Lady Margaret Primary School

E-Safety Policy and Acceptable Use Agreement

Approved by:	Full Governing Body	**Date:**	9th September 2021
Last reviewed on:	August 2021		
Next review due by:	August 2023		

Contents

Contents 2
1. Introduction 4
2. Aims 5
3. Legislation and guidance 5
4. Roles and responsibilities 5
5. Educating pupils about online safety 8
6. Educating parents about online safety 8
7. Cyber-bullying 9
8. Acceptable use of the internet in school 10
9. Pupils using mobile devices in school 10
10. Parents/carers visitors using mobile devices in school 11
11. Staff using work devices outside school 11
13. How the school will respond to issues of misuse 12
14. Training 12
15. Monitoring arrangements 13
16. Links with other policies 13
Appendix 1: acceptable use agreement (pupils and parents/carers) 14
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors) 18
Appendix 3: online safety training needs – self-audit for staff 20
Appendix 4: online safety incident report log 21

……

This policy supports the **Rights Respecting principles** adopted by Lady Margaret Primary School and is particular relevant to the following articles:

UNICEF - Convention on the Rights of the Child (CRC)

Article 3

The best interests of the child must be a top priority in all things that affect children.

Article 5

Governments must respect the rights and responsibilities of parents and carers to direct and guide their children as they grow up, so that they can enjoy their rights properly.

Article 6

Every child has the right to life. Governments must do all they can to make sure that children survive and develop to their full potential.

Article 13

Every child must be free to say what they think and to seek and receive all kinds of information, as long as it is within the law.

Article 17

Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.

Article 34

Governments must protect children from sexual abuse and exploitation.

1. Introduction

1.1. Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment.

1.2. Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting (Audio Sharing)
- Video Sharing
- Music Sharing / Downloading
- Gaming
- Mobile / Smart phones with functionality including: text, video, web, audio, music , global positioning (GPS)
- Other mobile devices with similar functionality (tablets, laptops, gaming devices)

1.3. Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

1.4. Ensuring children and young people are aware of the risks associated with the use of technologies, and can adopt safer behaviours, is vital in safeguarding them against cyber-bullying grooming, extremism and radicalisation.

1.5. At Lady Margaret Primary we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to

remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

1.6. This policy relates to both fixed and mobile Internet technologies provided by the school, and technologies owned by pupils, parents and staff, but brought onto school premises.

2. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

3. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation.
- It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

4. Roles and responsibilities

4.1. The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is **Day Njovana**.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

4.2. The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

4.3. The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT support provider and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

4.4. The ICT support provider

The school's ICT support provider is **Azteq limited**

The ICT support provider is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

4.5. All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

4.6. Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf
- Healthy relationships – Disrespect Nobody: https://www.disrespectnobody.co.uk/

4.7. Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

5. Educating pupils about online safety

5.1. Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

6. Educating parents about online safety

6.1. The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment J2E. This policy will also be shared with parents at parent workshops.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7. Cyber-bullying

7.1. Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour and anti-bullying policy.)

7.2. Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

An E-safety lesson is taught discretely at the start of each new computing topic, usually once every half term, and teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying within other subjects. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7.3. Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

8. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

The school denies access to social networking sites to staff and pupils within school.

More information is set out in the acceptable use agreements in appendices 1 and 2.

9. Pupils using mobile devices in school

Pupils are not allowed to bring personal mobile devices/phones to school. If a phone is needed by a pupil, it must be handed in to reception staff in the morning and given back at the end of the day.

The school is not responsible for the loss, damage or theft of any personal mobile device.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

10. Parents/carers visitors using mobile devices in school

The school recognises that visitors may wish to have their personal mobile phones with them for use in case of emergency.

However, safeguarding of children within the school is paramount and it is recognised that personal mobile phones have the potential to be used inappropriately and therefore the school has implemented the following policy:

- Mobile devices must not be used at all in the EYFS.
- Mobile phones and cameras should only be used away from the children, off site or in our staff room.
- Photos of children at school events taken by parents/carers or visitors must not be shared on social media platforms.

In circumstances where there is a suspicion that the material on a mobile phone may be unsuitable and provide evidence relating to a criminal offence, the 'Allegations of Abuse' process will be followed. (Please refer to the 'Safeguarding and Child Protection Policy').

Visitors remain responsible for their own property and will bear the responsibility of any losses.

11. Staff using work devices outside school

Work devices must be used solely for work activities.

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

Any form of transfer containing data relating to the school must be encrypted and any documents containing personal information must be sent via secure platforms e.g. Egress if communicating with the local authority or other services.

If staff have any concerns over the security of their device, they must seek advice from the School Business Manager.

