Timothy Hackworth Primary School

'Respectful and resilient; being the best that we can be.'

Staff Acceptable Use Policy

CRC Article 19: All children have the right to be safe.

Date policy approved/adopted:	**February 2024**
Next review date:	**February 2025**
Approved by:	**Governing Body**
Head Teacher signature:	*L. Boulton*
Governor signature:	*P. Crook*

Staff Acceptable Use Policy

Date of Policy: February 2024

Review Date: February 2025

Governors: Mrs. Pauline Crook – Safeguarding Governor
Curriculum and Standards Committee

This policy should be read in conjunction with our Safeguarding Policy, Keeping Children Safe in Education, September 2023, Behaviour (Respectful Relationships) Policy, Online Safety Policy, Data Protection Policy, Low-Level Concerns Policy, our Staff Code of Conduct and Timothy Hackworth Pupils' Online Safety Agreement. All policy and practice in Timothy Hackworth Primary School respects children's dignity.

Our Timothy Hackworth School Vision

May our Rights Respecting School be a happy place for us all to learn; where every one of us is valued and safe in our Timothy Hackworth School Family. May we all be the best that we can be by making a positive difference to each other, our community in Shildon and the wider world in which we all live.

Mission Statement (written by children):

We would like our school, which reflects British Values, to be at the heart of the community, sharing, supporting and learning together with everyone as equals. Our children have the right to high quality learning experiences to help them to be the best that they can be.
We encourage our children to be creative, unique, open-minded and independent individuals, respectful of themselves and of others in our school, our local community and the wider world.
We aim to nurture our children on their journey through life so that they can grow into safe, caring, democratic, responsible and tolerant adults who make a positive difference to British Society and to the world.

Values

Ours is a happy school with high hopes and ambitions for all our children and we welcome working in partnership with parents and carers to ensure that everything is done in the best interests of the children at all times.

All of our staff take their responsibility towards the children seriously and they strive to help each child reach their full potential as global citizens physically,

emotionally, socially and academically. We are fully committed to the CONVENTION ON THE RIGHTS OF THE CHILD.

To us, every child is unique and precious and we endeavour to foster a high level of motivation towards learning and behaviour. We are committed to the basic skills of English and Maths.

At all times, we aim to centre the teaching in an atmosphere of mutual respect and personal respect. A high quality education is the right of every child, and at Timothy Hackworth Primary School, we embrace that responsibility and strive to achieve it for all our pupils.

Equalities Information

This policy should be read in conjunction with our school's 'Equalities Policy Statement', 'Equalities Objectives Summary' and 'Equalities Information and Objectives'.

We welcome our duties under the Equality Act 2010 to eliminate discrimination, advance equality of opportunity and foster good relations in relation to age (as appropriate), disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation (LGBTQ+).

Rationale

It is important that all staff and governors are aware of a common set of rules for the safe use of computing technology. This is to protect pupils, staff, governors and the reputation of our school. This is a document which will continue to undergo modification as both technology and the law relating to technology develop further. This policy links to the schools wider safeguarding systems.

Schools have a duty of care to safeguard and protect staff under the Health and Safety at Work Act 1974, and the Management of Health and Safety at Work Regulations 1999. Key legislation also includes Section 11 of the Children Act 2004 which places a duty on key persons and bodies to ensure that their functions are discharged having regard to the need to safeguard and promote the welfare of children.

A Staff AUP is not intended to unduly limit the ways in which members of staff teach or use computing, but aims to ensure that the school and all members of staff comply with the appropriate legal responsibilities, the reputation of the school is maintained, and the safety of all users is ensured.

In order to protect staff members and governors, it is essential to have an AUP in place which has been viewed and understood. All employees of the school must be aware of the school's expectations for the use of information systems and professional conduct online whether on or off site.

It is important that all members of staff and governors are made aware that their online conduct, both in and out of school, could have an impact on their role and reputation. Civil, legal or disciplinary action could be taken should they be found to have brought the profession or the school into disrepute, or if something is felt to have undermined confidence in their professional abilities. It is therefore important that the AUP is firmly embedded within the school, and is part of the induction process for all members of staff, governors and volunteers. All members of staff and governors receive up-to-date and relevant training as appropriate. All members of staff and governors will read, understand and sign the AUP to indicate their understanding.

It is recommended that any contact with pupils and parents only takes place via school approved communication channels e.g. school email address, or the school learning platform, so it can be monitored and traced in the case of an allegation or concern.

Staff and governors are made aware of the boundaries and professional practices online in order to protect their professional status. Staff and governors should be advised to check their privacy settings on any personal social media sites they use, however, staff and governors are reminded that once content is shared online it is possible for it be circulated more widely than intended without consent or knowledge, even if the content is thought to have been deleted or privately shared.

Any online behaviour and activity by a member of staff or governor whilst using the school systems must be in accordance with this policy.

As a professional organisation, with responsibility for children's safeguarding, it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff and governors have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff and governors are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff and governors are reminded that computing use should be consistent with the school ethos, other appropriate policies and the law.

1) I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, tablets, iPads, digital cameras, email and social media sites**.**

2) School owned information systems must be used appropriately. I understand that the Computer Misuse Act 2022 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3) Staff mobile phones are stored in staff lockers during the school day and may only be used in the Staff Room. Staff mobile phones must not be used where there are children around, unless SLT have granted specific permission for this, due to specific circumstances.

4) Cameras on personal phones, personal iPads or personal tablets will not be used to take pictures of children in any circumstances. Images will be securely deleted from non-encrypted devices on a regular basis (e.g. transferred from a digital camera to the network on a weekly basis.

5) Images will not be kept for longer than is to be considered necessary and, in any event, not exceeding a maximum of three years after the child has left the school. A designated member of staff (Data Protection Officer) will ensure that systems exist so that all photographs are permanently wiped when no longer needed.

6) I understand that any hardware and software provided by my school for staff use can only be used by members of staff and can only be used for school related work.

7) To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

8) I will respect system security and I will not disclose any password or security information. I will use a 'strong' password. A strong password has numbers, letters and symbols, with 10 or more characters, does not contain a dictionary word and is only used on one system.

9) I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the Head Teacher.

10) Data Protection

a) I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018, or the General Data Protection Regulations 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary, and will be kept private and secure with appropriate security

measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any personal data which is being removed from the school site, such as via email or on memory sticks, will be encrypted by a method approved by the school. Secure means of transporting data are encrypted laptop, encrypted USB memory, encrypted HDD, or approved cloud-based system.

b) If I choose to use a portable device (phone, tablet, iPad etc…) to access my work e-mail, I will ensure that the device is locked by a pin code, password or ID authentication and will be wiped when I dispose of the device.

c) I will not transfer sensitive personal information from my school e-mail account, e.g. Safeguarding, SEND information, Medical Information and religious information, UNLESS the information is encrypted.

d) I will not keep professional documents which contain school-related personal information, including images, files, videos etc., on any personally owned devices.

e) Digital images or videos of pupils will only be taken from the school premises using encrypted memory.

f) I will not use unapproved cloud storage systems (Dropbox, iCloud etc.) for storing personal data of staff or pupils.

11) I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

12) I will respect copyright and intellectual property rights.

a) I have read and understood our school Online Safety Policy which covers the requirements for safe ICT use, including using appropriate devices, and the safe use of social media.

b) I will not communicate with pupils or ex-pupils using social media.

c) My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number.

d) My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications

and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the law.

e) I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute. This would include any comment made, even in the belief that it is private on social media.

13) I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Leads: Mrs. L. Boulton, Mrs. S. Simpson-May, Mrs. K. Kozlowski, Mrs. N. Nixon and Mrs. B. Mathwin and the Online Safety Leads, Mrs. L. Boulton and Miss M. Curbeson, as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Leads as soon as possible.

14) I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents, files or school access keys, then I will report this to the School Engineer, Mr. Graham Keenan, and to the Head Teacher, as soon as possible.

15) I will teach Online Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

16) If I have any queries or questions regarding safe and professional practice online, either in school or off site, then I will raise them with the Online Safety Leads, Mrs. L. Boulton and Miss M. Curbeson.

17) I understand that my use of the information systems, internet and email may be monitored and recorded to ensure policy compliance.

The school may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails, in order to monitor compliance with this Acceptable Use Policy and the school's Data Protection Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the school will invoke its disciplinary procedure. If the school suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.