IT and Information Security Policy for Supply Staff

Purpose

Information Technology (IT) and data security is of the utmost importance to Vision for Education, Smart Teachers and ABC Teachers, and it is integral to the schools and settings that we work with.

IT and data underpin the key teaching, learning, pastoral and operational functions of a school or setting, and similarly they can pose great risk to those functions if appropriate considerations and actions are not undertaken where required.

The purpose of this policy is to set out requirements and expectations in relation to IT and data security for all supply staff who complete a role through Vision for Education, ABC Teachers or Smart Teachers. This policy aims to outline responsibilities and best practice to maintain data security, and to ensure compliance with organisational requirements, along with those of our client schools and settings. Where we refer to a 'setting' in this document, this could be a school, college, alternative provision, or any other organisation that we arrange for you to complete supply work with.

Scope

This policy applies to all supply staff, including those who have access to a placement setting's IT systems, data, or physical records as part of their supply placement. It covers the handling of electronic, paper-based and verbally received information. It is to be adhered to in conjunction with the setting's own IT and data security policy (or similar), which always takes precedence in relation to that particular setting.

General principles

- To protect data from unauthorised access, alteration or destruction
- To prevent disruption that could occur through any misuse, or attempted misuse of ICT systems
- To comply with all relevant laws and policies
- To only access data which is necessary for you to carry out the agreements of your role
- To only share data securely within the agreements of your role, or on a need-to-know basis, e.g. for safeguarding purposes
- To report any potential security breaches without delay to the appropriate person(s)

Breaches of this policy may be dealt with in line with our internal policy on managing incidents and our staff code of conduct. Non-compliance which constitutes gross misconduct may result in termination of your engagement with our agency, and, if applicable, legal consequences.

It is important to note that data protection laws do not take precedence over the safeguarding of children, young people and vulnerable adults. If there is a risk to a child of not sharing information, then the sharing is justified.

All use of IT and technology during your work placement should be in line with the school or setting's IT acceptable use policy. All personal life use of IT and the internet must be representative

of the position of trust that you hold, must be in line with our staff code of conduct guidance, and should reflect the values set out in the Teachers' Standards statutory guidance.

You can find our **Privacy and Data** policies, along with our **Safeguarding** Policies on the **Key Documents** page of our website.

Types of data

Personal data should always be stored securely, especially when it is sensitive personal data. Personal data is considered any information which relates to an identified (or identifiable) living individual. Examples of personal data in a school environment may include:

- Identity details such as name, address, date of birth etc
- Contact details
- Exam and assessment results
- Pupil behaviour information
- Pupil attendance information
- Safeguarding information
- Information relating to pupil premium, pupils with special educational needs and disability (SEND), children in need (CIN), and children looked after by the local authority (CLA)

Please be mindful that within a school environment, some sensitive personal data may need to be readily available in order to keep a child safe from risk or harm. An example of this may be a medical alert sheet or allergy information. Measures should be taken to keep this kind of data accessible, but confidential e.g. away from public view.

Personal data you encounter during your placement may be:

- physical (printouts, pupil records)
- electronic (desktop files, local hard drive)
- cloud-based (emails, online storage, intranet)
- physical backups (USB sticks) or
- on mobile devices (laptops, tablets or mobile phones)

Special category data, whether in electronic or manual format, must be handled securely, accessed only by authorised personnel, and securely disposed of after use.

If such data is to be taken into a high-risk environment—such as leaving school premises, being sent via email, or transported to another location—it MUST be protected, either through encryption or a lockable case.

You should also be mindful that data you create or handle could be requested as part of a Data Subject Access Request (DSAR), for example, by a parent. Any data that you write into a school email or enter onto a school data management system record could be requested and shared with a parent or student. You should make only professional observations using language that you would be happy for the data subject to view.

Below we provide expectations on the secure storage and handling of data by our agency staff, which should be implemented in line with the expectations of the school or setting you are working with.

Data Access and Data Protection

- **Use any assigned credentials and don't share them with others** or leave them written in a visible place
- **Ensure access to all data is strictly limited** e.g. ensure that your laptop or desktop is locked when leaving it, do not leave unencrypted data on memory sticks and ensure that your screen, when in use, is not visible by others e.g. through a window or doorway.
- **Avoid using personal devices for work** unless explicitly authorised
- Follow the setting's policies of keeping devices up to date with the latest security updates

Password Management

- **Use strong passwords** - we would recommend using at least 12 characters and a mixture of letters, including capital letters, numbers and symbols
- **Change your password if you think it may have been compromised** – report any potential breaches to the organisation it may affect
- **Avoid reusing passwords across systems and devices**
- **Try to ensure that others cannot view you inputting your passwords into a device**

Email and Communication

- **Use only official communication channels for work-related correspondence.** Be mindful that your communications may be filtered and monitored by the setting.
- If the school provides you with an email address, then you should only use this for work related purposes.
- Be cautious of phishing attempts; **do not click on suspicious links or download unknown attachments.**
- **Verify requests for sensitive information**, especially those received via email, through a secondary confirmation method.
- **If you receive an email in error, the sender should be informed and the email deleted.** If the email contains sensitive or confidential information, you must not make use of that information or disclose that information.
- **Only visit websites that are permitted by the setting** – schools and other settings will monitor and may log the websites you visit. Please ensure they are appropriate and relevant to your role.

Device Security

- **Lock your computer or device** when not in use.
- **Ensure antivirus software and system updates are up to date.**
- **Report lost or stolen devices** that contain the setting's data immediately.
- **Ensure that you only install software that the setting's IT team has reviewed and approved.**
- Only download files or programmes from trusted sources

Data Sharing and Transfer

- **Share sensitive information only through secure, authorised methods** (e.g. encrypted email, password protected documents)
- **Ensure recipients of shared data are authorised to receive it** and are aware of their responsibilities for its protection
- **Avoid transferring sensitive information over unsecured public networks**

Physical Security

- **Keep work areas clear of sensitive documents when unattended** - operate a clean desk policy
- **Store physical records in locked cabinets when not in use**
- **Shred sensitive documents or use secure destruction bins**
- **Only take information off site if you are authorised to do so, and only when it is necessary.** Ensure that access is secure e.g. do not let others within your home view or use the school's laptop, or access any physical files containing student names and personal data

Incident Reporting

- **Immediately report any suspected or actual security breaches** to the IT department or designated security officer.
- **If you send an email in error that contains the personal information** of another person, you must immediately i**nform the Data Protection Lead** within the setting and follow any recording requirements.
- **Provide complete and accurate information about the incident** to facilitate investigation and resolution.

Further reading resource:

Government have provided a resource which details the policies and processes that schools and other settings need in place to protect personal data and respond effectively to a personal data breach.

https://www.gov.uk/guidance/data-protection-in-schools

This toolkit will help school staff, governors and trustees:

- **Understand how to comply with data protection law**
- Develop their data policies and processes
- **Know what staff and pupil data to keep**
- **Follow good practices for preventing personal data breaches**

Should you identify that you require any further training or CPD in relation to data security, please speak with your consultant who will seek to facilitate this for you.