Key Points of our Acceptable Use Policy for Adults

Moat Hall Primary School has provided computers for use by staff as an important tool for teaching, learning and administration of the school. Use of school computers, by both members of staff and pupils, is governed at all times by the following policy. Please ensure that you understand your responsibilities under this policy, and direct any questions or concerns to the ICT Network Manager (Kesar Singh) in the first instance.

The purpose of the policy is to ensure the school network is operated safely and all users of ICT are safe. It refers to our school ICT network and to the use of mobile technologies within it and explains the behaviours, which are acceptable and unacceptable within our school.

This document outlines the key points of our AUP. It has been written to ensure all adults working within school are aware of the rules, risks and procedures we operate under our full AUP, which is located on our ICT system.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Our AUP must be fully complied with at all times. All users of the school network should note that it is monitored on a regular basis. Any person who is found to have misused the school system or not followed our AUP could face the following consequences:

- Temporary or permanent withdrawal from the school system
- Suspension or exclusion from the school
- Disciplinary action
- In the most serious cases legal action may also be taken.

Whilst our network and systems are organised to maintain the most secure environment possible **it is your responsibility to make sure the children you are directly working with are safe**. All adults working in school must do so under the guidance of the member of staff to whom they are responsible.

As an adult working in school you may be the first point of contact in dealing with incidents of ICT misuse or abuse. Every such incident must be reported to the Class Teacher who will then follow the procedures set out in our AUP.

Your key responsibilities are:

- Maintaining an appropriate level of professional conduct in your own internet use within school.
- Developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children.
- Implementing our school AUP through effective classroom practice.
- Reporting any instances of ICT misuse to the Class Teacher who must report it to the E-Safety Coordinator (Anna Thompson) in line with our school AUP. If the Class Teacher is suspected of being involved, report directly to the E-Safety Coordinator or Head Teacher.
- Supporting pupils who experience problems when using the internet, working with the Class Teacher.

- Using the internet and ICT facilities to ensure that internet safety is not compromised e.g. evaluating websites in advance of classroom use, using chid oriented search engines.
- Embedding internet safety messages wherever possible.
- Following the school rules relating to acceptable use of our ICT equipment and other mobile technologies.

School ICT Network

The school Network and associated services may be used for lawful purposes only.

Passwords

- Each child and adult working within the school must log on to the computers using the username and password given to them (class account or individual account). Passwords need to be kept a secret. If for any reason a child or adult needs to leave their computer, they have to lock the computer to prevent others from using their account by pressing 'Ctrl, Alt and Delete'.
- It is forbidden to use other children's/adult's/class accounts or files. Both adults and children will respect copyright and not copy anyone's work and call it their own.
  For the children in our school who are unable to understand the 'Pupils Acceptable Usage Policy' and for the children who are unable to log in and log off using their own password, the adult(s) working with those children will take full responsibility for their safe internet use in school.
- Any supply teachers or visitors to the school must see our ICT Technician to obtain a guest account and password.

Software and Downloads

- All users of the network must virus check any USB device storage devices before using on the network. All mobile devices must be encrypted with software to comply with GDPR. All users are prohibited from installing software onto the network without permission from the ICT Technician. If users need a new program installing onto the computer, our ICT Technician will be asked to do this if possible.
- Copyright and intellectual property rights must be respected when downloading from the internet.

Personal Use

The school recognises that occasional personal use of the school's computer is beneficial both to the development of ICT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

- Most comply with all other conditions of the AUP as they apply to non-personal use, and all other school policies regarding staff conduct.
- Must not interfere in any way with your other duties or those of any other member of staff.
- Must not have any undue effect on the performance of the computer system; and
- Must not be for any commercial purpose or gain unless explicitly authorised by the school.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

Email

- All members of staff with a computer account in school are provided with a school email address for communication both internally and with other email users outside of school.
- No member of staff (including governors and non-teaching staff) must use non-school email accounts for any school/work related activity – no exceptions!

- Users are responsible for e-mail they send and should be aware that these are open to be read and should be treated as public.
- E-mail should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety.
- When writing emails, you should use appropriate language. You should not use language that could be calculated to incite hatred against ethnic, religious or other minority. You need to remember that you are a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- All emails both sent and received will be scanned by forensic software.
- E-mail attachments should only be opened if the source is known and trusted.
- Children are not permitted under any circumstances to e-mail a member of staff using their personal e-mail address. In addition, members of staff should not be emailing children using their personal email address.
- Privacy – I will not reveal any personal information (e.g. name, address, age, telephone number, social network details) of other users to any unauthorised person. I will not reveal any of my personal information to the pupils.
- I will not trespass into other users' files or folders.
- I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users. I will ensure that if I think someone has learned my password then I will change it immediately and/or contact ICT technician.
- I will ensure that I log off after my session has finished. If I find an unattended machine logged on under another username I will not continue using the machine – I will log it off immediately.
- Any unsuitable communications received must be reported to a member of staff immediately.

