INSPIRING PRIMARIES ACADEMY TRUST

Policy of Compliance with Password Protection (S29)

The Board of Trustees adopted this policy on: January 2025
To be reviewed: January 2028 or earlier if required.

Introduction

1. Information and data are key assets of any organisation. These assets are a primary target for criminals and fraudsters. If hackers get into your device or your accounts, they could access your money, your personal information, or information about the Trust and the people we serve. The Data Protection Act 2018 (aka UK-GDPR) states that organisations need to take suitable technical and organisational measures to protect data.

Policy

2. Staff are required to follow this policy to help ensure that staff and Trust data is suitably protected whether they are working within an IPAT site or elsewhere.

3. Always be aware of your surroundings when accessing your device so that others are not able to view your actions, keystrokes, screen. This will lessen the chance that device and system security will be compromised.

4. Failure to comply with this policy may result in staff disciplinary action.

5. Staff should use strong passwords of at least 14 characters to access the Trust's information technology systems. These passwords should be made up of a mixture of lower and uppercase letters, numbers and special characters. The longer the better.

6. Or you may choose to use three random words to create passphrases that are used to access the Trust's information technology systems. For example, Bunny-Desk-Cheese. Pass phrases like this are easier to remember. However, staff may wish to use special characters to enhance the security of the pass phrase. For example, Bunny@D&sk-Ch33se.

7. Do not use information people may know about you, for example your favourite football team, children's names or dates of birth to create your passwords.

8. Passwords must **not** be shared between staff. This includes when staff are covering the role of another member of staff, for example when someone is on holiday. Sharing work accounts, or even occasional use by anyone other than the account holder, introduces a

number of risks. As well as the possibility of users gaining access to unauthorised resources, sharing accounts negates the benefit of authenticating a specific user. In particular, the ability to audit and monitor a specific user's actions is lost, an essential forensic requirement for some accounts.

9. If temporary access to a system is required then a request to that system's Administrator will need to be made outlining the nature and purpose of the access required together with the length of time access is required. If approved, temporary access will be provided.

10. Do **not** re-use passphrases between applications and systems. Your personal data is important to you as is the Trust's data; therefore, it is imperative that you do not use the same passphrases you use at home at work.

11. Do not write down passphrases.

12. Do not allow internet browsers to store / save your login details.

13. The use of password managers is encouraged. Use a unique password, one not used to access an IT system, to unlock the passphrase manager. (See Annex 1: Point 3 for recommended password managers)

14. Do not reveal your password to anyone. IT staff and IT service providers do not need to know your passphrase. There is no need to reveal your passwords to anyone else.

15. Staff must change their passwords when they know (or suspect) they have been compromised. They must also report any such instance to Chris Hall (c.hall@ipat.uk) without delay.

16. If 2FA technology is available for any service or system then this should be enabled. The use of an authenticator app (such as Google Authenticator or Authy) is preferable to a text based system where this is permissible by the IT system being accessed. As an alternative to using an authenticator app, staff may use a hardware token or security key.

17. It is essential to use this technology when allowing remote access to the Trust's IT systems, e.g., by staff working away from the school regularly. Remotely accessing IT systems is a common approach used by criminals to access valuable data. When using 2FA it becomes considerably harder for criminals to remotely access systems even if they have stolen usernames and passwords as it's unlikely they have access to the device that is used to create the unique codes.

18. Staff should be aware that some web services have an option that allows you to turn off 2FA for particular login credentials used on a certain device. For example, there could be an option when logging on to a service using 2FA that states "Always trust this device" or "Do not ask for 2FA codes on this device again". If you turn on these options, it effectively disables 2FA for that particular device and service. Therefore, **this practice is discouraged**.

Mobile devices

19. Mobile devices, such as smartphones or tablets, must be protected by a pass code, passphrases or biometric technology, e.g. fingerprint or facial recognition.

Additional technical advice

20. Required minimum password length: 14 characters.

21. Some systems and services require that passwords should be changed occasionally, for example every 30 to 50 days. However, there is a risk that staff write down passwords (in plain sight) or reuse passwords. A password manager should be used to create and store a unique passphrase or password.

22. Passwords used by system services, for example a password used by a web server to connect to a database, should:

    a. only be made available to staff that need them;

    b. use unique system accounts, not regular staff accounts;

    c. be changed occasionally, at least twice per year;

    d. have the minimum level of security privilege to perform the necessary task; and

    e. be obfuscated to hide their intended purpose or system usage.

Highly privileged accounts

23. Senior staff and those responsible for IT systems typically have additional system privileges. These “administrator” accounts allow systems to be configured and staff to be added or removed from systems.

24. These additional privileges should be allocated to an individual account, one which is owned by a single person. This will ensure that when that senior member of staff leaves an organisation and their account is disabled, the additional privileges are not available to another person.

