Learning and Motivation leads to Progress and Success

E-Safety Policy
And
Acceptable Use Agreement

Revised September 2016

Contents

Introduction

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.

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)

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.

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.

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.

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.

Roles and Responsibilities

The Head and governors have ultimate responsibility to ensure that this policy and its practices become embedded and are monitored. The named e-Safety co-ordinators in our school are ***Miss Nandra and Miss Koriya*** who have been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the co-ordinator to keep abreast of current issues and guidance through organisations such as Ealing LA, CEOP (Child Exploitation and Online Protection), UKCCIS, and Childnet.

Senior Management and Governors are updated by the Head teacher and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour / pupil discipline (including the anti-bullying) policy and particularly to the curricular for PHSE and SRE.

Skills / awareness development for staff

- New staff receive information on the school's acceptable use policy as part of their induction and all staff sign this on a yearly basis.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)
- All staff are expected to incorporate activities and awareness within the computing, PSHE and SRE curriculum areas.

Managing the school e-Safety messages

- **We endeavour to embed messages across the curriculum whenever the Internet and / or related technologies are used. This is particularly reinforced in Beliefs and values, PHSE Rights Respecting, and computing lessons in relation to cyber-bullying, extremism and radicalisation and to grooming.**
- The policy will be introduced to the pupils at the start of each school year.
- Posters will be prominently displayed in each classroom.

Computing in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for guidance to be given to the pupils on a regular and meaningful basis. E-safety guidance is embedded within our curriculum and we continually look for new opportunities to promote.

- The school uses the adapted version of the Switched On scheme of work as a guide which can be found in the 'applications' drive on the school network. All computing plans and resources are located in the Staff shared folder under Computing 2016-2017.
- The school provides opportunities within a range of curriculum areas to make sure the children reach the required objectives for the new computing curriculum at the end of each key stage.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or the 'whistle' button on DB Primary.
- PSHE and computing lessons provide the opportunity to discuss issues relating to cyber-bullying, Internet grooming and extremism and radicalisation. (e.g.: through respect for others and appropriate / positive relationships) these lessons can equip pupils with the knowledge to keep them safe from harm.

Pupil e-safety curriculum

Lady Margaret School has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on LA / LGfL e-safeguarding and e-literacy framework for EYFS to Y6/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- (for older pupils) to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;

- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- (for older pupils Year 6) to understand why and how some people will 'groom' young people for sexual reasons;
- To understand the impact of cyberbullying, extremism and radicalisation and know how to seek help if they are affected by any form of online bullying or grooming.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- To know how to report any images which are not appropriate in school or outside to school to a teacher.
- Plans internet use carefully to ensure that it is age-appropriate objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.

Tackling Extremism & Radicalisation

The Preventing Extremism and Radicalisation Policy links to the following Lady Margaret School policies:

- Child Protection and Safeguarding policy
- Equality Policy
- Anti-bullying Policy
- Positive Behaviour Management Policy
- Tackling Extremism & Radicalisation Policy

As part of wider safeguarding responsibilities staff will be alert to:

- Pupils accessing extremist material online, including through social networking sites
- Distributing extremist literature and documentation
- See Computing in the curriculum above for more details.
- See Preventing Extremism and Radicalisation Policy for more details

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others. Staff and pupils are regularly reminded of the need for password security.

- All users read ***and sign*** an Acceptable Use Agreement to demonstrate that they have understood the school's policy.
- Staff are provided with an individual network login, email and LGfL, SIMs, Sleuth usernames and passwords and assessment tracker passwords.
- Pupils in KS2 are provided with individual logins for the computers (which are the same as their LGfL usernames and passwords, which they are reminded to keep private. KS1 are provided with class logins and LGfL individual logins, these individual logins they are reminded to keep private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If a user thinks their password may have been compromised or someone else has become aware of their password they are expected to report this to their class teacher or Leaders of learning for Computing.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems (including Sims) and the Learning Platform, including ensuring that passwords are "strong", not shared, and are changed periodically. Individual staff users must also make sure that workstations are not left logged on when away from the computer for long periods of time.

