Journey Independent School
IT User Security Policy
September 2025

Implementation Date: September 2025
Review Date: September 2026
Date Policy Agreed: September 2025

CONTENTS

1. Document Purpose

The purpose of this document is to define the policies relating to managing staff and student user accounts and access to Journey Independent School's systems and data by those user accounts.

2. Scope

This policy covers all Journey Independent School Offices including staff, students and third parties (where appropriate). This also includes temp staff and contractors.

3. Policy

3.1 Desktop / Laptop / Tablet Security

All staff and student users of workstations, PCs, Virtual Desktops, laptops, tablets and iPads (collectively referred to from here as devices) must lock access to their device or log off when it is not being used, this is particularly important for teachers in classrooms.

All users must save their work regularly in accordance with best practice, to prevent corruption or loss through system or power malfunction or loss. Saving of data to the local hard disk of a device is not recommended with the exception of mobile devices. Mobile device users must manually backup local files (USB memory sticks must not be used). Local devices are not backed up as part of the daily central backup routines. If offline files are used, the user must synchronise these files on a regular basis and check that the sync completes.

Journey Independent School employees are not permitted to load non-approved screen savers or software that is not required or approved on to the organisation's devices. All machines will be "locked down" to prevent users from installing software.

Journey Independent School employees are not permitted to use unapproved web based applications on to the organisation's devices. All web based applications need to be approved by the IT team, DPO and also if appropriate the Director of Primary or Secondary if it is an education focussed app. A Data Protection Impact Assessment form (DPIA) must be submitted and approved before the app is used.

All builds, of all devices, from the date of this policy, configuration should conform to an approved standard and controls should be in place to limit the changes to the configuration that can be made by the user.

Staff and Students program folders and shortcuts will be maintained centrally and Student Desktops will be managed centrally.

The following items must be part of the standard build:

- vendor-supplied defaults e.g. account passwords, network protocols etc. must be changed prior to installing the new system on any network;
- any unnecessary operating system components, services and protocols not required by the business must be removed;
- any unnecessary applications not required by the Centre must be removed;
- laptops must have firewall enabled;
- mobile devices to be taken outside of the Centre must be encrypted;

- SCCM management software must be installed including Anti-virus;
- all devices must have anti-virus (including anti-spyware and anti-adware) installed and a formal process for automatically updating virus signatures must be applied;
- all devices should be patched and be up to date;
- a screen saver must be configured, password protected and activated after no more than 10 minutes of user inactivity;
- all mobile devices need to be brought back into the Centre at least monthly and connected to the network for at least a day to get updates for the operating system and anti-virus.

Requests regarding changes to the device security configuration can only be approved by the IT Director, Head of Service Delivery or the Head of Infrastructure Services where a genuine business reason exists. Any such changes and business reason for the change must be fully documented and submitted through normal change management process.

There must be an automated process for notification and implementation of new end user device operating system and application patches.

Unless a genuine business reason exists, data must not be stored locally on any device.

Staff mobile devices that are likely to be removed from site and that contain confidential data (not student devices) must have full disk encryption installed.

The use of non-Journey owned equipment to connect via non approved wireless or wired connection is not permitted without specific written approval from the Centre support team. Personal equipment is defined as any non-Journey issued equipment, such as tablets, laptops, PCs, smart phones etc. permission will only be given where there is a legitimate business requirement.

Staff and students can connect personal devices to the wireless connection “My Device” which will allow limited access to Journey external facing systems and the Internet, including Virtual Desktops. It is the responsibility of the user to ensure that the device is patched and has up to date Anti-virus installed. There is no entitlement to support from the Journey team for personal devices whether on site at a Centre or at home.

Parents or other guests should not be given access to devices unless these are in the “Guest” network.

All contractors or third parties working on Journey Independent School’s systems or data must use Centre equipment, ideally virtual desktops. If a contractor or third party has to work on their own machine it must be checked for up to date AV and patching before connecting to the network.

No confidential data should be transported on any unencrypted device including USB memory sticks.

No user should have either unfiltered access to the Internet or proxyless access. All access to the Internet must be authenticated to allow full tracking.

Non-windows mobile devices such as iPads and smart phones must be locked down and managed by a Mobile Device Management system, such as Meraki.

Applications should not be able to be downloaded and installed by the end users.

USB memory sticks must not be used to transfer files between Centre devices and home/personal devices.

Personal Web Based email accounts should not be used whilst on a Centre network. These sites, such as Hotmail, Yahoo, Gmail etc. will be blocked by default the filtering software unless the CEO requests an exception.

3.2 Anti-Virus

The threat posed by the infiltration of a virus is high, as is the risk to the Journey Independent School's systems and data. Formal procedures for responding to a virus incident are in place to enable the Centre IT team to reduce the impact of any infection and to remove the infection as quickly as possible. Virus incident response must be regularly reviewed and tested in the local Centre.

