John Scurr Primary School
Cephas Street
London E1 4AX
Tel: 0207 7903647

Email: admin@johnscurr.towerhamlets.sch.uk
web: www.johnscurr.towerhamlets.sch.uk
Headteacher: **Ms Maria Lewington**

IT ACCEPTABLE USE POLICY

Reviewed by:	Leadership & Governing Body
Date:	20/10/2022
Review dates:	18th June 2007 amended 21st September 2011, reviewed November 2012, reviewed February 2014, reviewed February 2015, reviewed October 2016, reviewed Nov 2021
Next Review	01/09/2023
Ratified by Governors:	
Governor Signature: Headteacher Signature:	

Important terms used in this document:

1. The abbreviation 'IT' in this document refers to the term 'Information Technologies.
2. 'Cybersafety' refers to the safe and responsible use of the Internet and IT equipment/devices, including mobile phones
3. '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
4. 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.
5. 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 that can be caused by computer viruses.

You must not introduce or operate any programmes or data (including computer games) or open suspicious email s 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.

If you update your password, it should not be similar to the previous one (forexample 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/account 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.

If this is a shared machine like aclassroom, please log off rather than locking the machine to allow the next user to use theroom.

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 programme 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 out of normal working hours.

Personal 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 minimum 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 out 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 andnot 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.

Theuse 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 back-up 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, and 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 memberof staff is on holiday or is off sick, their email account may be monitored incase any urgent emails 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.

The School's IT Team do not and will not have the ability to view users' contents unless being instructed by Head Teacher and/or School Business Manager for investigative purpose. 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.

Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. email, Internet, network resources,

software, communication tools, equipment and systems.

John Scurr Primary regularly reviews and updates all AUA documents to ensure that they are consistent with the

school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected

and monitored by security and filtering services to provide safe access to digital technologies.

1. I will only use the school's digital technology resources and systems for Professional purposes or for

uses deemed 'reasonable' by the Head and Governing Body.

2. I will not reveal my password(s) to anyone.

3. I will follow 'good practice' advice in the creation and use of my password and change my

passwords regularly. If my password is compromised, I will ensure I change it. I will not use anyone

else's password if they reveal it to me and will advise them to change it.

4. I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school

systems, or any Local Authority (LA) system I have access to.

5. I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in

accordance with the school's network and data security protocols.

6. I will not engage in any online activity that may compromise my professional responsibilities.

7. I will not post about the school, my colleagues, or my work at the school on social media.

8. I will only use the approved email system(s) for any school business.

This is currently: LGfL StaffMail

9. I will only use the approved email system with pupils or parents/carers, and only communicate with

them on appropriate school business.

10. I will not support or promote extremist organisations, messages or individuals.

11. I will not give a voice or opportunity to extremist visitors with extremist views.

12. I will not browse, download or send material that is considered offensive or of an extremist nature by

the school.

13. I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the School Business Manager.

14. I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.

15. I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

16. I will not connect any device (including USB flash drive), to the network that does not have up-todate anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus and other ICT 'defence' systems.

17. I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.

18. I will follow the school's policy on use of mobile phones / devices at school and will only use them in staff areas at appropriate times.

19. I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system within school.

20. I will only I take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc., will not identify students by name, or other personal information.

21. I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.

22. I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.

23. I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.

24. I will not be online friends with any pupil/student, or any ex-student under the age of 18. Any exceptions must be agreed with the Head Teacher.

25. I agree and accept that any computer, iPad or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

26. I will only access school resources remotely (such as from home) using the LGfL / school approved system and follow e-security protocols to interact with them.

27. I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

28. I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

29. I will alert Maria Lewington if I feel the behaviour of any child may be a cause for concern.

30. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to Maria Lewington.

31. I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request.

32. I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.

33. I will only use any LA system I have access to in accordance with their policies.

34. Staff that have a teaching role only: I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

Acceptable Use Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature .....Date .....

Full Name ..... (printed)

Job title / Role .....

Authorised Signature (Head Teacher / SBM)

I approve this user to be set-up on the school systems relevant to their role

Signature ..... Date.....

Full Name ..... (printed)