- Staff must also NOT log onto computers for other staff or children to use as they have access to tools and data that is set to their specific user.

- Computers have been set to sleep mode after 30mins if the computer is inactive, staff/pupils then need to log back in, this gives added protection.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

- The schools data is backed up daily using an off-site solution, Gridstore, as recommended by LGfL.

Staff will:

- Not take any sensitive data off the school premises. Any work which needs to be completed off site will be done without any names or identifying features.
- Never save any personal information to their own computer / device. They will only save to school issued devices.
- Not leave the computer unattended while logged in remotely to school resources. Computers also have a sleep mode set up for 30mins.
- Never share passwords or leave on post-it notes etc.

Managing the Internet

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. In our school access to the Internet is via the London Grid for Learning. Internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- In our school students ***are not*** allowed unsupervised access to the Internet.
- Staff will preview any recommended sites before use with students.
- Raw image searches (e.g.: Google image search) are discouraged when working with pupils. The LGfL photo gallery is used in class **www.gallery.LGfL.net**
- If Internet research is set for homework, specific sites will be suggested. These will have been checked by the teacher. Where possible links from the school learning platform will be provided.
- It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- LGfL web filtering service has set up restricted access to YouTube, students do not have access to this site.

Infrastructure

- The London Grid for Learning (LGfL), provides, upon request, the facility to monitor and log web-based activity.
- School Internet access is controlled through the LGfL's web filtering service (WebScreen2).

- Lady Margaret Primary is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the Computer Leaders Miss Nandra and Miss Koriya. The offending URL will be reported to LGfL and / or the school technician.
- Sophos Anti-Virus protection is provided by the LGfL and is set to automatically update on all school machines. This is the responsibility of Trusol Ltd as per the contractual agreement for IT support.
- Pupils and staff are not permitted to download programs or files on school equipment without seeking prior permission from the technician.
- If there are any issues related to viruses or anti-virus software, the technical support company (Trusol) should be informed via the Trusol Helpdesk available on the school server.

Managing other Communication & Networking technologies

The Internet includes a wide range of communication and networking tools & sites. Children need to be educated about appropriate ways of communicating and about the risks of making personal information too easily available. if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- The school denies access to social networking sites to pupils within school. The school recommends children and parents to follow social networking age restrictions at home. These have been emphasised within the KS2 e-safety agreements.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are asked to report any incidents of bullying to the school.

- Pupils are introduced to a variety of Internet communication tools within the safe context of the school learning platform (DB Primary)
- Staff understand that it is highly inappropriate to use social networking sites and other personal communication tools to communicate with pupils and / or parents (e.g.: Facebook, Instagram, Twitter, email etc.). Staff are expected to use the tools within the school learning platform (DB Primary).
- Staff understand that it may considered a disciplinary offence if they mention on social networking sites; issues concerning students / parents / carers / other staff associated with the school.
- Teaching staff should not have parents as friends on their social networking sites and LSAs are strongly discouraged against this.
- All staff have been provided with a copy of the 'Appropriate use of ICT in schools' document which has been agreed by all the teaching unions as well as the Local Authority.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies (such as portable media players, gaming devices, Smart phones, etc.) are familiar to children outside of school. Allowing such personal devices to access the school network can provide immense benefits in collaboration, but also create risks associated with misuse, inappropriate communications, etc. Emerging technologies will be examined for educational benefit and the risk assessed before such use of personal devices is facilitated in school. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil using their personal device. However, in cases of emergency the Senior Leader can contact parents/ carers on a trip using their personal devices.
- 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.
- Technology may be used, for educational purposes, as mutually agreed with the Head teacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Capturing images & video is not allowed by students / staff unless on school equipment and for educational purposes.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image, video or sound recordings are made on the devices of any member of the school community.

