E-Safety Policy

Reviewed by the Proprietor, March 2017

Le Hérisson | Rivercourt Methodist Church, Rivercourt Rd, London, W6 9JT | 020 8563 7664
Administration@leherissonschool.co.uk | www.leherissonschool.co.uk

Introduction

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are beneficial to all, but can occasionally place children, young people and adults in danger. E-Safety covers issues relating to children and young people, as well as adults, and their safe use of the Internet, mobile phones and other electronic communication technologies, both in and out of school. It includes education for all members of the school on risks and responsibilities and is part of the 'Duty of Care' which applies to everyone working with children.

Our E-Safety policy sets out how the school plans to develop and establish its E-Safety approach and to identify core principles, which all members of the school need to be aware of and understand. It works alongside the school to ensure all members of the school community are kept safe.

Teaching and learning

Internet use is part of the curriculum and is a necessary tool for learning. The school has a duty to provide pupils with quality internet access as part of their learning experience to enable them to access a wealth of online resources and enrich their learning. Pupils need to learn how to evaluate internet information and to take care of their own safety and security. The purpose of the internet in school is to help raise education standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

The benefits of internet use on education

Benefits of using the internet in education include:

- Access to worldwide educational resources including museums and art galleries
- Educational and cultural exchanges between pupils worldwide
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational material and effective curriculum practice
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data
- Access to learning where and whenever convenient

Enhancing learning

The school's internet access is designed to enhance and extend education. Lessons incorporating IT will teach children about the internet and give the pupils clear objectives for internet use. The school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.

Staff will guide pupils to particular sites that support the learning intention and are appropriate for the age group being taught. Random searches on the internet are not productive or appropriate.

How pupils learn to evaluate internet content

Pupils at Le Hérisson will always be monitored when they are using the internet and will always use age-appropriate tools when accessing internet content.

Learning about e-safety and responsible use of technology

Pupils will learn about e-Safety under the guidance of their teachers as they access the internet.

Managing information

Maintaining information systems security

The school server is located securely and physical access is restricted. It is managed by Computrad who ensure that the server operating system is secure and kept up to date. Antivirus has been installed across the school network and these servers receive updates automatically. Access to the internet by wireless devices not joined to the school network e.g. visitors computers, mobile phones etc. is prohibited. A username and password is required to gain internet access wirelessly and these codes are only known to the **Proprietor, Maria Frost**. The school's firewall protects the school from undesirable sites and content available online. Staff should log off or lock their machines/tablets when leaving them unattended. Usernames and passwords to the school system must be kept confidential by all members of staff. Failure to do so will result in disciplinary action.

Computrad have provided Le Herisson School with a business-grade file sync service, eFolder that enables users to sync sensitive corporate data via the following:

- Compliant data centers and military-grade encryption
- SSAE 16 Type II or SOC Certified
- Silent Data Corruption Protection, end-to-end checksums to "tag" data with strongly verifiable identifiers
- HTTPS stand-alone processes running behind a firewall
- Persistent and transient encryption key
- Organizational privacy mode
- Data transferred over Secure Sockets Layer (SSL) encrypted connections
- Server Side Encryption (SSE), using 256-bit Advanced Encryption Standard (256-bit AES) in transit and at rest

Email management

Members of staff must only use the official school provided email accounts for school purposes and to communicate with parents/carers. Each classroom has been provided with an account and the passwords are only known to the Proprietor. Staff must not reveal personal details of themselves or others in email communication or arrange to meet or communicate with current/past parents/members of staff out of school hours. Staff must immediately alert the Proprietor if they receive offensive emails. They are only allowed to access their personal email accounts during non-direct teaching time. Personal accounts must not be used to fulfil any type of school business. Only the Proprietor, Administration and classroom email addresses will be used for communication outside of the school. Emails sent

to external organisations and parents must be written carefully in the same way as a letter written on school headed paper would be. The forwarding of chain messages is not permitted.

