# Transform Trust

# IT User Protocol

| Policy/Document Number | Author | Publication Date | Review Cycle |
|---|---|---|---|
| 008 | Chief Finance Officer | V3 September 2024 | Every 2 years |

## Scope

The intention of this protocol is to enable users to understand their responsibilities in representing their organisation in utilising digital devices, platforms and communication mediums and to indicate the overall approach being taken by the organisation.

The number of communication methods and choices available to both organisation and user have grown enormously over recent years and the aim of this protocol is to maximise usability and access for legitimate use, whilst recognising the challenges in securing these communication methods both for the organisation, its community and for any individual potentially impacted. This protocol focuses on a common-sense approach to managing communications with a balanced emphasis on securing relevant communications at source whilst also expecting the educated user to apply the protocol in both spirit and practice. This balance is struck with view to make the advances in communication technology usable and valuable to the user. This protocol also recognises GDPR regulations.

# Microsoft 365 Account

## Introduction

Transform is moving all schools into a single Trust 365 tenant. All use of MS Office products (e.g, TEAMS, Outlook, Word, Excel, Powerpoint, PowerBI) is within this Trust 365 environment and subject to the same security protocols to prevent the action of cyber criminals. The purpose of the protocol is to enable a Transform Trust/School user to navigate the use of the tools safely and securely.

## Procedures

- All staff/Governors/Trustees will have a strong MS365 password set which is not to be shared with anyone. Users can request a password reset by contact with the IT provider. We recommend using 3 random words together to comprise a strong password.
- All staff/Governors/Trustees will enable 2-factor authentication. This is possible through an app on a personal mobile (e.g, MS Authenticator) or through a 2-FA code sent to the mobile phone via text. 2-FA will not be sought when it has been successfully accessed before at a set IP address.
- All MS365 accounts will be secured by Geo Locking – users will therefore need to request access of their 365 account when abroad, and for a specified date period.
- All members of the tenant will have access to the Transform MS365 cloud, and should consider use of SharePoint for sharing files rather than sending by email. Email requires communication outside the tenant and should be considered more risky than using SharePoint.
- All Trust tenant MS365 emails are in the form "…@transformtrust.co.uk". School email domain names are retained as an alias, but all are within the Transform tenant.

# Email

## Introduction

Email is a global means of communication. It is often the primary communication and awareness raising tool within an organisation. Whilst email provides many benefits, email also poses security, privacy and legal risks. It is important that users understand how to use it appropriately in the Transform/School context.

The purpose of this protocol is to ensure the proper use of emails containing Transform/School relevancy and of the Transform/School email system, to make users aware of what Transform/School consider to be acceptable and unacceptable use. This statement outlines the minimum requirements for use of all email containing Transform/School relevancy whether or not on the Transform/School system.

It is also the stated specific aim of this protocol to traffic all Transform/School relevant emails on to the Transform/School email system. Private E-mail addresses should NOT be used to traffic Transform emails (unless a private email address is the primary means of communication with a consultant – additional security protocols are necessary). This is a fundamental security requirement of the protocol.

We have introduced specific security measures to protect and cover all email within the Transform domain.

## Procedures

- All use of email must be consistent with Transform/School policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- Transform/School email accounts should be used for ALL Transform/School business-related purposes; personal communication from Transform/School email accounts is also permitted on an occasional basis, but commercial uses (ie, for profit) are strictly prohibited.
- All Transform/School data contained within an email message or an attachment must be secured in accordance with General Data Protection Regulation.
- Email should be retained if it qualifies as a Transform/School business record, i.e. if there is a legitimate and ongoing business reason for maintaining the information contained in the email.
- Email identified as a Transform/School business record will be retained in accordance with Transform/School's Record Retention Schedule.
- The Transform/School email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about age, gender, race, disability, sexual orientation, religious beliefs and/or practice, political beliefs or nationality. Employees or representatives who receive any emails containing this type of content from any Transform/School employee/agent/representative should report the matter to their manager immediately.
- Users are prohibited from setting an automatic-forward for Transform/School email to a third-party email system. Individual messages which are manually forwarded by the user to such users must not contain Trust/School confidential or business information.
- Users are prohibited from using third-party email systems such as Google, Yahoo, MSN and Hotmail, etc. to conduct Transform/School business, to create or record any binding transactions or to store or retain email on behalf of Transform/School. Such communications and transactions should be conducted through proper channels using Transform/School approved systems/documentation.
- Occasional use of Transform/School resources for personal emails is acceptable, but non-work-related email shall be saved in a separate folder from work related email. Sending spam, chain

letters or joke related emails from a Transform/School email account is not appropriate and therefore prohibited.

