HADLEIGH INFANT & NURSERY SCHOOL

Data Handling Security Policy

2022-2023

Version	**5**
Document authors	**Sam Proctor**
Other contributors	**IGS**
Policy produced (date)	**September 2022**
Policy approved by	**SIRO / IC / IGG**
Policy approved (date)	**September 2022**
Policy to be reviewed (date)	**December 2022**
Other related policies	**Data Protection Policy** **Security Incident Policy** **Acceptable Personal Use Policy** **Statutory Request Policy** **Privacy Notice** **Complaints Policy** **Whistleblowing Policy**
Other paperwork attached	

Version History Log for this document

Version	Date Published	Details of key changes from previous version
5	September 2022	Changed references to Mr. S. Proctor to Mrs. D. Glanville - New Head Teacher. No changes made to main body of text.
4	December 2021	Further clarification linked to removing data from unmanaged equipment - why and how this can be done.
3	January 2021	Staff are instructed to not save passwords when logging into accounts. Section added to outline the responsibility to raise as a security incident any loss, unlawful access or theft of the data we are responsible for.
2	April 2019	Data Protection Act 1998 changed to Data Protection Act 2018
1	April 2018	New policy created - supersedes all previous policies.

Roles within the school

Data Protection Officer (DPO) - Ms. L. Almond

Senior Information Risk Owner (SIRO) - Mrs. D. Glanville

Information Champion (IC) - Mrs. A. Cain

Information Governance Governor - Mr. I. Holroyd

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting Mrs. D. Glanville(Head Teacher - SIRO - head@hadleigh-inf.essex.sch.uk)

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.

What I must do	Why I must do it	How I will do it
You must take responsibility for the security of the equipment allocated to you and that is in your custody.	You are the custodian of the equipment; it is your responsibility to keep it physically secure.	By following the points in this policy.
When you are physically transporting our data outside of our premises, on any medium, you must take steps to keep it secure.	To prevent any accidental loss (for example papers or removable media accidentally falling out of bags), or theft (by exposing papers or equipment by not securing them properly). Although laptops are encrypted, it is still possible for a motivated criminal with technical knowledge to access data.	This relates to paper files, phones, laptops and other removable media such as USB memory sticks, discs and external hard drives. Use equipment which reduces physical effort in order to appropriately manage the risk of overloading or forcing a tenuous hold over physical documents which can result in accidental loss of control over the information. 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.
You must not leave Official-Sensitive data unattended in a vehicle for longer than 10 minutes, and always keep it out of sight.	Experience in investigation of thefts at employee homes has shown that if equipment is left in plain view it will be taken, whereas storing away out of sight when not in use results in fewer cases of theft.	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 (maximum of 10 minutes for Official-Sensitive information) and must be kept out of sight (not visible to anyone looking in through a vehicle

		window). Locked in a boot is considered secure for a limited time if it cannot be taken with you when leaving a car.
You must take appropriate steps to secure our data at home and other organisations' premises.	To prevent accidental loss, unauthorised use and theft in your home and whilst in other Organisations' premises.	Only authorised users (this means people with IT accounts provided by us) 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. You must understand the limits of their access requirements and manage this access. 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. You must get