Published content

The school website is a great source of information for all the stakeholders in the school. Publication of any information online will always be considered from a personal and school security viewpoint. The contact details on the website will be the school address, email and telephone number. Staff or pupils information will not be published. Materials that contain key information such as letters to parents or staff school email addresses will be in a section of the website that is password protected. The Proprietor will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

Pupils' images and work

Images or videos published on the school website, that include pupils, will be selected carefully and will not provide material that could be reused e.g. small pictures of groups of pupils 'over the shoulder style' photos that do not show faces. Pupils in photographs will be appropriately clothed and written permission from parents or carers will be obtained before the images/videos/work of pupils in electronically published. Pupils full names will not be used anywhere of the website, particularly in association with photographs. General statements will be used to describe photos of the children where necessary.

Social networking, Social media, Personal publishing

Access to social networking sites, social media and personal publishing sites is not permitted in school and key sites such as Facebook/Twitter are blocked by filter. Staff are taught about the risks posed by these sites including the consequences of not enforcing privacy settings correctly. Staff will be made aware about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. Staff wishing to access such sites for curriculum related materials must gain permission from the Proprietor.

Outside of school staff must not post or write negative and damaging information about the school or any of its stakeholders e.g. the Board, staff, parents, children. Staff are aware that this goes against school policy, teaching standards and that publishing unsuitable material may jeopardize their professional status. School staff should not be 'friends' or connect with parents/carers of social networking sites. They are all expected to keep a 'professional distance' from the parent body of the school and in this respect are strongly advised NOT to enter into social media exchanges with any parents.

Staff members personal use of social networking, social media and personal publishing sites will be discussed as part of the staff induction and professional behaviour will be outlined in the school Acceptable Use Agreement.

Blogs *(ToutеMonAnnee.com)*

In order to facilitate parent communication, every classroom has a blog that showcases what the children have been doing during week and throughout the year. Parents are

required to sign a permission slip if they want their children to be featured on the blog and if they want to gain access to it. Each blog is password protected with a unique password, managed by Teachers and monitored by the Proprietor. Parents are also able to upload pictures of their children and comment on the information posted on the blog. All comments and pictures require approval from the teacher before being published. This ensures that content is moderated and appropriate for viewing. Parents who have opted out of having their children featured in the blog will have their children's pictures omitted or blurred if it is a group photograph.

To add video content to blog posts, *Toute Mon Anee* requires videos to be uploaded via 1 of 3 platforms: Vimeo, DailyMotion and YouTube. The school has a YouTube account to host the videos online and all teachers use the same account. Videos remain completely private and unpublished and the YouTube account is not accessible to anyone but the teachers and proprietor.

The blog ensures the confidentiality of data it collects. The collected personal information is intended for the blog and cannot be sold or disclosed to third parties. Apart from the information to the public school site, the information provided in the blog is protected by an access code that only the Proprietor / teachers have.

The blog keeps the data necessary for the creation of classroom logbooks for 3 months after the end of the school year. After this period, access to the log will be automatically deactivated and the files destroyed. The data made public on the school site will be kept for one year to ensure the sustainability of the school's website however, all data on the blog can be destroyed at any time of the year if requested by school.

In accordance with the "Data Protection" law, the processing of personal information by the blog has been acknowledged to the *Commission Nationale Informatique et Libertés (CNIL)* under number 1453244. This data can be continuously modified by the Proprietor and teachers at their discretion.

Filtering

The school's broadband Internet connection is filtered and managed by the school's technical company, Computrad, who use a reputable and effective filter. All sites on the Internet Watch Foundation (IWF) are blocked for all users. This filter allows for different levels of filtering staff and pupils dependent of the login used. The pupil login has the strongest filter applied. Staff are made to recognise that filtering is not always 100% effective and inappropriate content may be accessed. Any inappropriate sites accessed must be reported to the Designated Safeguarding Officer or the Proprietor immediately and recorded in the E-Safety Incident Log, which is kept in the Safeguarding Folder. Any material that the school believes is illegal will be reported to appropriate agencies such as the local Police and Local Authority Designated Officer. Websites which teachers believe should be blocked centrally must be reported to the School Manager, who will then forward their concerns to Computrad and readjust the levels of filtering.