- Transform/School employees shall expect only limited privacy in respect of anything they store, send or receive on Transform/School's email system. Emails held on Transform/School systems will belong to Transform and may be inspected from time to time or deleted to free up data storage once they reach an age.
- Whilst Transform/School reserves the right to monitor messages without prior notice, it is not obliged to.

### Monitoring

On a routine basis the Executive Team will request an internal/external audit of Transform/School emails to ensure compliance with this protocol. This will include review and/or monitoring of correspondence using software monitoring tools.

### Exceptions

Any exception to the above must be recorded and approved by the Executive Team/Headteacher or the Trust's Data Protection Officer in advance.

An employee/agent/representative found to have violated these procedures may be subject to disciplinary action or censure, up to and including termination of employment/contract.

## Internet

### Introduction

Much of a user's research and work involves access and use of the internet, and tools on the internet. Search engines and increasing use of AI tools means users can access both intentionally and unintentionally areas of the internet which are not appropriate for a school setting. Users should be aware of a number of steps the Trust has taken to protect children, staff, users and itself from harm.

### Monitoring

Transform has implemented tools for monitoring use of internet by users on all Trust/School devices. This is not designed to be invasive, but to detect key words and phrases that would/could cause concern. This is a broad umbrella designed to protect children and staff from harm, and inappropriate use will be flagged with Trust/School authorities.

### Filtering

Transform has a filtering standard across all Trust schools and Trust Centre designed to be age-appropriate for the setting. Inappropriate sites will not be accessible.

## Mobile Computing Protocol

### Introduction

Transform/School recognises that advances in technology around computers, tablets (including iPads), mobile phones, etc. mean that mobile digital devices have become everyday business tools. Because the devices are highly portable and can be used anywhere, they are vulnerable to loss or theft, and an unsecured device means they may be hacked or used to distribute malicious software. As mobile computing (in its broadest sense) becomes more common, Transform/School needs to address the significant security issues it raises in order to protect its information resources.

The purpose of this procedure is to establish a method for controlling mobile computing and storage devices which contain or access Transform/School's information resources.

This procedure covers all those who use mobile computing and storage devices on Transform/School networks or used to process Transform/School data. This includes Trust/School employees, supply and peripatetic staff, pupils, governors, trustees, consultants, contractors, visitors, etc. It also covers personal fixed and mobile devices used to carry out Transform/School functions, most commonly the mobile phone which can access email, make/receive calls, hold diaries, record notes and take/store photographs plus run a host of applications relevant to Transform/School use. The aim of the protocol is to continue to enable such use but to do so safely, securely and appropriately.

### Procedure

It is Transform/School's policy that ALL mobile computing and storage devices accessing school information resources must be approved before connecting to the school's internal information systems. This applies to all devices connecting to the Transform/School internal network regardless of device ownership. Guest networks can be accessed with Trust/school permission.

Mobile computing and storage devices include, but are not limited to: laptop/tablet computers, mobile phones, plug-ins, universal serial bus (USB) port devices, compact discs (CDs), digital versatile discs (DVDs), memory sticks/flash drives, modems, handheld wireless devices, wireless networking cards and any other existing or future mobile computing or storage device, either personally or Trust owned, that may connect to or access the information systems at the school. An assessment for each new device/media type will be conducted and registered prior to its use or connection to the network at Transform/School unless the device/media type has already been approved. Transform/School will maintain a list of approved mobile computing and storage devices.

Mobile computing and storage devices are more easily lost or stolen, presenting a high risk for unauthorised access and introduction of malicious software to the Transform/School network. These risks must be mitigated to acceptable levels before connection to the school network will be allowed.

