‘Achieving excellence fulfilling potential’

Millbrook Primary School

Computing Systems Policy

‘Achieving excellence fulfilling potential’

Agreed – March 2023
To be reviewed – March 2025

‘Achieving excellence fulfilling potential’

COMPUTING SYSTEMS POLICY

1 Policy Statement

1.1 This IT and communications systems policy is intended to promote effective communication and working practices within Millbrook Primary School. This policy outlines the standards employees and pupils must observe when using these systems, the circumstances in which Millbrook Primary School will monitor their use, and the action which will be taken in respect of any breaches of these standards.

1.2 All employees and pupils are representatives of Millbrook Primary School and the LACT academy trust and all communication through the school’s systems (whether by telephone, e-mail or otherwise), must be conducted in an appropriate manner.

2 Who is covered by the Policy?

2.1 This systems policy is to cover all members of staff, pupils and visitors to the site of Millbrook Primary School including senior managers, officers, directors, employees, consultants, contractors, trainees, home-workers, part-time and fixed-term employees, casual and agency staff [and volunteers] (collectively referred to as staff).

2.2 Any visitors to the school should adhere to and follow the guidelines set out in this policy in relation to the IT and communication systems within and in relation to Millbrook Primary school and the LACT academy trust. Showing their understanding by signing and agreeing to the acceptable use agreements.

3 The Scope of the Policy

3.1 This policy deals mainly with the use (and misuse) of any computer related equipment such as, e-mail, the internet, telephones (including mobile and other smart-phones), personal digital assistants (PDAs), iPads, personal computers and voicemail. It also applies to the use of photocopiers, scanners, CCTV, and electronic entrance systems (such as the door entry system).

3.2 Any breach of this policy may be dealt with under a Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

4 Who Is Responsible For This Policy?

4.1 This policy has been written by the Computing curriculum lead and will be reviewed and checked by the governing body of Millbrook Primary school at set intervals with revisions being made as the use of technology changes over time.

4.2 Any misuse of the electronic communications systems or equipment linked to the school or LACT academy trust should be reported to a member of SLT as soon as possible. If involving a safeguarding issue the safeguarding policy should be followed and a report made as soon as possible using CPOMS.

5 Equipment Security and Passwords

5.1 Staff are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than in accordance with this policy. If leaving their device unattended or on leaving the classroom/school you should ensure that any device (classroom computer, staff iPad) is locked or logged off to prevent unauthorised users accessing the system in their absence.

5.2 Staff passwords should be unique to each user and must be changed regularly to ensure confidentiality. Passwords must be kept confidential and must not be made available to anyone else unless authorised by the computing lead. Two factor authentication should be used where possible to protect sensitive information that maybe stored on mobile devices and web-based applications such as email (Office 365).

5.3 Staff and Pupils should not move or tamper with desktop PCs, computer suite PCs or cabling for the telephones or computer equipment to avoid unnecessary damage.

5.4 If you have been issued with a laptop and/or iPad, you must ensure it is kept secure at all times especially when travelling. Before devices are allowed to be removed from site you must complete the relevant paperwork and return it to the Site Manager/Business manager. When using the devices off site only access safe and secure connections in order to lower the risk of unwanted programs being able to access the device.

6 Systems and Data Security

6.1 It is both staff and pupil’s responsibility to ensure they **do not** delete, destroy or modify existing systems, programs, information or data which could have the effect of harming the school and/or exposing it to risk.

6.2 Staff and pupils should not download or install software from any external sources without first obtaining authorisation from either the computing lead or the IT technician. Key software for all members of staff and pupils will be installed through the central server by requests, from members of staff, made to the IT technician through the computing issues logbook located in the staffroom. Apps will be installed through the central management system upon request to the IT Technician or Computing lead.

6.3 Any websites which are not to be accessed by both staff and pupils within the school system will be filtered through the current filter system (EXA filtering system and internet service provider). This system will be updated as websites are identified as inappropriate or appropriate to be allowed or blocked through the system by either the IT technician or the computing lead.

6.4 While on site access to social media sites such as Facebook, instagram, Twitter, and other social media sites will be blocked for pupil devices through the filter system to prevent access to unwanted material. (School social media accounts will only be accessible via staff devices.)

6.5 Personal devices used within school to access school systems are done so by prior permission from the computing lead and those using said devices should do so adhering to this policy on access of materials including the use of social media such as instagram, facebook etc. The only exception is the use of school social media accounts which are accessed through the staff school/personal devices where appropriate (SLT Computing Lead).

7 E-mail Etiquette and Contents

7.1 All staff will have access to a work based email account which is linked to the school through the address of @millbrook.swindon.sch.uk. As a result it is important that all emails sent and received through this email address are of a professional type, as to uphold the ethos and outside view of the school and academy trust.

7.2 When using the school email system (Office 365) all staff are required to check their emails do not contain chain mail, cartons, jokes or gossip which can be seen as inappropriate for the workplace. If any are received this is to be reported to SLT/IT technician or Computing Lead and not passed on to any other members of staff.

7.3 Any material being passed through emails must follow the copyright protection laws, especially when passing on music files and or images taken from the internet or other downloadable materials.

7.4 When composing emails to fellow professionals remember all staff are representing the school and the schools views on different points. All emails composed should follow these simple tips to show professionalism.