- Where the school provides mobile technologies (e.g.: phones, laptops, iPads etc.) for offsite visits and trips, only these devices should be used.

Use of personal mobile phones and cameras by parents/carers and visitors:

- 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 setting 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 phones and cameras should only be used away from the children, off site or in our staff room.

- The schools main telephone number can be used for emergencies.

- Photos of children at school events **must not** be taken by parents/carers or visitors (please refer to the document 'Guidance for settings on the use of Images, Mobile Phones and Cameras in accordance with the Data Protection Act 1998').

- 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.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and be aware of what constitutes good 'netiquette'.

- The school gives all staff an individual LGfL StaffMail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and that of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. Staff LGfLmail should be used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- **The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder.**
- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Head teacher, line manager or designated office account.

- Pupils may only use school approved email accounts within the school learning platform DB Primary on the school system and only under direct teacher supervision for educational purposes.
- London Mail incorporates Safemail which allows the school's Nominated Contact to control who can send / receive emails, to / from whom.
- All email users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive message and keep the offending message(s) as evidence.
- Staff must inform the Computing Leaders if they receive an offensive email.
- Pupils are introduced to email as part of the computing 'Switch on ICT' Scheme of Work in year 3.

Safe Use of Images / Video

Taking of Images and Video

Digital images / video are easy to capture, reproduce and publish and, therefore, easily misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images / video by staff and pupils with school equipment.
- Staff are not permitted to use personal devices, (e.g.: mobile phones and cameras), to record images of pupils, this includes when on field trips. Staff must use technology which belongs to the school. This is then transferred immediately and solely to the schools network and deleted from the device.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos/ video in the following ways:

- on the school web site
- on the school's Learning Platform (DB Primary)
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g.: divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Storage of Images / Video

- Images/ videos of children are stored on the school's network in the named 'Multimedia' drive.
- Pupils and staff are not permitted to use personal portable media (e.g.: USB storage devices) for storage of images without the express permission of the Head teacher

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network and the Learning Platform.
- Staff need to use encrypted USB storage devices.

Webcams and CCTV

- CCTV is used in the following areas: Outside the main gates, in the car park, the reception area, the upper and lower hall and all the corridors.
- The school uses CCTV for security and safety. Notification of CCTV use is displayed at the front of the school. There is a screen showing the CCTV in the administration/reception office and the caretaker's office.
- Webcams in school are only ever used for specific learning purposes, (e.g. Monitoring hens' eggs) Images of children or adults are never broadcast.
- Webcams / CCTV is only used for staff training or development with the permission of the staff concerned.
- Misuse of a webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)

The Learning Platform- DB Primary

- All staff will be trained and given advice on how to effectively use the DB Primary Learning Platform.

- Parents will be informed about what the DB Primary Learning Platform is and how it can enhance the learning of each child. All children will be given training on how to effectively use the DB Primary Learning Platform within computing lessons.

- All children will use their LGFL passwords to access secure resources and facilities through the DB Primary Learning Platform. Children will be taught to keep this secure.

- The DB Primary Learning Platform will be regularly monitored for incidents of cyber-bullying, inappropriate use of language or the uploading of inappropriate files. Children will be informed that the sending of messages through the DB Primary Learning Platform is monitored and misuse of the messaging system will result firstly in a warning, followed by removal as a user should such behaviour be repeated.

- Children will be allowed to upload 'age-appropriate' photographs of groups or group activities, or of themselves onto their homepage.

- Class teachers will monitor the use of the DB Primary Learning Platform. Any misuse will be reported to the Computing Leaders, and subsequently the Head teacher/ Deputy Head teacher.

Misuse and Infringements

Complaints
Complaints relating to e-Safety should be made to the e-Safety co-ordinator or Head teacher. Incidents should be logged (see Incident Log in Appendix)

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Head teacher
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Head teacher, and depending on the seriousness of the offence may lead to:
    - Reporting to the Child Protection / Safeguarding Officer
    - Investigation by the Head teacher / LA
    - Immediate suspension
    - Dismissal
    - Involvement of police

- Users are made aware of sanctions relating to the misuse or misconduct when signing the Acceptable Use Agreement at the beginning of each school year.