		approval for storing our data in premises not managed by us from your manager if the location is anything other than your permanent office base.
If working with our data on approved unmanaged equipment, you must remove the data when finished, including from cloud storage, and prior to leaving the school's employment.	School data may become available to unauthorised persons. Data in the browser cache or temporary file storage may be useable by other subsequent users of the same device.	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. All school data must be permanently deleted from a personal device when no longer being worked on or when the employee leaves the school.
If you are taking Official-Sensitive information out of the office, this must be recorded.	To make sure that others know who has custody of important information at all times.	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.
You must make sure that conversations discussing sensitive data are only audible by an appropriate audience.	We have a duty even within our premises to make sure that personal data is only made available to those with the business need to access it. This applies verbally as well as in recorded form.	Most employees who handle Official-Sensitive data will have been located with those of similar roles or be in self-contained spaces. However, there is always the possibility of unauthorised persons being in the vicinity when you may need to discuss sensitive personal data with colleagues near you or over the phone, or display on a screen. You must make sure as the person who is custodian of the information that it is appropriate to discuss or display the information in the circumstances. 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.
You must not allow anyone access to your IT equipment through your IT account.	All activity on your IT account is assumed to be yours. Logs of activity are maintained. You are accountable for any wrongdoing through your 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 (for example a service user in their home may need to read content on your screen and select options from menus).
You must not use any equipment to store our business data that has not been approved.	Equipment purchased through us will have appropriate technical security installed, or will have best practice guidance on how to use the equipment securely. Only personal equipment which has been approved by the school can process school data.	This is including but not limited to computers, printers, phones, tablets and cameras. Order equipment through us and follow any conditions of use associated with an exception to policy, and follow any standard instructions that are supplied with the device. Where technically feasible, encryption will be applied to secure the contents of storage devices.
You must not allow unauthorised people to be able view information on your IT equipment display.	Unauthorised people may be able to see sensitive information on your screen.	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 hotdesking within our premises when viewing Official-Sensitive data unless you are certain that others around you are allowed to see similar data.

You must not save your passwords to any web based system which holds our data in the browser.	This introduces the risk of someone who can gain access to your device also getting easy access to the data on your work emails.	Do not approve any offer from your device's browser to save your password when logging in.
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.	Make use of the facilities for secure disposal of paper documents and IT storage devices.
You must return all equipment which has been issued to you by us prior to leaving your employment.	Providing such items is costly and represents a data security risk. We reserve the right to treat instances of refusing to return such items as theft.	Follow a leavers checklist with your manager.
You must report as quickly as possible if your equipment is lost or stolen and assist with any investigation.	This enables to promptly remove data from devices remotely, therefore reducing the risk. Such investigations may lead to disciplinary action, and in extreme circumstances could lead to the service area seeking financial remuneration. Having all the information about a security incident helps us to resolve it quickly and take the appropriate action to manage any risks of information being lost.	Raise a security incident and inform your manager. Provide any information requested of you by an investigating officer.
You must ensure that all security functions are enabled on your portable equipment, such as pin codes and password access.	Such measures help keep the device and information available on it secure.	Follow the instructions provided to you with your equipment.
You must keep your portable equipment, clean and serviceable, including keeping it charged.	Correct use and basic maintenance helps us gain best value from the investment we make in our equipment.	Follow the instructions provided to you with your equipment.

You must not take any of our equipment abroad unless you are traveling in a business capacity with approval.	We need to be aware of any risk of using our equipment abroad, especially in countries who do share common legislation to safeguard personal data, and where internet services may expose our devices and therefore our network to malicious threats. There may also be costs involved in replacing equipment which is subject to precautionary measures on your return. The costs of reviewing requests and replacing equipment are not appropriate for instances of employees wanting to use equipment whilst on holiday. Business continuity cover arrangements and delegation should be able to manage instances of leave.	Request an exception to policy request have your case considered.
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. Being able to accurately evidence who holds what equipment is an important assurance we give to the Information Commissioners Office over our ability to manage our assets and the information available on them.	Ensure that any equipment given or received by you is through our processes.
You must immediately raise as a security incident any loss, unlawful access or theft of the data we are responsible for.	Reporting security incidents allows us to manage our risks and ensure that we take step to avoid similar occurrences.	Follow the Security Incidents policy.

Contacts

If you have any enquires in relation to this policy, please contact Mrs. D. Glanville(the school's Head Teacher) on 01702557979 or head@hadleigh-inf.essex.sch.uk . The Head Teacher will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office - www.ico.gov.uk

References

- Data Protection Act 2018
- General Data Protection Regulations 2016
- Article 8, The Human Rights Act 1998