12. The use of removable media

There is an increased risk that uncontrolled and unmanaged removable media may be used to, deliberately or inadvertently introduce malicious software or inappropriately remove, hold or transfer data.

There have also been a series of personal data losses across a number of UK Government Departments in recent years.

The introduction of Microsoft Office 365 provides the facility to save and share files online via SharePoint, OneDrive or Microsoft Teams means that staff can access their files remotely from any device without the need to transfer data between devices using media storage devices.

Following the advice of the school's Data Protection Officer, staff are not permitted to introduce or use any USB memory stick other than those provided by the school.

Encrypted memory sticks will be provided at the sole discretion of the headteacher to staff whose roles may require them to transfer data for example to facilitate off-site training.

Those who have been authorised by the headteacher to use encrypted USB memory sticks for the purposes of their job roles are responsible for the secure use of those devices at all times.

13. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

14. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

15. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed annually by the school business manager. At every review, the policy will be shared with the governing board.

16. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Prevent Duty

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school's ICT systems and accessing the internet in school, I will not: o Use them for a non-educational purpose o Use them without a teacher being present, or without a teacher's permission o Access any inappropriate websites, social networking sites or chat rooms o Open any attachments in emails, or follow any links in emails, without first checking with a teacher o I will only open/delete my own files. o Use any inappropriate language when communicating online, including in emails o Share my password with others or log in to the school's network using someone else's details o Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer o Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision o If I bring a personal mobile phone or other personal electronic device into school I will hand it in to the school office before registration. o I will immediately: o let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. o tell a teacher straight away if something is broken or not working properly o Log off or shut down a computer when I have finished using it I understand that my parent/ carer will be contacted if a member of school staff is concerned about my e-Safety. **I will always use the school's ICT systems and internet responsibly.** **I agree that the school will monitor the websites I visit.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Dear Parent/ Carer

Re: Acceptable Use Agreement for pupils

Computing, including the Internet and mobile technologies, such as digital cameras and iPads has become an important part of learning in our school. We expect all children to be safe and responsible when using any digital technology.

Please be aware that your child/children should not be using social media sites such as Facebook, Instagram, Snapchat or WhatsApp, no one under the age of 13 is allowed to use these site and WhatsApp requires users to be 16 and over.

Please read and discuss these e-Safety rules with your child, then sign the slip below and return it to your child's class teacher. If you have any concerns or would like some explanation please contact the school at: office@ladymargaret.ealing.sch.uk and your query will be forwarded to our leader of learning for computing.

Yours faithfully,

Mrs H. Rai

Head teacher

✂----------

Name of child…….. Class…….

Acceptable Use Agreement for Pupils

We have discussed this and ……..(child name) agrees to follow the e-Safety rules and to support the safe use of ICT at Lady Margaret Primary School.

Parent/ Carer Signature …….

Child signature …… Date…….

Dear Parent/ Carer

Re: Acceptable Use Agreement for pupils

Computing, including the Internet, J2E, DB Primary and mobile technologies, such as digital cameras and iPads has become an important part of learning in our school. We expect all children to be safe and responsible when using any digital technology.

Please read and discuss these e-Safety rules with your child, then sign the slip below and return it to your child's class teacher. If you have any concerns or would like some explanation please contact the school at: office@ladymargaret.ealing.sch.uk and your query will be forwarded to our leader of learning for computing.

Yours faithfully,

Mrs H. Rai

Head teacher

✂----------

Name of child…….. Class……..

Acceptable Use Agreement for Pupils

We have discussed this and ……..(child name) agrees to follow the e-Safety rules and to support the safe use of ICT at Lady Margaret Primary School.

Parent/ Carer Signature ……

Child signature …… Date ……

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors
Name of staff member/governor/volunteer/visitor:
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature**. I understand that to do so may be considered a disciplinary matter, and in some cases a criminal offence.** • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Introduce or use any USB memory stick, key or flash drive other than those provided by the school. • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without first checking the school has parental consent. • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I agree that images & videos of pupils and / or staff will only be taken, stored on school equipment and will only be used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images & video will not be distributed outside the school network / MLE without the permission of the parent/ carer, member of staff or Head teacher.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

I will ensure that all electronic communications with pupils, parents and staff are compatible with my professional role, and never via personal email / phone accounts / social networking profiles.

I will not discuss school issues on social networking sites, for example Twitter or Facebook or on web-blogs.

I will not give out to pupils, my own personal contact details, such as mobile phone number and personal email address.

I will only use the approved, secure email system(s) and MLE tools for communications related to my professional role.

I am aware that communicating with students / pupils via private email / SMS and social networking sites may be considered a disciplinary matter.

I will respect copyright and intellectual property rights.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**