IT Acceptable Use Policy

Governors Meeting:	**18 July 2022**
Safeguarding Governor:	**Jane Owens**
Chair of Governors:	**Gail Webb**
Review:	**17 July 2022**

Contents

1. Overview

Huxley CE Primary School has provided computer equipment for use by staff as an important tool for teaching, learning, and administration of the school. Use of school computer equipment by members of staff is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to the Admin Officer in the first instance.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Deliberate abuse of the school's computer system may result in disciplinary action (including possible termination), and civil and/or criminal liability.

Please note that use of the school network is intended to be as permissive and flexible as possible under current UK legislation, DfE guidelines and the UK General Data Protection Regulations (UK GDPR). This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the school and staff, to safeguard the reputation and Cyber Security of the school, and to ensure the safety of all users.

2. Computer Security & Data Protection

- I understand that I **must not disclose** any **password** or username to anyone, other than the persons responsible for running and maintaining the IT systems.
- I understand that I must not allow any pupil to use my login to any of the IT systems for **ANY** reason.
- I understand that pupils must not be allowed to use staff computers.
- When leaving a computer unattended, I must ensure I have either logged off my account, or locked the computer to prevent anyone else using my account in my absence. Failure to do so would result in a breach of UK GDPR.
- I must not store any sensitive and/or personal information about staff, students, or any individual, on any portable storage system (such as a USB memory stick, portable hard disk, or personal computer).
- I understand that I will not insecurely store sensitive data in cloud storage of any kind. For example; share sensitive information with external sources. I understand that I must take every reasonable precaution to secure any data or equipment removed from any of the school's premises.
- I must not make any copy of data to any storage systems other than the network storage drives or equipment provided for business use. This includes USB memory sticks and external hard drives (even those owned or issued by the school), cloud storage (non-school) or a personal computer. Advice regarding backups can be obtained from the relevant IT Support team.
- I will only use any personal device (that is any equipment not issued by the school) for school or business-related work in accordance with the Mobile Device policy.
- I must ensure that items of portable computer equipment (such as laptops, iPads, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended on the premises.
- I understand that the school can monitor any data on the network to ensure policy compliance, and to aid in resolving networking issues.

- I understand that any assets (electronic data or otherwise) created during employment with the school remains the property of the school, during and at the end of employment. The continued use of any school assets (e.g. learning resources) in another setting or context once employment with school has terminated requires prior authorisation from the Headteacher.
- Removable media of any type is not permitted on any of the school IT equipment. This includes (but is not limited to) USB Sticks, External Hard Drives, CD and/or DVD discs, personal cloud storage.
- I must ensure that only computers with full and up-to-date anti-virus and anti-malware will be connected to any school network.
- Only devices owned and managed by the school will be connected to any core network.

3. Student and Staff Protection

- I am aware of all guidelines to conceal student identities when publishing to the public domain.
- I understand that pupils must be supervised at all times when in an IT suite or on computer equipment.
- I will escalate noncompliance by puils in accordance with school policy.
- The school acknowledges that staff photographs and personal data will not be published without permission.

4. Use of Email & other electronic communications

- Email has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of emails may therefore have to be made available to third parties. You must be cautious when sending both internal and external emails. The professional standards that apply to internal memos and external letters must be observed for email.
- Email to outside organisations has the same power to create a binding contract as hardcopy documents. Check emails as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending.
- You must not purchase goods or services on behalf of the school via email without proper authorisation.
- All school emails you send should have a signature containing your name, job title and the name of the school you work at .
- I must not send chain letters or unsolicited commercial e-mail (also known as SPAM).
- I agree that the use of email and any attachments is intended for the addressee only, and that I will try my utmost to ensure that it is virus/malware free.
- Any opinions expressed within emails are those of the author and do not represent those of the school.
- The school accepts no responsibility for any loss or damage arising in any way from the use of an email.

- I agree that I shall only use the email services provided by the school for any work-related communication.
- Email is only permitted for use on a personal mobile device if that device complies with the required policy (i.e. it has a passcode set).
- If any form of video conferencing is being used, always ensure that you are aware of your surroundings and what may be able to be seen or heard through your computer.
- Any email sent in error should be reported in accordance with the Data Breach policy.

