A Catholic Independent Primary School for boys and girls aged 3 to 11

LALEHAM LEA SCHOOL & NURSERY

E-SAFETY POLICY

This is a whole school policy which applies to all sections of the school, including Early Years Foundation Stage, Out of School Care and Clubs.

Person responsible for this policy:
Karen Barry
Head teacher

Laleham Lea Primary School, 29 Peaks Hill, Purley, Surrey, CR8 3JJ

Introduction

Technology and communications are rapidly changing and becoming more sophisticated. With this change come new ways of being unsafe and feeling threatened. E- Safety has become a very important issue which it is essential to address in school throughout different areas of the curriculum to ensure that all children and adults remain safe and in control when using technology. This could be either using mobile telephones or computers or other mobile devices with access to the internet

1. Aims

We aim to help every pupil and adult to:
- Feel safe and confident when using new technologies.
- Know who to speak to when they unsafe.
- Know how to report any abusive behaviour.
- Know how to use the internet correctly, without misuse.
- Stay in control and keep personal information private.
- How to take the necessary measures to block and delete accounts, messages and people.

2. Roles and Responsibilities

All the adults that are involved in the life of the school community, whether governors, teaching staff, support staff, or technicians, have roles and responsibilities that are associated with E-Safety as well as all pupils who come into contact with computers.

Governors

The Governors are responsible for the approval of the E-Safety Policy and reviewing the effectiveness of it regularly. Regular meetings and information will be provided to the Governors so they are able to make the correct recommendations; they will also be able to carry out regular monitoring of E-Safety incident logs when required.

Headteacher and Senior Leadership

The Headteacher is responsible for ensuring the safety, including E-Safety, of the members of the school community. Although the day to day managing of E-Safety will be delegated to the E-Safety Co-ordinator.

The Headteacher and Senior Leadership Team are responsible for ensuring that all staff and the E-Safety Co-ordinator receive correct and suitable Continuing Professional Development (CPD).

The Headteacher and Senior Leadership Team will ensure that there is a system in place to monitor the usage of internet and other technologies and that the person who carries out the internal E-Safety monitoring receives support and is also monitored. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Headteacher and Senior Leadership Team will ensure that they receive regular updates and reports from the E-Safety Co-ordinator.

The Headteacher and another member of the Senior Leadership Team are to ensure they know the correct procedures that need to be followed when a serious allegation has been made by a child or in regard to a member of a staff.

E-Safety Co-ordinator

The E-Safety Co-ordinator will take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school E-Safety policies / documents.

The E-Safety Co-ordinator will ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place and will provide training and advice for all staff.

The E-Safety Co-ordinator will liaise with the Local Authority and liaise with school computing technical staff.

The E-Safety Co-ordinator will receive reports of E-Safety incidents and create a log of incidents to inform future e-safety developments.

The E-Safety Co-ordinator will meets regularly with Governors to discuss current issues, review incident logs and filtering / change control logs and reports regularly to Senior Leadership Team.

Technical Staff

The Network Manager /Computer Technician is responsible for ensuring:
- that the school's computing infrastructure is secure and is not open to misuse or malicious attack.
- that users may only access the school's networks through properly enforced password protection, in which passwords are regularly changed.
- that he/ she keeps up to date with relevant E-Safety technical information and guidance in order to carry out the role effectively.
- that monitoring software/ systems are implemented and up dated regularly.

Teaching and Support Staff

Teaching and Support Staff are responsible for-
- Ensuring they stay up to date with current E-Safety matters and policies and practice.
- They read, understand and carry out the Acceptable Use Policy (AUP).
- They report any misuse or problems to the E-Safety Co-ordinator/ Headteacher for further investigation.
- That any digital communications with pupils (email, Learning Platform) should be strictly professional and only carried out using school systems.
- That E-Safety issues are embedded throughout the curriculum.
- That pupils follow the AUP and E-Safety policy.
- Being are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

Child Protection Officer

The Child Protection Officer needs to ensure that they are fully trained in E-Safety issues and are aware that serious child protection issues could occur due to-
- Cyber- bullying
- Sharing of personal data
- Inappropriate online conduct with adults/ strangers
- Potential or actual incidents of grooming

Pupils/ Students

Pupils and students are responsible for-
- Knowing and acting accordingly to the school's AUP.
- Knowing the importance of reporting abuse, misuse or access to inappropriate materials and know how to report them.
- Knowing the policy on mobile phones, digital cameras and other hand held devices and to realise these can be used for cyber-bullying.

Laleham Lea Primary School, 29 Peaks Hill, Purley, Surrey, CR8 3JJ

- Understanding that the E-Safety policy also covers their actions out of school, if related to their membership of the school.

