WOODLANDS SCHOOL
PURSUE EXCELLENCE & SEIZE OPPORTUNITIES

Data Handling Security Policy

Version 1:	June 2018
Date approved:	June 2018
Approved by:	Standards, Staffing and Curriculum
Next review:	June 2019

Purpose

This policy is used to explain the responsibilities for managing IT equipment, removable storage devices and papers. Locations for data handling include, in the office, in transit, and at home or other work locations.

Principles

1. You must take responsibility for the security of the equipment allocated to you, and that under your supervision.

2. When you are physically transporting our data outside of our premises, on any medium, you must take steps to keep it secure, preventing accidental loss. This relates to paper files, phones, laptops and other removable media such as USB memory sticks, discs and external hard drives. Items should not be visible to others; even partially. This means they should be secured within an appropriate bag or other robust container. Laptop bags are suitable, ensuring that zip compartments are closed concealing the contents. Employees frequently needing to transport quantities of information that are too bulky to carry under full control and/or transporting Official-Sensitive data must review with their manager the need for being supplied with wheeled suitcase-style equipment with code locks to further secure the information.

3. You must not leave Official-Sensitive data unattended in a vehicle for longer than 10 minutes, and always keep it out of sight. Items such as paper files, phones, laptops and other removable media left in a vehicle should only be unattended for a short period of time and must be kept out of sight. Locked in a boot is considered secure for a limited time if it cannot be taken with you when leaving a car.

4. You must take appropriate steps to secure our data at home and other organisations' premises. Only authorised users can use your IT equipment and only through using their own accounts. It is not acceptable to allow family members or friends to use IT facilities or have access to our information even if you are present. You must also make sure that when IT equipment and hard-copy information is not in use, that it is stored securely out of sight. If you are located temporarily in the premises of another organisation, or your work requires site visits or entering homes of service users, you must secure IT equipment and hard-copy information. Make sure you understand what information your role allows you to share with partners or service users and limit the information you make available accordingly. Your role may require you to allow someone to have access to your IT device, for example a service user in their home may need to read content on your screen and select options from menus. If you are located in the premises of another Organisation as a semi-permanent base, it is reasonable to leave our data in your allocated office or team area provided that you have the same level of secure storage for equipment and hard-copy as you would in our buildings.

5. If working with our data on approved unmanaged equipment, you must remove the data when finished. On most systems this can be done by selecting 'public network' when setting up the access. Otherwise it will need to be done manually in the web browser options.

6. If you are taking Official-Sensitive information out of the office, this must be recorded. You should have access to systems or a log which allow you to 'sign-out' or record what information you are taking custody of, when taken, when returned and (if appropriate) why and under whose authority. Where such facilities are available they must be used.

7. You must make sure that conversations discussing sensitive data are only audible by an appropriate audience. You must make sure that if you are overhearing or otherwise being exposed to data to which you should not have access, you alert the information custodian to the fact that they are not managing the information appropriately. We have a duty to make sure that personal data is only made available to those with the business need to access it.

8. You must not allow anyone access to your IT equipment through your IT account. Make sure that you lock your screen at all times if you leave your laptop/ desktop or phone unattended to avoid someone accessing your account without your knowledge. Always supervise and monitor anyone using your device in the strictly limited circumstances where allowing someone access is acceptable. All activity on your IT account is assumed to be yours.

9. You must not use any equipment to store our business data that has not been approved. This is including but not limited to computers, printers, phones, tablets and cameras. Where technically feasible, encryption will be applied to secure the contents of storage devices.

10. You must not allow unauthorised people to be able to view information on your IT equipment display. Ensure that no-one in your vicinity can see and read the screen of your device. This applies to working in public places (such as cafes with Wi-Fi), in partner organisations' offices, and even when hot-desking within our premises when viewing Official-Sensitive data unless you are certain that others around you are allowed to see similar data.

11. If you use Outlook Web Access from an unmanaged device, you must not save your password in the browser. Saving your password, introduces the risk of someone gaining access to private work information.

12. You must always use an approved secure method of disposing of physical documents and data storage devices. Secure destruction processes safeguard the information stored on IT devices and physical documents and prevent data being accessed by unauthorised persons

13. You must return all equipment which has been issued to you by us prior to leaving your employment. We reserve the right to treat instances of refusing to return such items as theft.

14. You must report as quickly as possible if your equipment is lost or stolen and assist with any investigation. If this happens, you must raise a security incident and inform your manager. This enables prompt removal of data from devices remotely, reducing the risk.

15. You must ensure that all security functions are enabled on your portable equipment, such as pin codes and password access.

16. You must keep your portable equipment, clean and serviceable, including keeping it charged.

17. You must not take any of our equipment abroad unless you are traveling in a business capacity with approval.

18. You must not give your portable equipment to another person if you are not using it. Portable equipment is asset managed across our estate and assigned to an individual.

Complaints

Complaints about the above policy should be made to the I.E.B/Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Contacts

If you have any queries or concerns regarding these policies/procedures then please contact Mr S Cox, Headteacher.

Signed:_____ Dated: 11th June 2018

Head Teacher

Signed:_____ Dated: 11th June 2018

Chair of Governors

U**pdated June 2018**

PURSUE EXCELLENCE AND SEIZE OPPORTUNITIES