(a) ***Short subject lines which are correctly spelt and informative, keep formality and courtesy levels high until the relationship between the recipients dictates otherwise.***

(b) ***Choose when to use BCc and Cc to fit the situation (BCc should be used when copying professionals in to a group where they do not know each other).***

(c) ***Use only the reply all if and when everyone needs to know your response, if this is not the case, you should remove the contacts that are not required to see your response.***

(d) ***When using attachments, check whether it is useful to them and will not clutter their inbox. Always check that the contact has the same software and are able to receive a large file e.g. a PowerPoint presentation.***

8 Use of the Internet

8.1 The use of the internet is a wide resource, which is used on a regular bases within school, however staff and pupils should always be aware of the extent they are using the internet and the searches and uses which are being made on the school system. As mentioned previously the school’s filtering system (Currently EXA education) will be used to block any potentially harmful and inappropriate material from appearing on the system. Staff and pupils therefore are responsible for the search words and phrases which are used while using the school internet system. No member of the school community (staff, pupil, visitor, parent, governor) should be having access to any web page or any files (whether documents, images or other) downloaded from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral. Any such material found on the school system should be reported to a member of the SLT (Senior Leadership Team) and/or the safeguarding team.

8.2 The school’s computing systems should not be used by any staff to access sites which involve internet chat rooms, message boards, blogs or wiki documents. Unless linked to the schools approved platforms, such as purple mash and TT Rockstars. The above sites have these activities locked down to the groups/communities which have been allowed by the Computing lead and class teachers.

8.3 Staff should not be accessing personal chat rooms such as internet dating sites or inappropriate communication tools even in their own time such as break times, lunch times and after school times while on site.

9 Personal Use of Systems

9.1 Staff are permitted to use school based systems for personal use such as checking personal emails, browse the internet and make personal telephone calls, only when it does not affect their professional duties e.g. only when not working with children such as break, lunch and off duty times. When working in class personal emails, phone calls and browsing of the internet should not be taking place.

9.2 Personal use of the schools computing systems may be monitored and, where breaches of this policy are found, action may be taken under the disciplinary procedure.

9.3 Whenever personal use of equipment including the use of technology, such as tablets, laptops, cameras etc, is taking place staff must act in a professional manner at all times, maintaining the ethos and point of view of the school for example while out on school trips- cameras on mobile devices can be used with prior agreement from SLT and or Computing lead and images uploaded via foldr at the earliest possible opportunity and removed from the personal device.

10 Monitoring of Use of Systems

10.1 The use of systems within the school will be monitored using the EXA monitoring system with regular reports on usage of the internet and websites used during set periods.

10.2 The use of the photocopier is monitored on a regular basis with a report produced at the end of every waste toner collection pot. Numbers of copies made are checked regularly to ensure reasonable use is taking place.

10.3 The use of school IPADs will be monitored and managed using the MDM service provided by the online software by Meraki.

10.4 At Millbrook Primary School there is CCTV in operation around the exterior of the building which is checked on a regular basis by the site team.

11 Inappropriate Use of Equipment and Systems

11.1 Staff and pupils should be made aware of any misuse of school equipment such as the telephone or e-mail system, or inappropriate use of the internet in breach of this policy will be dealt with in accordance with a Disciplinary Procedure and that serious cases of deliberate discrimination may amount to gross misconduct resulting in dismissal.

11.2 Examples of inappropriate use of Equipment and systems can include:

- Use of the schools internet connection to access websites and or apps which are connected to social media e.g. Instagram, Snapchat, and Facebook during work hours unless during break, lunch or off duty times away from children and while using the school social media accounts.
- Personal uses such as banking, emailing, phone calls during the school day, apart from during off duty times such as lunch and break times.
- Accessing websites with inappropriate material e.g. pornography, racist views etc

12 Outside of school use of social media (impact on school)

12.1 Pupils are not permitted to use any form of social media while on site at Millbrook Primary School as this will break the acceptable use agreement and safeguarding procedures currently in place on site.

12.2 Millbrook primary school, including pupils or staff, should not be mentioned on any social media accounts accept the approved school social media accounts (Facebook, Instagram and Twitter). Any mentions of staff or pupils relating to Millbrook Primary will be reported to a member of SLT and dealt with following the appropriate disciplinary policy.

12.3 Staff should remember that any use of social media outside of school has an impact on their professional appearance. As a result staff should use the thought of ‘If I would place it on my desk for all to see, then it can be posted online’.

12.4 Staff will be trained and updated on how to maintain their security and their professional online profile on a regular bases through staff meetings and regular safe internet practices updates sent out through email.

12. 5 Staff should check and review their security settings regularly to ensure they are secure and personal data is not accessible to anyone other than trusted contacts.

12.6 Staff should not be accepting or sending friend/follower requests from present pupils or parents in order to maintain a professional relationship with the pupils and/or parents.

12.7 Pupils will be taught through the schools computing curriculum and curriculum policy to understand their use of any form of social media and public posts.

12. 8 Any pupils found to be using social media outside of school, which is to have an impact on the school or other pupils within the school, will be reported to a member of the SLT and parents of pupils involved will be informed of any misuse.

Reporting of issues:

All issues/incidents should be recorded using the Millbrook Primary school incident report log form and given to either the head teacher or computing lead.

Agreed – March 2023
To be reviewed – March 2025