A managed proven enterprise scale anti-virus solution with scalable deployment functionality meeting the needs of the Centre must be installed on all devices within scope. All programs must be capable of detecting, removing and protecting against all known types of malicious software and all antivirus mechanisms must be current, actively running and capable of generating audit logs and email notifications (immediate and summary). The policy also covers the application of anti-spyware and anti-malware (including anti-adware).

Any computing devices not owned or managed by Journey which are brought into Centre premises must be scanned for viruses before being allowed to connect to the network unless they are clearly configured with up to date recognised AV software.

Virus-signature (including anti-spyware and anti-malware) updates must be obtained from a trusted source and applied as soon as they are available when a new vulnerability and signature is announced by the vendor, tested where appropriate to ensure that a new signature does not negatively impact the Journey system infrastructure and then updated on the anti-virus servers.

Virus signature updates (including anti-spyware and anti-malware) must be automatically pushed out to computing devices from a managed point in the
Journey Independent School infrastructure as soon as they are available.

A virus incident response procedure must be in place to facilitate the removal of any infection with minimal disruption. Such procedures must be regularly reviewed and tested within the local Centre IT team.

Journey Independent School users must take great care when downloading information and files from the Internet to safeguard against both malicious code and also inappropriate material.

Regular AV scans should be run on all servers and user devices, with the exception of Virtual Desktops.

Journey email and Internet access should be scanned for virus at the entry point to the Network. All web access should also be filtered for inappropriate content.

3.3 Authentication

Access to computing resources must be limited to only those who need it.

Users must only use their own login account. Access to resources including the Internet is tracked and monitored to the logged in user.

Generic or shared login accounts should not be used with the exception of the following:

- Shared class logins for Primary students (ideally infants only)
- Guest accounts
- Controlled assessment accounts
- Delegated admin accounts
- Supply teacher accounts
- Third party support companies

For the last five generic account types a register should be kept of who is assigned the account, for how long and whether it is disabled. Generic accounts should be disabled when no longer required, for instance support companies only have their account enabled when required to carry out specific work.

User authentication for all users must be managed on all system components, and must include the following:

- The addition, modification and deletion of user IDs, credentials and other identifier objects must be controlled (delegated admin accounts only);
- Unique user IDs must be assigned before the user is granted access to the system, with the exception of the Generic accounts detailed above;
- User accounts which have been inactive for at least 90 days will be removed or disabled;
- User accounts that have been disabled for three months will be archived and deleted as appropriate, with the exception of any that have specific retention instructions;
- Accounts used by vendors for remote support and maintenance may only be enabled during the time period required: they must be disabled at all other times;
- Restriction of access rights for Delegated Admin accounts to least privileges necessary to perform job responsibilities;
- Assignment of privileges is based on an individual user's job classification and function;
- Requirement for an authorisation form signed by management that specifies changes to the expected privileges through the normal change management process.

Users should only have one active user account. For users that leave one role and move to another role, their account should be moved and a new user account should not be created. If there is a crossover period where the user needs access to data from both roles then a security update will be applied to the role and then removed once the move is complete.

Access to resources should always be granted via membership of a group and not assigned directly to the individual.

For roles that cover multiple Centres the preferred route would be to make the user a Centre user rather than create multiple accounts for each school.

3.4 Web and network based application authentication

Any Centre web and network based applications must implement a secure mechanism to authenticate all users that access the applications, for instance Bromcom and Concur. Role-based access control will be implemented in the application and authentication will be implemented using a password mechanism with appropriate complexity rules (see below)

All external facing web applications should use https secure protocol.

3.5 Voice Authentication

Journey Independent School telephone enquiries regarding confidential information must only be disclosed once the identity of the caller has been verified.

Centre staff must be aware of "social engineering" attacks, where the aim is to trick people into revealing passwords or other information that compromises the Centre's system security, and be able to prevent and report such attack attempts to the Group IT Director.

3.6 Email Authentication

Incoming email to the Journey Independent School information systems must be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible viruses or other malicious code. Do not open attachments from unknown external senders.

Personal web based email accounts should not be used on Centre sites as attachments cannot be scanned by our perimeter virus protection mechanisms.

3.7 Passwords

All passwords must conform to the following minimum standards where the operating system or platform supports them. Where systems do not support this standard this must be documented and a risk assessment undertaken to identify additional compensatory controls and mitigating actions for those systems.

Journey Independent School system owners must, at the earliest opportunity, change default passwords installed by vendors at initial delivery of equipment and software. Generic vendor default accounts such as Guest must be removed, renamed or disabled at the earliest opportunity.