Images/Videos

- All children need parental permission to have photographs or videos published electronically or in a public area even if they are unidentifiable.
- No photos or videos which include nudity or inappropriate actions are permitted to be taken or downloaded under any circumstance.

Network Protocol

- School computer and Internet use must be appropriate to a pupil's education or to staff professional activity.
- Respect other people's material and do not corrupt, interfere with or destroy them.
- Do not open other people's files without expressed permission.
- When working with personal data ensure that the data is secure.

Internet Usage

- Pupils must be supervised at all times when using the internet.
- Activities should be planned so 'open searching is kept to a minimum. The facility for caching sites should be used prior to using the internet with pupils.
- When searching the internet with pupils, adults should encourage the children to use 'child safe' search engines. However safe search is set on all computers in school as a default on search engines.
- The use of social networking sites, public chat rooms and messaging systems (e.g. Facebook, Messenger, Twitter) is not allowed in school.

- Use the internet for personal financial gain, gambling, political purposes or advertising is forbidden.
- I will not attempt to visit websites that may be considered inappropriate or illegal. I am aware that downloading some material is illegal and that the police or other authorities may be called to investigate.

Use of Social Networking Sites and Online Forums

Staff must take care when using websites such as Facebook, Twitter, Dating Sites etc, even when such use occurs in their own time their own computer at home. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You must not allow any pupil to access personal information you post on a social networking site. In particular:

- You must not add a pupil to your 'friends list', nor invite them to be friends with you.
- You must ensure that personal information is not accessible via 'Public' setting, but ensure it is to a 'Friends only' level of visibility.
- You should avoid contacting any pupil privately via social networking site, even for school-related purposes.
- You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them to access to your personal information.

It is advised not to accept invitations from the pupils' parents or careers to add me as a friend to their social networking sites, nor should you invite them to be your friends. As damage to professional reputations can inadvertently be caused by quite innocent postings or images. You will need to ensure that any private social networking sites/blogs that you create or actively contribute to are not to be confused with your professional role in anyway.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, you must not post comments on websites that may appear as if you are speaking for the school.
- You should not post any material online that can be clearly linked to the school that may damage the school's reputation.
- You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass or defame the subject.

Use of your own Equipment

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and must not be used until approved. This test must be performed at regular intervals as required by school's normal rules on electrical safety testing.
- You must not connect personal computer equipment to school computer equipment without prior approval from ICT Technician, without the exception of encrypted storage devices such as USB memory sticks.

Mobile Devices

(See mobile phone policy for further guidance and information)

- Personal mobile phones should not be used in areas of school where pupils have access.
- During teaching time, mobile phones should be turned off or put on silent mode and stored in teachers' personal lockers away from the children.
- Adults are allowed to access their personal phones on breaks, lunch times and after school in designated areas e.g. staff room (safe, suitable places where the children are not present).
- It is forbidden to take photographs/videos of the children on personal mobile phones.
- No images of the children should be taken without parental consent and permission from a member of staff using any mobile device e.g. phones, school cameras. These devices must not be removed from the school premises if they contain images of pupils and without permission from a member of staff.

Supervision of Pupil Use

- Pupils must be supervised at all times when using school computer equipment. Supervising staff needs to ensure that pupils have signed the class computer log and if the pupils are unable to sign the log book they are responsible for doing it for them. When arranging use of computer facilities for pupils, you must ensure supervision is available.
- Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.
- Supervising staff must ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils.

Reporting Problems with the Computer System

It is the job of the ICT Network Manager to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible.

- You should report any problems that need attention to ICT Technician.
- If you suspect your computer has been affected by a virus or other malware, you must report this to ICT Technician immediately.
- If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the less chances of your data being recoverable.

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform the ICT Technician or the Head Teacher, of abuse of any part of the computer system. In particular, you should report:

- Any websites accessible from within school that you feel are unsuitable for staff or pupil consumption.
- Any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc.
- Any breaches, or attempted breaches, of computer security, or
- Any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school computer system.

All reports will be treated confidentially.

Electronic Devices - Searching & Deletion

In accordance to 'The Education Act 2012' school has the right to search and or delete anything from personal devices if they believe illegal or suspicious activity is taken place.

Exemptions
All the above stands unless given permission from the Head Teacher e.g. while on residential trips, permission may be given to designated staff to upload photos onto our Springwell School Facebook or Twitter account.

Review and Evaluation
This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.
Our Acceptable Use Policy (AUP) has been created by our school governors and senior managers and approved by the whole school community.

I have read, understood and agree to comply with the AUP:

Signed: _____ Date: _____

Print Name: _____

Position in School: _____