

Jackson Public School District | Information Technology Services
Implementation of Changes to JPS Email and Network Account Management

Beginning January 5, 2022, procedures for obtaining and managing all JPS employee email and network accounts will change. This document provides information and guidance to help employees navigate these changes.

Key changes include:

- New procedures for the creation of new employee JPS Office 365 and jpsms.org accounts.
- New procedures for resetting email and network account passwords.
- New JPS Identity Automation portal requirement for logging in to email accounts and resetting passwords.
- New requirement for multi-factor authentication for all cloud accounts (Office 365 and jpsms.org).
- New, stronger password requirements.
- **New JPS Identity Automation Portal.** <https://jpsd.us001-rapididentity.com/>

Frequently Asked Questions

Why are we making these changes?

Technology changes with time. We are now able to take advantage of newer technology that allows us to be more efficient, more effective, and more secure.

What is the JPS Identity Automation Portal?

What is multi factor authentication (MFA)?

Multi-factor authentication (MFA) is an authentication method that requires the user to provide two or more independent verification factors to login to an online application or account. MFA is not unusual, as most online banking and credit card management accounts require MFA.

There are three types of multi factor authentication:

- Things you know, such as a password or pin.
- Things you have or possess, such as a cellphone or badge.
- Things you are, such as fingerprints or facial recognition

Why is MFA important?

MFA improves account security by requiring each user to identify themselves by more than just a username and password. Usernames and passwords are vulnerable to brute force attacks and can be easily stolen by third parties. Social engineering is often used by criminals to try and get users to willingly provide usernames and passwords through email phishing or even simple

Jackson Public School District | Information Technology Services
Implementation of Changes to JPS Email and Network Account Management

phone calls. Using only one-factor such as a username and password makes is very easy for criminals to gain access to a user's account.

What type of multi factor authentication will be required in JPS?

JPS is providing several MFA options for employees. All employees must choose username and password as the initial authentication factor but can choose their second factor from the list of JPS MFA options. Users can choose the method that works best for them. JPS MFA second factor options are:

- Username and password + **SMS text message**
- Username and password+ **QR code**
- Username and password + **time based one-time password application (TOTP)** – examples are apps such as Google Authenticator, Microsoft Authenticator, or Authy Authenticator. Links to these are on the JPS ITS department web site and in the new JPS portal. <https://jpsd.us001-rapididentity.com/>
- Username and password + **Challenge Questions**

Will users have to use a cell phone to login using MFA?

No. Users can elect to use a QR code or challenge questions for their second factor. Neither option requires a cell phone. Individual users will be responsible for printing and maintaining their own QR codes. QR codes requires a camera on the device in order to use this method.

What if I lose my QR code or cell phone? Can I still login to my email account?

Yes. If a user loses their QR code or cell phone, or changes their cell phone number, users can always login to the JPS Identify Automation Portal using Challenge Questions and change their phone number or print a new QR code.

When will all employees have to being using MFA?

All employees will be required to sign up/claim an JPS Identity Automation account and enable MFA by January 17, 2022. Any employee who has not claimed/signed up by Monday, January 17, 2022, will not be able to access their email accounts on Tuesday, January 18, 2022, until they claim their account and reset their password. **All login attempts to both Office 365 and jpsms.org accounts will be redirected to the JPS Identity Automation portal on January 18, 2022.** <https://jpsd.us001-rapididentity.com/>

What steps will be required of all employees?

1. All employees must go to <https://jpsd.us001-rapididentity.com/> and claim their account using their personal information.
2. All employees must reset their passwords to comply with new password requirements.
3. All employees must login to the JPS Portal and add MFA to their portal account.

Jackson Public School District | Information Technology Services
Implementation of Changes to JPS Email and Network Account Management

What happens if an employee doesn't complete the required steps?

The employee will lose access to their account on January 18, 2022, and it will remain inaccessible until the process is complete.

Will an employee have to use MFA every time they login to their email?

No. The browser will remember you are logged in and will not require to authenticate with MFA each time. Changing browsers or changing networks or locations will require re-authentication with MFA.

How can I get help claiming my new portal account and using MFA?

All directions and support documentation including video and static documents can be found on the JPS ITS website at <https://www.jackson.k12.ms.us/Page/15921>.

What happens if I can't remember the answers to my challenge questions?

Employees who forget the responses to their challenge questions must call the JPS ITS helpdesk at 601.973.8601 during regular business hours to have the challenge questions reset. Employees must be able to identify their identity when calling.