The unauthorised possession and / or use of password sniffing or other hacking tools are forbidden on the Journey Independent School infrastructure.

When a user leaves the employment of Journey Independent School or changes role, any Delegated Admin account passwords that they may have known must be changed immediately. On termination of employment access to all user and delegated admin account access is to be disabled.

Journey Independent School employees and third parties with access to the network environment must treat passwords and / or other access credentials as confidential and protect them appropriately. Usernames and passwords should never be disclosed to another person.

Under no circumstances should users use another person's network login account unless this is in relation to solving an IT problem; in which case the user must make sure that they only disclose their password to an authorised IT staff member and that the password is changed once the issue is resolved. The IT staff member should set to 'force password change' upon next login when the work is complete.

Prior to resetting a password, the systems administrator must perform an appropriate form of authentication to validate that the user is who they say they are.

Group / shared passwords are prohibited with the exception of the cases highlighted above.

A password transmission process for delivering new sign-on passwords to users must be applied which releases it only to the owner or their line manager. This password must only be allowed to be used once, and must be changed immediately.

Passwords must:

- be changed immediately after first use;
- be stored in irreversibly encrypted form;
- have a minimum age of 1 day;
- be changed immediately whenever accounts have been compromised;
- never be sent in the same email or other communication as the username to which they relate. Ideally, the username and password should be sent by two different methods e.g. email and SMS text message;
- be complex, min 8 characters long and a mixture of a minimum of one capital letter, one lower case letter and one number;
- be changed at least every 90 days i.e. no less frequently than quarterly;
- not allow the re-use of the previous 5 passwords;
- have an account lockout duration of a minimum of 30 minutes;
- have an account lockout threshold of 3 invalid logon attempts before being locked;

Passwords must not:

- be the same as or derivation of (e.g. Password123);
- Username
- First name
- Last name
- Password
- Journey
- be viewable when entered;
- be written down;
- be shared with anyone;
- be used by unauthorised users to access systems / information they are not authorised to access.

3.8 Remote Workers

There are four approved methods of accessing the Journey Independent School systems remotely:

Virtual Private Network (VPN) connection from a Centre managed laptop or device. This is not the preferred solution for remote access and should only be used if the other methods are not appropriate or available. This method will be phased out.

Another method which is really only to be used for third party support, is the use of remote control software. Most RC software is blocked by LGfL but the following are supported:

- Logmeinrescue (LGfL version);
- GoToMyPC;
- Webex;
- Skype.

Laptop and Tablet users must regularly (at least every **30 days**) bring the device into the office and log into the network, otherwise certain systems will not work and the user will eventually be locked out of the laptop.

Mobile users must ensure that the tablet / laptop gets updates/patches and Anti-virus installed and kept up to date.

Data on laptops and tablets must be backed up on a regular basis, daily or weekly if possible, depending on the risk of losing the data. The user of the mobile device needs to ensure the data is backed up, this is not a responsibility of the Centre IT team.

Data must not be transferred to or from a non-Centre device to a Citrix session.
The Citrix sessions will be locked down to prevent any unauthorised data upload or leakage.

If work is carried out on Centre data files on personal devices it is the responsibility of the user to ensure that the device is free from Viruses, has up to date anti-virus and anti-malware and is patched up to date.

Users should not use removable media (USB memory sticks etc.) to transfer files to and from personal devices. All files associated with work should be stored on an appropriate Centre Shared Drive or OneDrive.

Users must not use personal web based email or file stores such as DropBox to transfer files to and from personal devices.

Any confidential data being transferred on mobile devices must be encrypted.

The Remote Worker must keep all Journey Independent School owned equipment and data secure when it is not in use particularly when travelling.

All acceptable usage and security policies etc. apply when working from home as they do whilst working on Centre and / or third party premises

Family and friends are not permitted to use Centre equipment.

Proxy settings and filtering software should not be disabled on Centre Managed devices when using off-site. The new filtering system should allow the same settings to be used when on or off site.

4. Roles and Responsibilities

Role	Responsibility
Group IT Director	Ensure that the user based security recommendations are appropriate to business needs. Define the User Security Requirements, gain business signoff. Establish a sensible balance between secure access and letting employees easily perform their job duties.
Journey Users	Safeguard their access control credentials. Not attempt to circumvent access controls or elevate their privileges in order to access information they have no business reason to see. Comply with the policies.
Infrastructure Team	Manage user access controls and safeguard access control lists.
System administrators	To manage the users within the applications that they are responsible for.

5. Exceptions

There are no exceptions to this policy.

6. Enforcement

IT management will perform regular audits to ensure policy compliance. Non-compliance will be escalated to Centre management. Any employee (or student) found to have violated this policy may be subject to a disciplinary process.

Journey Independent School

Author | Angela Cousins | Journey Independent School Managing Director