HADLEIGH INFANT & NURSERY SCHOOL

Acceptable Personal Use Policy

2021-2023

Version	**4**
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)	**January 2023**
Other related policies	**Data Protection Policy** **Data Handling Security Policy** **Security Incident Policy** **Statutory Request Policy** **Privacy Notice** **Complaints Policy** **Procedures for Reporting and Handling Security Incidents Policy**

Version History Log for this document

Version	Date Published	Details of key changes from previous version
4	September 2022	Changed references to Mr. S. Proctor to Mrs. D. Glanville - New Head Teacher. No changes made to main body of text.
3	January 2021	Names of key data protection roles added.
2	March 2019	Data Protection Act 1998 changed to Data Protection Act 2018
1	April 2018	New Policy created superseded all previous versions.

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

Purpose of the policy

This policy will set out what is acceptable use of resources and assets provided by the school, including IT facilities and covering personal use of these.

What I must do	Why I must do it	How I will do it
You must use our facilities economically; your personal use must not create extra costs for us.	To ensure we use our IT and other facilities resources effectively, making sure that our reputation is maintained and to ensure that staff working time is used efficiently on delivering our business outcomes.	By checking with your manager or where you have any uncertainty over what is appropriate.
You **must not** use our facilities to undertake any unlawful, libellous, immoral or offensive activities, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, pornographic, sexual, violent or criminal content and racist, sexist or otherwise discriminatory material.		By complying with the points of this policy.
Personal use must not interfere with your productivity and how you carry out your duties.		You must only make personal use of our IT facilities outside of time you are recording or is designated as your 'working hours'.
Personal use must not reflect adversely on our reputation.		By complying with the points of this policy.
You must not leave personal-use websites open during your working time, even if they are minimised on your screen and you are not actively viewing/ using them.		Closing websites when you are not actively using them.
You must not use browsers or access/ attempt to access sites that are knowingly unacceptable, even if this is in your own time.		By taking care over the sites you are about to open, including reading search report information before opening.
You must not send or forward chain, joke or spam emails.		By deleting such items if you receive them.
You must not use the Organisation's facilities for commercial purposes not approved by us or for personal financial gain.		By checking with your manager where you have any uncertainty over what is appropriate.
You must not use your access rights or identity as an employee to mislead another person, for personal gain or in any other way which is inconsistent with your role.		By checking with your manager where you have any uncertainty over what is appropriate.

You must not disclose (in writing, speech or electronically) information held by us unless you are authorised to do so, and the recipients are authorised to receive it.		If you are not sure if you are authorised to disclose information, speak with your manager in the first instance.
When you print, photocopy, scan or fax official-sensitive information, you must not leave the information unattended.		If you are faxing information outside your immediate office, always make sure that there is someone waiting at the other end to receive it. For other devices, if there is no secure release facility which requires you to be present, you must ensure you wait for the process to complete and remove any originals and copies from the equipment.
You must not connect any equipment to our IT network that has not been approved.		Check that equipment has been tagged or marked as an accepted and managed device before insertion/ connection.
You must not do anything that would compromise the security of the information held by us, such as downloading/ spreading any harmful virus/ program or disabling or changing standard security settings.		IT controls should prevent your ability to download anything harmful, but if in doubt, contact your manager in the first instance.
You must not make personal use of the information available to you that is not available to the public.		If you wish to utilise Organisation data in a personal capacity, you must make a formal request for information to the Organisation.

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.

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