

GROUNDWORK

CHANGING PLACES
CHANGING LIVES



R2W Process of Sending Secure Information via E-mail Policy GWSNT – COL10

This policy applies to all Groundwork South and North Tyneside Route2Work College Staff (hereafter referred to as Groundwork)

Department for Education - What constitutes a security breach?

- Sharing your account details, or allowing someone else to use your account. Each user should have their own user account, and accounts that are no longer required should be removed immediately. 'Generic' accounts are prohibited.
- Sending a learner's ULN number and any of the 5 demographics (Given Name, Family Name, Date of Birth, Gender or Postcode) in an unencrypted email
- Sending more than one of the 5 demographics in an unencrypted email (Given Name and Family Name are deemed as one demographic in this instance)
- Sending an encrypted file containing learner data, where the password has also been sent via email

Never send more than 1 identifiable piece of information about a person, in a non-secure email.

Therefore, when sending an email containing personal information, please ensure you apply the following in order of priority: -

1. Use a 'Portal' where possible and available
2. Sent the ULN/Participant Number/Initials only and no attachments
3. If a file needs to be attached and sent, and/or personal information use 'Egress' or another secure portal
4. If for some reason you can't access or use Egress, use the 'Encrypt' function on Outlook as well as also securing the file with a password. Create new e:mail and search 'Options' in the header for the 'Encrypt' function. Ensure that your files are encrypted to AES 256-bit encryption standards using acceptable encryption software such as WinZip. Create and use a passphrase with a recommended minimum of 15 alpha-numerical characters including symbols, for example L3arN!ngr3C0rds. After emailing encrypted files for example to the DfE, you must contact the LRS Service Desk and communicate the password using a different communications method, such as telephone or text.
5. If the Encrypt function doesn't work – password protect information in a document (Word/Excel etc.) i.e., File – Protect Document – Encrypt with Password... and then email securely. You must then ensure the password is sent to the receipt via a text message, **not emailed**.

Policy review

Created By:	Rachel Kitson
Valid Date:	September 2025
Review Date:	September 2025
Review Date:	September 2027
:	04

Version Control

Version Number	Date	Name	Job Title	Document Status
01	September 2022	Rachel Kitson	Head of Provisions and Achievements	Approved

02	September 2023	Rachel Kitson	Head of Provisions and Achievements	Approved
03	September 2024	Rachel Kitson	Head of Provisions and Achievements	Approved
04	September 2025	Rachel Kitson	Director	Approved