



The Societas Trust

ICT (Data Protection) Guide

Date of Policy	2026
Reviewed and Agreed by	The Directors' Board
Adopted	Autumn 2024
Review Date	Autumn 2026
Review Date	
Next Review Date	Autumn 2028

Contents

SIMPLE TUTORIALS	2
HOW TO PRINT SCREEN CAPTURE	2
PRTSCR BUTTON	2
SNIPPING TOOL	2
PASSWORD PROTECT A DOCUMENT IN MICROSOFT OFFICE	2
ENCRYPT OR RESTRICT AN EMAIL IN MICROSOFT OUTLOOK OR OFFICE 365	3
ACADEMY ICT SPECIFICS	4
STAFF DOCUMENT SHARE	4
PRINTING POLICY	4
ICT PLATFORMS	5
VISITOR PROTOCOL	5
DATA PROTECTION FOCUS	6
KEYBOARD SHORTCUTS	7
WINDOWS OS	7
OFFICE	7
INTERNET BROWSER (IE)	7
EMAIL ENCRYPTION	7

SIMPLE TUTORIALS

HOW TO PRINT SCREEN CAPTURE

Two useful ways of capturing a screenshot of anything displayed.

PRTSCR BUTTON

NOTE: The PrtScr function may need to be actioned by pressing Shift along with the PrtScr button depending on the keyboard layout.

- Press the PrtScr button on the keyboard to capture exactly what is onscreen at that moment. This will be saved to the computer memory or Clipboard.
- Open a paint programme such as MS Paint or create a new Word document for example.
- Right click and select Paste to paste the contents of the Clipboard into the new file or document. Alternatively, press CTRL + V together to paste.
- Save the document.

SNIPPING TOOL

- Press the Start  button.
- Type snip and then click on Snipping Tool utility.
- Click New.
- Drag the cursor to highlight the area required to snapshot.
- In the Snipping Tool window, click File and Save As.
- Choose a location to save and give the image file a name.

PASSWORD PROTECT A DOCUMENT IN MICROSOFT OFFICE

This feature is relatively the same in Microsoft Office from versions 2013 to 2019 and covers each Office application including Word, Excel, Powerpoint and Publisher.

- When ready to secure the document, go to File.
- Under the Info tab, click on the Protect Document button.
- Enter a password, click OK and then confirm it in the second box.
- The document is now password protected and will require it on opening.
- Click File and Save to save changes.
- DO NOT forget the password or else the file will no longer be accessible.

ENCRYPT OR RESTRICT AN EMAIL IN MICROSOFT OUTLOOK OR OFFICE 365

This may differ between academies and how staff access their emails however the general process is much the same. Across the Trust, it is advised to keep the process as generic as possible.

- Open Outlook or log into Office 365.
- Click **New Email** in Outlook or **New** in Office 365.
- Once the new email window has opened, enter the recipients email address as per normal in the **To** box.
- In the **Subject** box, at the beginning of the text enter the word **Encrypted or Restricted** followed by any other text to be included in the subject bar to describe the email. The word **Encrypted or Restricted** in the subject text box are the keywords used by the Trusts Office 365 mail client to initiate the process of encryption or restriction. Whenever these keywords are used in the subject box, encryption or restriction will commence when the email is sent.

The Encrypted keyword provides the following permissions;

- The recipient will be able to forward the email
- The recipient will be able to copy the content of the email
- The recipient will be able to print the email
- The recipient will have full edit permissions to any document attached

The Restricted keyword provides the following permissions;

- The recipient will not be able to forward the email
 - The recipient will not be able to copy the content of the email
 - The recipient will not be able to print the email
 - The recipient will not have full edit permissions to any document attached
- Enter any content in the **Message** box to be included in the email as normal. Click **Send**.

On receipt of the email, the recipient will have two scenarios. Depending on how their system is configured and whether they use Office 365 mail client, the recipient will either see the email as normal in the email window if the Microsoft Azure Information Protection add-in has been installed and enabled on the machine. Or an email will be received containing a link to Office 365 online to log in to view the email decrypted content.

ACADEMY ICT SPECIFICS

(ICT PROCEDURE DETAILS PER SITE)

Although each academy will use uniform methods under the ICT policy, it is determined that each academy will use variations in software and procedure also. Any site specific ICT tutorials or documentation for staff use are to be located in a central shared folder on the network for all staff to view. Path to doc store in the following section.

STAFF DOCUMENT SHARE

The path to the central storage folder for all sitespecific tutorials and documentation.

