MARLBOROUGH PRIMARY SCHOOL
ACCEPTABLE USER POLICY
POLICY FOR STAFF
MARCH 2018

Date of Policy Review:	Reviewer:	Date Ratified by Governors:	Date Shared with Staff:	Date of Next Review:
March 2018	M.Leon	N/A	March 2018	March 2019

Article 28: *Children have a right to a good quality education*
Article 29: *Children have the right to an education which develops their interests, talents and abilities*

Rights Respecting Schools
As a Rights-Respecting School, we use children's rights to underpin everything we do and learn. Marlborough Primary School has been working closely with UNICEF, and is a 'Rights Respecting' School. The term is bestowed on those schools who, in the eyes of UNICEF, put the 'UN Convention on the Rights of the Child', (UNCRC) at the heart of their planning, policies, practice and ethos.

UNCRC is a list of rights that all children, everywhere in the world, have. The rights are all the things that children and young people need to make sure they are healthy, happy and safe. A rights-respecting school not only teaches about children's rights, but also models rights and respect in all its relationships: between adults and children, between children themselves, and between adults themselves.

Data Protection Statement
The procedures and practice created by this policy have been reviewed in the light of our Data Protection Policy. All data will be handled in accordance with the school's Data Protection Policy.

Data Audit for this Policy					
What?	**Probable Content**	**Why?**	**Who?**	**Where?**	**When?**
Acceptable User Policy	User names Full names Signature/	Accessing ICT equipment	All staff where appropriate	Paper Copy of AUP is kept on file. These are kept securely locked away.	Held on File Throughout member of Staff's Time at School and archived thereafter.

As such, our assessment is that this policy:

Has Few / No Data Compliance Requirements	Has A Moderate Level of Data Compliance Requirements	Has a High Level of Data Compliance Requirements
✓		

Introduction:

This policy covers use of all digital technologies while in school: i.e. **email, internet, intranet, network resources,** learning platform, software, communication tools, social networking tools, school website, apps **and other relevant digital systems provided by the school or school Local Authority.**

Furthermore, it extends to the use of school equipment when used outside of school, use of online systems provided by the school or school umbrella body when accessed from outside school, and posts on social media made from outside school premises/hours which reference the school or which might bring your professional status into disrepute.

Marlborough Primary School regularly reviews and updates all AUP 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. Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may therefore be subject to monitoring.

- 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.

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

- 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.

- I will not allow unauthorised individuals to access email / internet / intranet / network / social networks / mobile apps / or any other system I have access to via the school or school umbrella.

- 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.

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

- I will only use the approved email system(s) for any school business. This is currently: *LGfL StaffMail*

- I will only use the approved method/s of communicating with pupils or parents/carers: *LondonMail* and only communicate with them in a professional manner and on appropriate school business.

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

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

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

- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Headteacher (Safeguarding) and Computing Technician (Micheal Jefford).

- 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.

- 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.

- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software and that is not sufficiently encrypted with a secure password. In addition, I will also ensure that I keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.

- 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.

- I will follow the school's policy on use of mobile phones / devices at school and will *only use in staff areas during breaktime and lunchtime unless I have prior consent from the Headteacher.*

- 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 staff-only drive within school*.

- 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.

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

- 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.

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

- I agree and accept that any computer 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.

- 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.

- 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.

- 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.

- I am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.

- 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 the Designated Safeguarding Lead (Mrs Daphne Byron)

- I understand that all internet and network usage can be logged and this information can be made available *to the Head*teacher and Designated Safeguarding Lead on their request.

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

- I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.

- *Staff that have a teaching role only:* I will embed the school's online 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 / Deputy)

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

Signature .... Date

Full Name .... (printed)