25. However, it is recognised that some systems may allow only a single account to be used as an administrator. In these cases, it is common to find that a number of members of staff know the account and password details. This allows for circumstances when staff are not available and essential administration needs to be performed.

26. In these cases, the password for the administrator account should be changed as soon as the senior staff member indicates that they wish to leave the organisation.

System default accounts

27. The default passwords for new software or hardware devices (e.g., network devices, firewalls and printers) should be changed at the point of installation. If possible, the name of the account should also be changed. For example, “admin” to “Amanda Jackson”, using a random person’s name will obfuscate the account and make it less prominent to a criminal.

Annex 1

Guidance

You can improve your cyber security by taking the following 7 actions:

	Action	Guidance
1	Use strong and separate passwords for your email and all other online accounts	● Hackers can get access to your account by using software to crack your password, by using one password in lots of places or by trying to trick you into disclosing your password through scams (e.g. phishing) ● If a hacker gets into your email, they could reset the passwords for your other accounts by using the “forgotten password” feature ● Tricking someone into revealing their password via social engineering (including phishing and coercion) ● Using the passwords leaked from data breaches to attack other systems where users have used the same password ● Password spraying (using a small number of commonly-used passwords in an attempt to access a large number of accounts) ● Brute-force attacks (the automated guessing of large numbers of passwords until the correct one is found) ● Theft of a password hash file, where the hash can be broken to recover the original passwords ● ‘Shoulder surfing’ (observing someone typing in their password) ● Finding passwords which have been stored insecurely, such as sticky notes kept close to a device, or documents stored on devices ● Manual password guessing (perhaps using personal information ‘cribs’ such as name, date of birth, or pet names) ● Intercepting a password (or password hash) as it is transmitted over a network ● Installing a keylogger to intercept passwords when they are entered into a device
2	Create strong passwords using 3 random words	● A good way to create strong, memorable passwords is by using 3 random words ● Do not use words that can be guessed such as your pet’s name

		● You can include numbers and symbols if you wish e.g. “BabysittingBureaucratsGruel3£” ● You can check whether one of more of your passwords has already been compromised by a data breach by going to https://haveibeenpwned.com/
3	Save your passwords in a password manager	● The National Cyber Security Centre (NCSC) recommend the use of password managers for secure storage wherever appropriate. As well as providing secure storage, password managers can help users by generating and auto-filling passwords when required. This can help ensure that you do not lose or forget your passwords ○ There are several options available, including: ○ Bitwarden – it’s free and can sync passwords across all your devices ○ Keypass – free, but possibly for technically minded users ○ Dashlane – ideal for beginners, $40 per year ○ 1Password – for technically minded users, $24 per year
4	Turn on multi-factor authentication (2FA)	● One of the most effective ways of providing additional protection to a password protected account is to use MFA (2FA). Accounts that have been set up to use MFA require a second factor, which is something that you (and **only** you) can access. This could be a code that's sent to you by text message, or that's created by an app, so even if an attacker discovers a password, they won't be able to access the associated account without also compromising the other factor. 2FA helps to stop hackers getting into your accounts, even if they have your password. ● There are several apps available to manage 2FA which are more secure than text messages to your phone: ○ Authy ○ Google authenticator ○ Microsoft authenticator ● Alternatively, you may use a hardware token for 2FA. Hardware tokens are small physical devices that you plug into your computer or laptop that are used to authenticate your device. Once set up, a hardware token does not require any other devices, mobile data or internet connection for you to login to your account, although you will need to set up another authentication method before you can set up a hardware token, so you will need a phone at initial set-up. There are several keys

		available, including Google Titan hardware keys and Yubico keys.
5	Lock devices when they are not being used	● It is important to lock your device, log out or shut it down completely, when you are not using it. ● You can lock a windows machine by holding down the flag key and pressing the L key. ● There are different ways to lock a chromebook. These include: press and hold the **Lock** key on your keyboard; press and hold the **Power** button, then select **Lock**; press the **Magnifying Glass key + L** on your keyboard ● Leaving your device accessible for others to use or view may lead to a loss of data, a potential Data Breach. ● Be mindful of who can see the contents of your screen particularly if that device is linked to a larger screen such as a class interactive touchscreen.
6	Update your devices	● Out-of-date software, apps and operating systems contain weaknesses making them easier to hack. ● Some devices and software offer automatic updates; others need to be updated manually and you will get reminders on your phone or computer. Do not ignore these reminders.
7	Backup your data	● Backing up means creating a copy of your information and saving it to another device or to cloud storage (online). No member of staff should be saving information locally to their PC, laptop, chromebook, tablet or phone. ● Where necessary data should be stored on school servers which are regularly backed up across the MAT. Individual machines will not be backed up. ● The Trust makes use of cloud services such as Google, Arbor, Xero. All staff should be storing their documents on Google.