Acceptable Use Policy for Staff, Governors and Volunteers including school password security

To be reviewed Bi-Annually.
Policy Agreed September 2018. To be reviewed September 2020

Everton Nursery School and Family Centre

Varying forms of new technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet as well as other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They can also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe Internet access at all times.

This Acceptable Use Policy is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the Internet and other communication technologies for educational, personal and recreational use;
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- Staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for children's learning and will, in return, expect that staff and volunteers agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that all children receive opportunities to gain from the use of ICT. I will where possible educate the young people in my care in the safe use of ICT and embed online safety in my work with all children.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school.

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and/or password unless approved by the Headteacher.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.

Password Security

The management of the password security will be the responsibility of the Network Manager. All staff will have responsibility for the security of their username and password and MUST NOT allow other staff to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new staff and replacement passwords for existing staff will be allocated by the Network Manager. Any changes carried out must be notified to the manager.

Staff passwords:

- should be changed at least every 60 days
- are not re-used for 1 year
- are significantly different from previous passwords created by the same member of staff
- should be a minimum of 8 characters long and include an uppercase character, lowercase character, number and special character
- should not be written down or printed or displayed on screens

Temporary passwords issued to new staff or staff who have forgotten their password will be requested to change immediately upon the next account log-on. Requests for password changed will be authenticated by the Network Manager to ensure that the new password can only be passed to the genuine staff member. The administrator passwords for the school IT system used by the Network Manager are also available to the Headteacher.

Staff are made aware of the password procedure through induction and training.

Monitoring – The Network Manager will ensure records are kept of user ids and requests for password changes and any security incidents. These will be shared with the Headteacher and Governors.

I will be professional in my communications and actions when using school ICT systems:

- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others, I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (e.g. on the school website), it will not be possible to identify by name or other personal information those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with children and parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use.
- I will not open any attachments to emails unless the source is known and trusted due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials, which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will only install software or apps deemed appropriate for the classroom or office use and will review the use of all apps before using in the classroom.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will report any damage or faults involving equipment or software, however this may have happened.

When using the Internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Security and CCTV Equipment

- Everton Nursery School and Family Centre uses CCTV cameras for security purposes and to ensure the safety and welfare of all staff, visitors, children and their families when visiting the setting.
- Cameras are installed in various locations throughout the setting both inside and outside the building.
- All images taken on the CCTV cameras comply with the Data Protection Act and guidance issued by Merseyside Police Authority. Images are stored on the Centre's/School's hard drive for a maximum period of 31 days and then are automatically recorded over. Access to the hard drive is restricted and images are only transferred to CD if needed as evidence.
- Staff will ensure that security systems are maintained and in operation at all times. Where key fob access is required or passwords or security keys are given to staff, staff members will ensure that they are not shared with any other person unless specifically instructed otherwise by a member of the SLT.

<u>Policy review</u>

This policy was reviewed by the Children, Family and Curriculum Committee on Tuesday 2nd October 2018. This policy was ratified by the full Governing Body on Thursday 11th October 2018.

This policy will be reviewed bi-annually or earlier in response to changes in guidance.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the Police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer / Governor

Name _____

Signed _____

Date _____