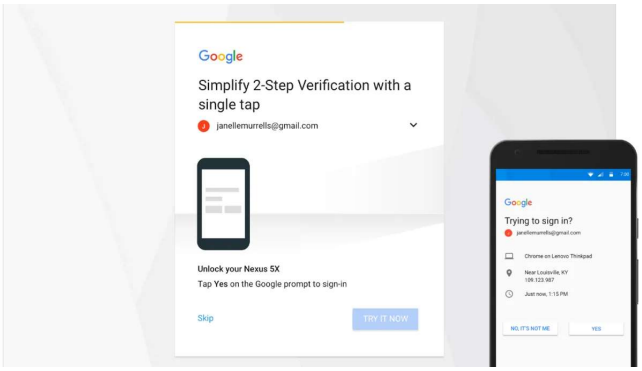

King's Group Academies: Multi-Factor Authentication (MFA) Policy

Introduction

As part of our ongoing efforts to enhance security and protect sensitive data across King's Group Academies (KGA), all staff members will be required to set up Multi-Factor Authentication (MFA) for accessing Google services (including Gmail and Google Classroom) and Arbor. This change is crucial to safeguard against increasing cyber threats, which are targeting educational institutions across the UK.

What is Multi-Factor Authentication (MFA)?

Multi-Factor Authentication (MFA) adds an additional layer of security to your account by requiring you to verify your identity in two or more ways before gaining access to online systems. This is a common practice with many online services, including banking, and ensures that even if a password is compromised, unauthorized access is prevented.

MFA typically involves:

- **Something you know**: Your password.
- **Something you have**: A physical item like a mobile phone, smart card, or USB dongle.

By using MFA, we add a second line of defence to protect our systems from cybercriminals who might try to access sensitive data, including staff and student information.

Cost and Implementation

- As a Google Trust, we have access to **MFA tools at no additional cost**, aside from setup and training time. Staff are familiar with Google and the Google Authenticator app is used for a range of websites, meaning this is one less system to become familiar with.

What will the staff need?

Recommended Setup Process:

- **Mobile Phone Authenticator App**: This is the most convenient option, as it does not require a phone signal and ensures that you don't have to carry an extra device.
- **Alternative Options**: If you prefer not to use a mobile phone the alternative method is a **USB Dongle** - A physical USB device stick used for verification. This will be available from your IT department.

FAQ

Using Phones in Class for MFA

Our school policy does not allow phones to be out in the classroom during lessons. Once you are logged into your Google account, you will stay logged in for 60 days, and you won't be prompted for MFA unless you log in on a new computer or log out of Chrome. Therefore, we encourage staff to log in before lessons to avoid any disruption. If you do need to use your phone to complete the MFA process during a lesson (e.g., for logging in), this is acceptable. The Headteachers are aware of this and have supported it. Your phone should only be used for this activity, and once you've completed the process, it should be put away again to maintain focus and follow the school's policy.

In terms of safeguarding, the purpose of MFA is to protect sensitive data. It is part of our broader safeguarding procedures to ensure that all personal and school data remains secure. This aligns with our other safeguarding advice regarding the protection of personal and sensitive information.

Response Regarding Concerns About Using Personal Phones for MFA

We understand that some staff may prefer not to use their phone for Multi-Factor Authentication (MFA). If you'd rather not use your phone, you can request a USB key (also known as a security key) to log in instead. The first USB key will be provided to you free of charge. However, based on experience across other schools within KGA that already have MFA in place, we've found that using a mobile phone for MFA tends to be the most convenient option. This is because the USB key can be easily misplaced or forgotten, and if you do not have it with you, you would need to visit the IT department to obtain a new one in order to log in.

Why aren't students required to use Multi-Factor Authentication (MFA)?

Students are not required to use MFA because their accounts are already highly restricted, with limited access to sensitive data. Many students, especially in Key Stages 2 and 3, do not own mobile phones, and requiring MFA would either create a barrier to learning or necessitate issuing USB keys to all pupils. Additionally, student devices and access are closely monitored, and email functionality is often restricted, reducing the risk of misuse. In Key Stage 4, where students are prohibited from using phones during the school day, enforcing MFA would contradict existing behaviour policies.