Parents/ Carers

Parents and carers have the responsibility to ensure that their children use the internet and mobile phones correctly and do not misuse these technologies. They must be aware of the schools AUP and agree to it.

3. Education

- All children will receive planned E-Safety lessons throughout Computing/ P.S.H.E lessons. These lessons will be regularly revisited and revised to suit the new technologies in and out of school. Key messages will be delivered through a variety of assemblies to ensure all children are aware of the matter. They will also be made aware to question the validity of information which they find online.
- Parents will be invited to attend regular E-Safety meetings, where they will also have the opportunity to ask questions regarding E-Safety. They may also receive information at parents' evenings and by newsletters.
- All staff will receive regular training regarding E-Safety and an audit of their E-Safety needs will be carried out. All new staff will receive E-Safety training as part of the induction process, ensuring they are fully aware and understand the E-Safety policy and the AUP. The E-Safety Co-ordinator will be able to attend to regular updates provided by the Local Authority or other training schemes and report back to staff any new issues that they need to be aware of. The E-Safety Co-ordinator will provide guidance for any member of staff that seeks it.
- Governors will attend regular meetings which will provide information about E-Safety.

4. Technical

Laleham Lea School receives a filtered broadband service through the broadband connectivity. This service is intended to stop users from accessing any material that is illegal or would be regarded as inappropriate for the learning environment.

All staff and pupils will be made aware that there is also a monitoring system in place and any online activity can be traced. The person responsible for monitoring this will also be monitored by the Headteacher to ensure that this is being done effectively and correctly.

All personal data will be stored on the school server only (which is virus and malware protected) according to the Personal Data Act 1998. Staff must access personal data via secure password protected machines and devices only, ensuring that they 'log off' at the end of any session to minimise any chance of the data being seen by others. Personal data is not permitted to be stored on any USB or mobile device.

5. Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages in the use of Computing across the curriculum.
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg weapons, which could be part of a study on the Roman Army) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should have clear

reasons to support the need of these websites. Requests for website release should be made on an appropriate request pro-forma.

-Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.

Communications

This is an area which is rapidly developing and will need to be constantly revisited as technology advances and changes. Laleham Lea School recognises that different communications can have the potential to enhance learning and therefore can be a powerful tool.. But we are also aware of the risks that may come with these in regard to E-Safety.

Use of Digital Video and Images

The development of digital images and videos has significant benefits within the curriculum and enhances learning. Image and videos can either be taken by staff and pupils for educational purposes or downloaded from the internet to support learning in the classroom. However, staff and pupils need to be aware of the risks associated with sharing images, especially via the internet. Staff and pupils need to be aware that once an image/ video is posted on the internet that it will remain there forever. This could cause harm or embarrassment in the future.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational purposes, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken that when capturing images/ videos that all pupils concerned are appropriately dressed and not participating in activities that could bring either the pupils or the school into disrepute.

- Pupils full names will not be used anywhere on the website or in blogs and particularly not associated with photographs there.

- Written permission must be obtained from the parent or carer of any child before pictures are published on the website. Written permission is provided for every child that starts the school to indicate whether the parent or carer allows their child to be photographed.

- Laleham Lea School will always comply with the Data Protection Act 1998 in regards to digital images and videos.

Unsuitable Use, Sanctions and Reporting

It is expected that all users will be responsible and safe users of computers, who understand the policy and work within it. However, at times an infringement of the policy may occur whether through carelessness or, very rarely, deliberately.

If any apparent or actual misuse appears to involve illegal activity ie.

• child sexual abuse images

• adult material which potentially breaches the Obscene Publications Act

• criminally racist material

• other criminal conduct, activity or materials,

the correct reporting procedure is in place and all staff are aware of who to speak to in the first instance. This being, speaking to the E-Safety Co-ordinator who will then investigate the matter. If the matter is of a serious

nature then either the Child Protection Officer or the Headteacher will be informed, who will take the matter further.

All children will be made aware of the importance to report any incident to an adult at school that they can trust, regarding any incidents that may occur outside of school.

If an incident has occurred due to carelessness, this will to be investigated and the correct sanctions will be implemented. All users within the school are aware that there is a monitoring system that is in place and is sensitive enough to pick up slight infringements regarding; cyber-bullying, searching for inappropriate content etc.

In all cases the Headteacher when notified will decide what action to take and whether the incident needs further action, e.g. reporting to police, Local Authority.

6. Monitoring and Review and Policy Ownership

Working with Parents

Our school seeks to work in partnership with parents to provide effective E-Safety. Parents need to know that the school's E-Safety programme will complement and support their role as parents and that they can be actively involved in the determination of the school's policy.