5. Reporting Incidents

- I will immediately inform the Headteacher any websites accessible from within the school feel are unsuitable in any way for student consumption.
- I will immediately inform the Headteacher of any abuse to the IT system(s) - software and hardware - providing the location and names where possible.
- I will immediately inform the Headteacher of any inappropriate content suspected to be on the IT system(s). This may be contained in email, documents, pictures etc.
- I will immediately report any breaches, or attempted breaches, in security to the Headteacher in writing.
- I will inform the school UK GDPR representative if I have either committed or become aware of a UK GDPR data breach or UK GDPR near miss data breach.

6. Software, Hardware, Copyright & Licensing

- I will not attempt to install any software or hardware without consent from the relevant school IT Support team, and any software agreed will require the appropriate licence(s).
- Before purchasing any hardware or software I will consult the Admin Officer to check compatibility, licence compliance, UK GDPR compliance, and discuss any other implications that the purchase may have.
- I will respect copyright and make sure I do not use any information breaching copyright laws.
- Under no circumstances must any software from potentially illegal sources be installed.
- I will not engage in activities that waste technical support time and resources.
- It is agreed that computer devices are supplied for professional use, and therefore any personal use (such as storing photos, music, videos and games etc.) is not the responsibility of the school and is not permitted.
- Computer equipment has been supplied to me on the basis that I will look after it responsibly and treat it as if it were my own property. I understand that any damage caused to, or any loss of equipment assigned to me, not considered to be general “wear and tear” may be charged to me.

7. Unacceptable Activity

The following actions are considered to be unacceptable and will result in investigation which may result in disciplinary action:

- Visiting internet sites that contain obscene, racist, or other offensive material.
- Making or posting obscene, indecent, racist or offensive remarks or comments on the internet or email systems, nor should you entice others to do so.
- Soliciting email or other internet-based services which are not directly related to the school or using the internet or any of the associated services for personal gain.
- Transmitting any material that is defamatory or which is intended to offend, annoy, harass, bully, or intimidate another person or persons.
- Expressing any personal opinions as being representative of the school, whether in private emails or in public areas of the internet.
- Downloading from the internet any music, video, or software for personal use.
- Uploading, downloading or transmitting any copyrighted materials belonging to parties outside of the school (note: some publishers allow the downloading of copyright material but this must then not be distributed. Users should ensure that they adhere to any publishers' download policies).
- Publishing or otherwise revealing any commercially sensitive, confidential or proprietary information including but not limited to: financial data, internal memos, minutes of meetings, management reports, or business operation details unless required to do so in the pursuit of normal business operations.
- Downloading any software or other electronic files for school purposes without utilising the appropriate TPLT approved anti-virus and anti-malware protection measures.
- Intentionally interfering with the normal operation of the TPLT network by downloading excessively large files (over 1GB) or making use of streaming video or audio feeds (without proper reason). This activity significantly impacts our communications lines and will negatively affect others.
- Attempting to access information for which you are not authorised.
- Sharing login details and/or passwords with others.
- Attaching a modem, router or another networking device to your computer in order to gain direct and unmonitored internet access (this can also introduce viruses and malware onto our network).
- Changing the configuration of the school supplied computing equipment to alter network settings or Internet access controls unless directed to do so by the IT Support staff at your school.
- Unauthorised sharing of any personal data, including that of students, staff or other contacts known to the school, which could be in breach of UK GDPR legislation.

When using school systems you are required to:

- Make use of your internet access in a judicious and considerate manner
- Ensure that every precaution is taken to protect the school's reputation and good name
- Report any breaches of this Policy (or any other IT Policy) by any staff member or student to the appropriate person
- Note that all use of staff email systems will contain a disclaimer and legal notices automatically

Failure to follow this policy will result in disciplinary investigation which may lead to disciplinary action. The school also reserves the right to report any illegal or criminal violations to the appropriate authorities.

8. Agreement

By accepting this document, you agree that you have read and understood the acceptable use policy and your responsibility of enforcing it, and other IT related policies.

9. Policy Review

The working of this policy will be reviewed by the IEB annually. As well as examining the specific review data, the policy statement will be checked for continuing relevance against any changed statutory requirements.