Mulberry
Academy Woodside

White Hart Lane
Wood Green
London N22 5QJ
T 020 8889 6761

mail@mulberrywoodside.org
www.mulberrywoodside.org

Headteacher: Ms Angela Wallace BA Hons, PGCE, MA

IT Acceptable Use Policy

Created: March 2018
Reviewed: September 2020 by Mark Reid
Next Review: November 2023

HoD = Head of Department
HoY = Head of Year
SLT = Senior Leadership Team
SEN = Special Educational Needs

Important terms used in this document:

(a) *The abbreviation 'IT' in this document refers to the term 'Information Technologies.*
(b) *'Cybersafety' refers to the safe and responsible use of the Internet and IT equipment/devices, including mobile phones*
(c) *'School IT' refers to the school's computer network, Internet access facilities, computers, and any other school IT equipment/devices as outlined in (d) below*
(d) *The term 'IT equipment/devices' used in this document, includes but is not limited to, computers (such as desktops, laptops, tablets, PDAs, smart devices), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), Social Media Accounts, Gaming Consoles, and any other, similar, technologies as they come into use.*

Introduction

This policy sets out the requirements with which you must comply when using the School's email and Internet services including the use of mobile technology on School premises or otherwise in the course of your employment (including 3G / 4G / 5G technologies) whether on a School or personal device. This policy also applies to the use of email and Internet services off school premises if the use involves any member of the School community or where the culture or reputation of the School are put at risk. Failure to comply will constitute a disciplinary offence and will be dealt with under the School's disciplinary procedure.

Property

You should treat any property belonging to the School with respect and reasonable care and report any faults or breakages immediately to the Business Manager. You should not use the School's computers unless you are competent to do so and should ask for training if you need it.

Viruses
You should be aware of the potential damage caused by computer viruses. You must not introduce or operate any programs or data (including computer games) or open suspicious emails without permission from your line manager or IT technicians,

Passwords
Passwords protect the School's network and computer system. They should not be obvious, for example, a family name or birthdays, and should be a mix of uppercase and lowercase, numbers, and special characters (e.g. #, &, !). You should not let anyone else know your password. If you believe that someone knows your password you must change it immediately. Passwords should be changed regularly (for example every month) and your updated password should not be similar to the previous one (for example do not change your password by just adding a number each time, e.g. orchard', orcharc12., orchard3, etc). You should not attempt to gain unauthorised access to anyone else's computer or to confidential information which you are not authorised to access.

Leaving workstations
If you leave your workstation unattended you should take appropriate action and, in particular, you should lock your screen to prevent access.

Concerns
You have a duty of care to report any concerns about the use of IT at the school to the Headteacher. For example, if you have a concern about IT security or pupils accessing inappropriate material.

Internet Downloading
Downloading of any program or file which is not specifically related to your job is strictly prohibited.

Personal use
The School permits the incidental use of the Internet so long as it is kept to a minimum and takes place substantially outside of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the School discovers that excessive periods of time have been spent on the internet provided by the School or it has been used for inappropriate purposes either in or outside working hours, disciplinary action may be taken and Internet access may be withdrawn without notice at the discretion of the Headteacher.

Unsuitable material
Viewing, retrieving, or downloading of pornographic, terrorist or extremist material, or any other material which the School believes is unsuitable is strictly prohibited and constitutes gross misconduct. This includes such use at any time on the School's network, or via 3G, 4G or 5G when on School premises or otherwise in the course of your employment and whether or not on a School or personal device. Internet access may be withdrawn without notice at the discretion of the Headteacher whilst allegations of unsuitable use are investigated by the School.

Location services
The use of location services represents a risk to the personal safety of those within the School community, the School's security, and its reputation. The use of any website or application, whether on a School or personal device, with the capability of publicly identifying the user's location while on School premises or otherwise in the course of employment is strictly prohibited at all times.

Contracts
You are not permitted to enter into any contract or subscription on the Internet on behalf of the School, without specific permission from the Head Teacher.

Retention periods
The School keeps a record of staff browsing histories for a legal period of 6 months. Subject to any associated or pending investigations.

Email Personal use
The School permits the incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially outside of normal working hours. Personal emails should be labelled "personal" in the subject header. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. The School may monitor your use of the email system, please see paragraphs 22 and 23 below, and staff should advise those they communicate with that such emails may be monitored. If the School discovers that you have breached these requirements, disciplinary action may be taken

Status
An email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. You should not include anything in an email which is not appropriate to be published generally.

Inappropriate use
Any email message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation, or religious belief (or otherwise contrary to our equal opportunities policy), or defamatory is not permitted. The use of the email system in this way constitutes gross misconduct. The School will take no responsibility for any offence caused by you as a result of downloading, viewing, or forwarding inappropriate emails.

Legal proceedings
You should be aware that emails are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a backup system or other storage areas.

Jokes
Trivial messages and jokes should not be sent or forwarded to the email system. They could cause the School's IT system to suffer delays and or damage.

Contracts
Contractual commitments via email correspondence are not allowed without prior authorisation of the Head Teacher.

Disclaimer
All correspondence by email should contain the School's disclaimer.

Data protection disclosures
Subject to some limited exceptions, potentially all information about an individual may be disclosed should that individual make a subject access request under the General Data Protection Regulation (GDPR). There is no exemption for embarrassing information (for example, an exchange of e-mails containing gossip about the individual will usually be disclosable). As such staff must be aware that anything they put in an email is potentially disclosable.

Monitoring
Staff will need to acknowledge and agree that the School regularly monitors and accesses the School IT system for purposes connected with the operation of the School. The School also uses software that automatically monitors the School IT system (for example, it would raise an alert if a member of Staff visited a blocked website or sent an email containing an inappropriate word or phrase). The School IT system includes any hardware, software, email account, computer, device, or telephone provided by

the School or used for School business. The School may also monitor staff use of the School telephone system and voicemail messages. The purposes of such monitoring and accessing include:

- To help the School with its day-to-day operations. For example, if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent smalls are received; and
- To check staff compliance with the School's policies and procedures and to help the School fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.

The monitoring is carried out by the Business Manager. If anything of concern is revealed as a result of such monitoring then this information may be shared with the Head Teacher and this may result in disciplinary action. In exceptional circumstances, concerns may need to be referred to external agencies such as the Police.

Other Policies

This policy should be read alongside the following:

- Code of Conduct;
- Data protection policy for Staff;
- Information security policy;
- Social Media Policy;
- Acceptable use policy for pupils.