The approach Transform/School is taking to secure its data is to protect ***the device*** accessing the personal or special category data, to secure the access point to that data, and to secure the data itself. This involves a number of different specific protocols now listed for users to consider:

- all devices (whether personal or Transform/School provided) holding commercial, proprietary, personal or special category data must be secured by a password. For mobile telephones a finger-

print or facial recognition would present an acceptable password. Any inputted password will be subject to regular update as required by Transform/School and SHOULD NOT BE DIVULGED TO ANYONE. Quite simply, users must accept full responsibility for communications coming from their own Transform/School account.

- Any forgotten passwords will be reset by your IT provider and users will be expected to set a new password accordingly.
- Mobile Devices are easily viewable by others. Users must think carefully about the setting they use and access Transform/School information. If in a public space, screens can be viewed by others and screenshots taken from mobile phones. This is pertinent on public transport, public places (e.g, coffee shops) but applies to any location where a screen is viewable by others.
- If using a personal device, **it is a condition of use** that a password is set on that device.
- Memory sticks should **NOT BE USED** – this is media which is easily lost or stolen. If a memory stick has to be used, **IT MUST BE ENCRYPTED** with a password or PIN code. Any files stored on the memory stick should also be encrypted. **AVOID USING MEMORY STICKS.**
- Any personal or special category data to be sent in an email must be password protected. This provides an additional layer of security and is particularly pertinent when data is to be necessarily sent to a non-Transform/School email address. Users should also bear in mind that data may be forwarded on by others who may assume the file is password protected – do not take the risk and always password protect the file. See your Admin team to help you learn how to set passwords.

## Loss, Theft or Damage

To report lost, stolen or damaged mobile computing and storage devices (regardless of ownership), staff should call Transform/School immediately. This may constitute a data breach and if so, will require immediate reporting by the Trust to the Information Commissioner's Office (ICO) which must be done with 72 hours of the breach being reported.

## Roles & Responsibilities

Users of mobile computing and storage devices must secure such devices from physical loss/theft of the equipment. Before connecting a mobile computing or storage device to Transform/School, users must ensure it has been approved by Transform/School and is on the device register.

The Headteacher/Executive Team/IT Support Team (or equivalent) must be notified immediately upon detection of a security incident, especially where a mobile device may have been lost, stolen or damaged.

Trustees/Local Governing Bodies are responsible for this policy at Transform/School but on a day-to-day basis the school's Headteacher is responsible for the operation of this protocol and they shall authorise appropriate risk analysis work to document safeguards for each media type to be used on the network or on equipment owned by Transform/School.

The Executive Team/Headteacher is also responsible for developing these procedures for implementation. The Trust/School will maintain a list of approved mobile computing and storage devices.

### Monitoring

On an ad hoc basis the Executive Team/Headteacher may authorise or request an internal/external audit of the above to ensure compliance.

### Exceptions

Any exception to the above must be recorded and approved by the Executive Team/Headteacher or the Trust's Data Protection Officer in advance.

An employee/agent/representative found to have violated these procedures may be subject to disciplinary action/censure, up to and including termination of employment/contract.

## Printing

### Introduction

Transform/School recognises the need to print documents. The purpose of the procedure is to ensure printing of personal and/or special category data is appropriately secured and the requirements of GDPR are fully observed. Printing presents a particular high risk of data breach given unsecure physical access to printers, copying facilities are readily available across Trust/School, and/or it is possible to print and for others to remove those prints from the printer.

### Procedure

All printing of personal and special category data should be secured, and then handled and stored confidentially. This is possible in a number of ways:

- Secure print – this means setting a password when the user commands a print. The user enters the password at the printer to print the job. Where this method is employed, the user must wait at the printer while the job completes.
- Use of Papercut – software to secure print
- Dedicated secured printer for confidential printing (e.g, in Head's office).
- The process for secure printing will be shared with staff once fully set-up.

### Monitoring

All printing not collected must be reviewed by a suitably responsible person in Transform/School to ensure the protocol is being observed. The Head should be made aware of any breaches of the procedure.

## Related policies and processes

- Data Protection Policy
- Freedom of Information Policy
- Online/E-Safety Policy including Acceptable Use Agreements
- Other legislation or regulations (including audit, equal opportunities and ethics) affecting the school or Trust

## Monitoring and Review of this Policy

This policy may be amended at any time to take account of changes in legislation. The normal cycle of review for this policy will be 2 years.