- Computer
- T:\Staff ICT Documentation

PRINTING POLICY

Xxxxxx Primary Academy

Each member of staff is given a unique code to use for operating the shared network photocopiers. Whether printing, copying or scanning, each user is required to enter a passcode to use the features and this will be assigned to the user by the IT department upon request. When printing to a copier, all jobs are stored in a Secure Print user box. To release any stored print jobs:

- At the copier, choose username from the menu.
- Enter passcode and OK.
- From the main screen, select User Box.
- All print jobs sent to the copier will be displayed.
- Select those required and click Print to release the documents.

All jobs are stored for 24 hours after which are deleted from the queue.

ICT PLATFORMS

Details of 3rd party ICT platforms used and designated authority within the school.

Examples – please complete

Arbor	XXXX
DC Pro	XXXX
Computer Network access	XXXX
Teachers to Parents	XXXX
Email/network/VPN accounts	XXXX
TT Rockstars	XXXX

VISITOR PROTOCOL

- If a visitor requires Internet access, the user can connect using the guest wi-fi network.
 - SSID: xxxxGuest
 - Key: example
- Prior to connection, devices must have working antivirus with current definitions.
- If a visitor does not have a device but requires access to the Internet, an isolated guest user account can be used with no access to shared network drives.
- If possible, the visitor is to send any files required for presentation or use in advance so that the necessary ICT facilities can be configured.
- Whilst USB devices are not recommended, if required then all USB devices are to be scanned for virus and malware prior to use on an isolated PC.

DATA PROTECTION FOCUS

(BITESIZE DETAILS OF DATA PROTECTION POLICY STAFF SHOULD BE AWARE OF AND ADHERE TO)

- User accounts must have passwords that are not less than 6 ASCII characters in length and will use upper and lower case letters as well as numbers.
- Passwords to be changed on a frequent basis (at least every 3 months) as per the Information Security Policy.
- Authorised users are responsible for keeping their password(s) secure and must ensure their password(s) is neither disclosed to, nor used by anyone else under any circumstances.
- Personal Data, Special Category Personal, confidential and sensitive information sent or transmitted externally using an electronic system or service must be secured using a process that ensures the Data is encrypted and Users must carefully check the recipient's contact details before sending.
- Laptops, cameras, iPads and tablets should be locked away when not in use.
- Any academy mobile device or camera used to record photos/footage offsite is to be signed out and again on return. Any such footage is to be downloaded securely and then erased from the device within 48 hours of use.
- Documents containing Data must not be left unsecured, unattended at mail points or on printers, photocopiers, scanners and must be removed immediately when received.
- USB should not be used on site without being encrypted..
- Any such USB device is to be encrypted prior to use by the academy specific IT Representative. (These devices should be phased out as per the Data Protection Policy)
- Staff are not permitted to use their personal devices where the academy provides alternatives, such as work laptops, tablets and USB sticks, unless instructed otherwise by the headteacher.
- If staff are instructed that they are able to use their personal devices, they will ensure that they have an appropriate level of security and firewall to prevent any compromise of the academy's network security. This will be checked by the IT Representative.
- Staff members will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any laptops, tablets or other devices.
- The use of personal cloud storage solutions (Skydrive, Onedrive Personal, iCloud, GoogleDrive etc.) for the transfer of Academy information is expressly forbidden. Any cloud solutions should use HTTPS for transmitting data with a check for the padlock icon.
- When Police request any evidence from CCTV footage, all footage MUST be provided on a secure encrypted USB drive only.

KEYBOARD SHORTCUTS

WINDOWS OS

Account options	CTRL, ALT + Delete
Lock the workstation	⌘ + L
Open Start Menu	⌘
Show the desktop	⌘ + D
Display open applications	⌘ + TAB
Cycle through open applications	ALT + TAB
Close window/application	ALT + F4
Open Explorer	⌘ + E

OFFICE

Open document	CTRL + O
Create new document	CTRL + N
Save document	CTRL + S
Print document	CTRL + P
Undo previous actions	CTRL + Z
Redo previous actions	CTRL + Y
Cut selection	CTRL + X
Copy selection	CTRL + C
Paste selection	CTRL + V
Bold	CTRL + B
Italic	CTRL + I
Underline	CTRL + U
Select all content in document	CTRL + A
Find on page	CTRL + F

INTERNET BROWSER (IE)

New window	CTRL + N
New tab	CTRL + T
Close tab	CTRL + W
Print	CTRL + P
Refresh page	F5 (may require to hold Fn key)
Full screen	F11 (may require to hold Fn key)
Find on page	CTRL + F

EMAIL ENCRYPTION

Email keyword for Encryption	Encrypted
<i>To be typed in Subject box of email</i>	