Appendix 1

ICT Acceptable Use: Agreement form (Staff)

EMAIL / INTERNET / INTRANET / NETWORK USAGE POLICY

•I will only use the school's Email / Internet / Intranet for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

•I will not browse, download or send material that could be considered offensive to colleagues or children.

•I will report any accidental access to inappropriate materials to the appropriate line manager.

•I will not download any software or resources from the Internet that can compromise or damage the network, or is not adequately licensed.

•I will ensure all documents are saved, accessed and deleted appropriately.

•I will not connect a computer or laptop to the network / Internet that does not have up-to-date version of anti-virus software.

•I will not use personal digital cameras or mobile telephone cameras for transferring images of pupils or colleagues without permission from the Head Teacher.

•I will ensure I am aware of digital safety-guarding issues so they are appropriately applied in my classroom practice.

•I will not allow unauthorised individuals to access Email / Internet / Intranet.

•I understand that all Internet usage will be logged and this information could be made available to the Head Teacher and Governing Body on request.

•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 not use my mobile telephone when in class or in charge of pupils. I will only use my mobile telephone during my personal breaks, or with the express permission of my line manager in emergencies.

•I understand that failure to comply with the Usage Policy could lead to disciplinary action.

•I will exercise discretion when using Social Networking Websites and will notify the Headteacher immediately if I am contacted by pupils or former pupils of the school. I will not respond to any contact made to me electronically by any child.

•I will notify the Headteacher if, when using the internet, I recognise any children from school using Social Networking Websites inappropriately or illegally.

User Signature

I have read and understood the E - safety policy.

I agree to abide by the above Acceptable Usage Policy.

Signature …………………………………

Date ……………………

Full Name …………………………….……………………………….(printed)

Job title . . . .

Authorised Signature (Head Teacher)   …………………………………………....

Is this member of staff temporary? NO / YES

If yes, contract end date: ……………

I approve this email account / connection to the Internet / Intranet.

Signature …………………………………......

Date ……………………

Full Name …………………………….………...(printed)

One copy is retained by member of staff / Second copy for school file

Laleham Lea Primary School, 29 Peaks Hill, Purley, Surrey, CR8 3JJ

Appendix 2   Pupil Acceptable Use Policy

Rules For Responsible Internet Use

> **Please note, this document must be returned signed, to the office before your child will be allowed to use the internet. This agreement will be updated annually.**
>
> **PLEASE KEEP A COPY FOR YOUR INFORMATION**

The school has installed computers with internet access to help learning. These rules will help keep us safe and help us to be fair to others. We suggest that you use these rules at home to stay safe.

Using the computers:

- I will only access the computer system with the login and password I have been given
- I will not look at or delete other people's files
- I will not bring files into school without permission

Using the Internet:

- I will ask permission from a teacher before using the internet
- I will only use the internet when an adult is present in the classroom
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself
- I understand that the school may check my computer files and may monitor the internet site I visit
- I will not complete and send forms without permission from my teacher
- I will not give my home address, phone number, send a photograph or video, or give any other personal-information that could be used to identify me, my family or my friends, unless my teacher has given permission
- I will not open an attachment or download a file unless I have permission or I know and trust the person who has sent it.

Using e-mail

- I will ask permission from a teacher before checking e-mail
- I will immediately report any unpleasant messages sent to me because this will help protect other pupils and myself
- I understand that e-mail messages sent to me may be read by others
- The messages I send will be polite and responsible
- I will only e-mail people I know, or who my teacher has approved
- I will only send e-mail when it has been checked by a teacher
- I will never give my full name, my home address or telephone number in an email

Laleham Lea Primary School, 29 Peaks Hill, Purley, Surrey, CR8 3JJ

- I will never arrange to meet someone I have only ever previously met on the internet or by email or in a chat room, unless my parent or guardian has given me permission and I take a responsible adult with me.
- I know that use of some Social Networking Websites is illegal under national law for children. I will not set up or use a Facebook, Twitter, Snapchat, Google+, Instagram or You Tube account, even if older brothers or sisters or parents say that it is OK, as I know that children under the age of 13 may not uses these sites.

Parent/Pupil E-Safety Agreement Form

Keeping safe: stop, think, before you click!

Pupil name: _____

I have read the school 'rules for responsible ICT use'. My teacher has explained them to me.

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and other ICT in a safe and responsible way. I understand that the school can check

my computer files, and the Internet sites I visit and that if they have concerns about my safety, that they may contact my parent / guardian.

I understand that the use of Facebook and YouTube is illegal to children under the age of 13.

Pupil's signature _____

Parent's signature _____

Date: __/__/__