Equal Opportunities

Pupils with additional needs
The school endeavours work in partnership with parents to convey a consistent message to all pupils. This in turn should aid the establishment and future development of the schools' rules.

Staff are aware that some pupils will require additional reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Activities are planned to make use of best available resources and are carefully managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school while appreciating the benefits provided by technologies generally. We regularly consult and discuss with parents/ carers and seek to promote a wide understanding about the link between technology and safeguarding.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to where appropriate in the form of;
    - Information and celebration evenings
    - Posters
    - The school website
    - Weekly newsletter
    - E-safety workshops

Writing and Reviewing this Policy

Review Procedure

There will be an on-going opportunity for staff to discuss with the co-ordinator any issue of e-Safety that concerns them.

This policy will be reviewed every *12* months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read, amended and approved by the staff, head teacher and governors on the _____

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

The school Acceptable Use Policy is designed to ensure that all staff are aware of their responsibilities when using any form of Information & Communications Technology within their professional role. All staff are expected to sign this policy and adhere at all times to its contents.

- I will comply with the ICT system security protocols and not disclose any passwords provided to me by the school or other related authorities.
- 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 ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will ensure that SIMS data is not accessed from home.
- I will ensure that I only take school personal data off school site in encrypted form, or will access the data remotely.
- I will not install any hardware or software without permission of the Computing leaders.
- I will not browse, download, upload or distribute any material of a pornographic, offensive, illegal or discriminatory nature. **I understand that to do so may be considered a disciplinary matter, and in some cases a criminal offence.**
- 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 respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.
- 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.

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …… Date ……

Full Name ……(printed)

Job title . . . . . .

Acceptable Use Agreement for Pupils

Primary Pupil Acceptable Use
Agreement / e-Safety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my DB Primary email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my LGFL password OR use another pupils.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address.
- ✓ I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my e-Safety.
- ✓ I will not give private details (home address, mobile number, email address etc.) to people I meet online.

Lady Margaret Primary School

Lady Margaret Road, Southall, Middlesex, UB1 2NH
Tel: 020 8566 6486 **Fax:** 020 8566 6713
Email: office@ladymargaret.ealing.sch.uk **Web:** www.ladymargaret.ealing.sch.uk
Head teacher: Mrs H Rai MA NPQH **School Business Manager:** Mrs A Hancock
Chair of Governors: Mr D Mankoo

Dear Parent/ Carer

Re: Acceptable Use Agreement for pupils

Computing, including the Internet, 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 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 Ms Nandra or Ms Koriya by leaving your name at the school office or emailing the office at: office@ladymargaret.ealing.sch.uk

Yours faithfully,

Mrs H. Rai
Head teacher

Ms Nandra & Ms Koriya
Computing Leaders of Learning

✂----------

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……

Lady Margaret Primary School

Lady Margaret Road, Southall, Middlesex, UB1 2NH
Tel:020 8566 6486 **Fax:** 020 8566 6713
Email: office@ladymargaret.ealing.sch.uk **Web:** www.ladymargaret.ealing.sch.uk
Head teacher: Mrs H Rai MA NPQH **School Business Manager:** Mrs A Hancock
Chair of Governors: Mr D Mankoo

Dear Parent/ Carer

Re: Acceptable Use Agreement for pupils

Computing, including the Internet, 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 Ms Nandra or Ms Koriya by leaving your name at the school office or emailing the office at: office@ladymargaret.ealing.sch.uk

Yours faithfully,

Mrs H. Rai
Head teacher

Ms Nandra & Ms Koriya
Computing Leaders of Learning

✂----------

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 ……

Incident Log (suggested format)

'School name' **eSafety Incident Log**

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying should be recorded on the 'Integrated Bullying and racist Incident Record Form 2'

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons