ALDERMAN RICHARD HALLAM PRIMARY SCHOOL

ARH – Educating a community of life-long learners

Acceptable Use Policy

Policy Reviewed: September 2024

ALDERMAN RICHARD HALLAM PRIMARY SCHOOL

Acceptable Use 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 have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff 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 are reminded that I.C.T. use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

All members of staff, students on placement, supply teachers etc. must sign a copy of this policy statement before a system login password is granted. All children must be made aware through class discussion of all the important issues relating to acceptable use, especially the monitoring of internet use.

1. I understand that Information Systems and I.C.T. include networks, data and data storage, online and offline communication technologies and access devices. This includes, but is not limited to: staff laptops, iPads, digital cameras, email, mobile phones and social media sites**.** The computer system is owned by the school whether as part of the school's integrated network, stand-alone, or taken offsite.

2. School-owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: 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. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use; under no circumstances should staff allow anyone else to use their laptop or iPad, including family members such as a partner or children. 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.

4. I will not attempt to install any purchased or downloaded software, including browser toolbars or hardware, without permission from the Business Manager and as long as it is legitimately licensed and poses no threat to the school network. For the iPads, no apps are to be brought or in-app purchases to be made by anyone other than the ICT/Computing team (Computing Lead, ICT Technician or Business Manager).

5. 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). I will keep a passcode on any iPad that has been loaned to me; I understand that this is for safeguarding and security reasons.

6. I will ensure that any personal data of pupils, staff or parents and carers is kept in accordance with the GDPR 2016 / Data Protection Act 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 that meet the EU and UK regulations). Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the Internet Publishing Statement (see Online Safety Policy) and will always take into account parental consent.

7. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones) nor will I connect them to the school's network without express permission from SLT and the school Business Manager.

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information. I will protect the devices in my care from unapproved access or theft; the school's insurance policy does cover equipment, including laptops, when they leave the school premise. Note: our school insurance policy provides cover for equipment onsite, provided it is looked after with due care and offsite as long as it is locked in the boot in transit and correct precautions are used when storing at home.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school's Online Safety Policy, which covers the requirements for safe I.C.T. use, including using appropriate devices, safe use of social media websites (Social Media Policy) and the supervision of pupils within the classroom and other working space.

11. I will report all incidents of concern regarding: children's online safety, accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to a Designated Safeguarding Lead and/or the Online Safety Co-ordinators (Wayne Holder and Louise Ellis) as soon as possible.

12. 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 or files, then I will report this to the ICT/Computing team as soon as possible.

13. My electronic communications with pupils, parents and carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school-approved communication channels e.g. via a school provided email address, Seesaw Family messages or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership Team in line with the Staff Code of Conduct.

14. I will ensure that my online reputation and use of I.C.T. and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of I.C.T. and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school's AUP, Staff Code of Conduct and the Law.

15. 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 City Council, into disrepute.

16. I will promote 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.

17. 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 a Designated Safeguarding Lead and/or the Online Safety Coordinators or the Headteacher.

18. I understand that my use of the information systems, internet and email is monitored by the Smoothwall monitoring system and recorded to ensure policy compliance. It is the responsibility of the Headteacher, the Deputy Headteacher, DSLs and the Business Manager to review this activity periodically. It is the duty of the Business Manager or other DSLs to report any transgressions of the school's Online Safety or Acceptable Use Policy and/or use of obscene, racist or threatening language detected by the system to the Headteacher. Where it is believed that unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, it will be reported to the Headteacher and will be dealt with according to the school's and LA's disciplinary policy, or through prosecution by law. This is in line with our Safeguarding and Child Protection Policy which follows KCSiE 2024 and the 4 key areas of risk relating to online safety (Part 135).

19. Use of portable equipment
    The school provides portable I.C.T. equipment such as laptop computers, iPads and tablets etc. to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.
    - Certain equipment will remain in the care of the ICT/Computing team and may be booked out for use according to staff requirements. Once equipment has been used, it should be returned to the staff room as soon as possible and put on charge ready for the next user. Any costs generated by the user at home, such as phone bills, printer cartridges etc. are the responsibility of the user;
    - Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc.) or maternity leave, arrangements must be made for any portable equipment in their care to be returned for school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it;
    - If an individual leaves the employment of the school, any equipment must be returned, including iPads, laptops, memory sticks and memory cards etc.;
    - Equipment such as cameras (and accessories), storage devices (memory pens etc.) are the sole responsibility of the individual and must be replaced with like for like if lost or misplaced if proven that the individual has been negligent. This is at the Headteacher or Deputy Headteacher's discretion only;
    - All provided equipment is loaned to individuals and remains the property of the school;
    - Do not sign in to your personal Apple account on the school iPads or make use of your own iCloud service;
    - Inform the ICT/Computing team if there is any damage to the devices straight away;
    - Staff iPads may be added to home networks for internet access and updates, however they will require the use of Futures Browser that will screenshot any inappropriate use as per point 18;
    - All staff will keep a passcode on any iPad that has been loaned to them; this is for safeguarding and security reasons;
    - If any staff iPad or pupil iPads are lost, stolen or damaged, the ICT/Computing team must be informed as soon as possible so that it can be found and remotely wiped as quickly as possible to avoid data falling into the incorrect hands;

- All iPads have management software on them that allows them to be found, install software and wiped. This is for the safety of the school as all iPads remain the property of the school, even if assigned to an individual user.

20. I.C.T. in the Foundation Stage
    - Personal mobile telephones or cameras are not allowed in the Foundation setting to take photographs for a child's Learning Journey.
    - Only tablets or school iPads will be used for this purpose. Once photographs have been printed, they will be stored securely on the server or uploaded to Seesaw.
    - Once a child leaves the Foundation Stage, photographs will remain on Seesaw as evidence of a child's achievement or proof that certain activities have been completed.
    - Parents and carers are requested to complete a consent form which allows the school to use photographs for displays around school, on the school website or for stories about the school in the press in line with UKGDPR 2016/ Data Protection Act 2018.
    - For more information regarding the use of I.C.T within the EYFS, please speak to either the EYFS Lead, Computing Lead or Business Manager.

21 Use of AI
    - AI is a powerful tool and can be used to support in the school. However, it must be used appropriately and in line with both the rest of the AUP, the policies linked below and the DFE's guidance surrounding AI (Generative artificial intelligence (AI) in education - GOV.UK (www.gov.uk)) .
    - As the use of AI is in its infancy, the use and abilities will be continually changing. Use must not involve the sharing of any personal data of pupils, their families or staff members.
    - For further guidance on the use of AI, please speak to a member of the SLT.

Policy Links

This policy is to be read in conjunction with the following other policies and documents:

- Mobile Phone Policy
- Online Safety Policy
- Social Media Policy
- Safeguarding and Child Protection Policy

I have read and understood and agree to comply with the Staff Acceptable Use Policy, Mobile Phones Policy, the Online Safety Policy and the Social Media Policy.

Signed:_____ Print Name:_____ Date:_____

Alderman Richard Hallam Primary School 2024

Policy review date: September 2025