Subject: The pupils data you wanted...(ENCRYPT)

This will work in any email client – Outlook, Outlook Web Access, tablet apps or another email program.

You then just send the email as normal.

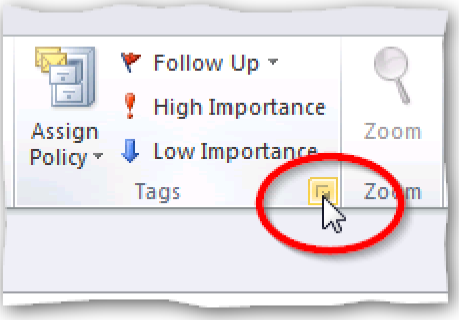
It will not work if you make mistakes in the spelling or capitalisation of ENCRYPT.

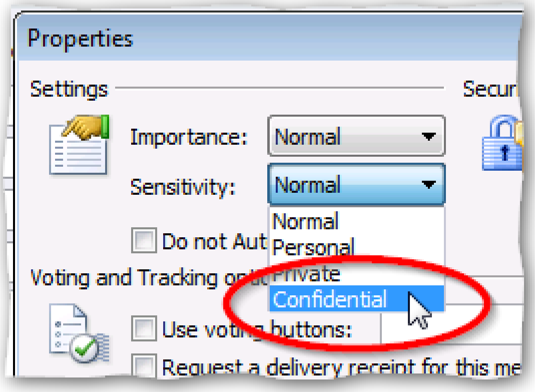
By flagging the message as *confidential* where a tag/flag is available

Microsoft Outlook and Outlook Web Access let you tag the sensitivity of a message as *normal*, *personal*, *private* or *confidential*. We have set the system to automatically encrypt all messages tagged as **confidential**.

Using Outlook 2010

You need to open the particular email's **properties** by clicking on **message options** marker for the email.





Properties

Settings

Importance: Normal

Sensitivity: Normal

Normal
Personal
Private
Confidential

□ Do not Aut

Voting and Tracking op

□ Use voting buttons:

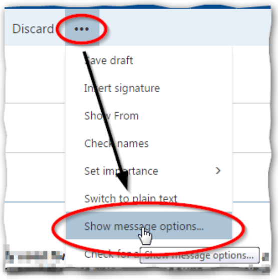
□ Request a delivery receipt for this me

Secur

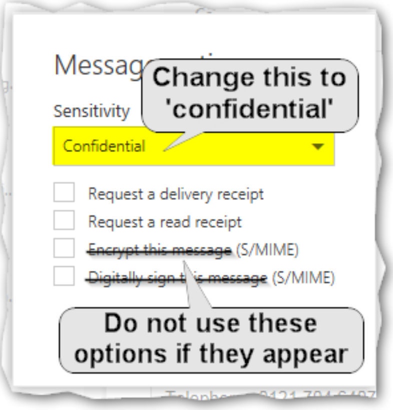
Then change the sensitivity to **confidential**.

Using Outlook Web Access

You need to **show message options** for the particular message.



And then change **sensitivity** to **confidential**.



Messag

Sensitivity

Confidential

Change this to 'confidential'

□ Request a delivery receipt

□ Request a read receipt

□ ~~Encrypt this message~~ (S/MIME)

□ ~~Digitally sign this message~~ (S/MIME)

Do not use these options if they appear

Do not use either of the **S/MIME** options *if* they appear as they will generate error messages. S/MIME is for encrypting between users in the same organisation and not necessary.

Then, once again, you just send the email as normal.

These ways of marking emails for encryption are less prone to error.

System detection

- *If the system detects that the recipient's email system is **secure**, the email is sent as normal.*
- *If the system detects that the security of the recipient's email system is not trusted to be secure, the system encrypts the email.*

What happens when someone receives an encrypted email?

The unsecure recipient is sent a notification, explaining that they've been sent an encrypted email. This has instructions attached to it.

The unsecure recipient is asked to download an HTML file that they have to open.

The unsecure recipient then either –

- requests that a special one-time passcode is sent (to the same email account) that they use to access the email – while it is held on a secure server; or
- uses a Microsoft identity account (such as a domestic Outlook account or a different system's Office 365 account) to access the email, again while it is held on the secure server. They can create a Microsoft identity if they need to – particularly if they expect to regularly get Office 365 encrypted emails.

Both of these allow a degree of authentication – the passcode can only be sent to the email account the system sent the encrypted email to or, alternatively, the Microsoft identity has to be linked to that account. That way, you're sure that the email is being accessed by the person you originally sent it to.

The unsecure recipient can use the secure server to reply to the email if they need to and download any attachments. But, for information, they can still forward it if they want to - even potentially to an insecure server.

- You can't stop someone misusing *any* information once you sent it to them in any way – for example, they could even screenshot something and leave it somewhere.
- But you have done everything you can reasonably do to protect the information. And to protect you and your school.

If you want to know more, or have any questions, please contact	
Name	**David Butt**
Email	**dbutt@solihull.gov.uk**
Telephone	**0121 704 6407**