Children will always be supervised when using internet access. No unsupervised access by pupils to the internet is allowed. Acceptable Use Agreements are in place for staff and internet safety rules are displayed next to the computers in classrooms. Teachers will always evaluate any websites/search engines before using them with their class; this includes websites shown in class as well as websites accessed directly by pupils. This means that all members of staff are responsible for checking search results before their lessons due to the

constantly changing nature of website. Children should be directed to websites by shortcuts/links not via a Google search.

Videoconferencing

The use of Facetime and other such technologies on handheld devices is not allowed for use by pupils and staff within the school unless connected to a curriculum focus. The teacher must seek permission for this from the Proprietor. Parents will be informed of curriculum activities involving videoconferences/Skype/Facetime calls by the teacher prior to the activity taking place so that they can ask further questions if required.

When using video conferences equipment or opportunities, conferences will always be booked as private and not made public if using a third-party provider. Staff should always check who has signed into their conference as a guest without a camera would not be visible. Staff should discuss the requirements for any video conferences with Proprietor before embarking on the project to ensue E-Safety guidelines and technical requirements are managed effectively. Only team members versed in Skype/Video conferencing will be allowed to use those technologies to ensure safe usage.

Emerging technologies

Emerging technologies will be examined for education benefit before use in school is allowed. Access will be denied until proper thought and examination of the benefits is complete as new technology will change teachers' pedagogy as well as giving pupils access to online material.

Data protection

In accordance with the Data Protection Act 1998, everyone at Le Hérisson School has a legal duty to protect the privacy of information relating to individuals. Teachers should not save work containing pupil details or data of photos to their desktop especially if they take the laptop offsite. Staff should not take USB memory sticks or portable hard disks containing pupil data out of the building.

Internet access authorisation

Access to the internet will always be by adult demonstration with occasional directly supervised access to specific and approved online materials via a web link or shortcut. Older pupils will have access to a wider range of sites and undertake searches using age-appropriate search engines, once 'safe searching' has been discussed in their E-Safety lesson. Access will always be supervised.

Risk assessments

The school will take all reasonable precaution to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school will not accept liability for the material accessed, or any consequences resulting from internet use. The school will audit ICT to establish if the e-Safety policy us adequate and that the implementation of the e-Safety policy is appropriate.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the local police. Methods to identify, access and minimise risks are reviewed regularly.

Responding to incidents of concern

Staff may report incidents of concern in person or anonymously to the Proprietor. All reported incidents and actions taken will be recorded in the E-Safety Incident Log or in the administration drive if of a confidential nature. The Designated Safeguarding Officer will be informed of any E-Safety incidents involving Child Protection concerns, which will then be escalated appropriately. The school will inform parents/cares of any incidents of concerns as and when required.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required. Where there is a cause for concern or fear that illegal activity has taken place, the school will contact and escalate the concern to the Police. If the school is unsure how to proceed with any incidents of concern relating to a member of staff, the Designated Safeguarding Officer and Proprietor will seek the guidance of the Hammersmith and Fulham LADO.

Handling complaints

Complaints about Internet misuse will be dealt with under the school's complaints procedure. Any complaint about staff misuse will be referred to the School Manager. All E-Safety complaints will be recorded by the school, including any action taken, in the Complaints folder. All members of the school have been made aware of the importance of confidentiality and need to follow the official school procedures for reporting concerns. Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection/safeguarding procedures. All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress, or offence to any other members of the school community.

Management of mobile phones and personal devices

Staff must not use their mobile phone during direct-teaching time or in parts of the school shared by pupils during their non-contact time. When in classrooms or teaching children, mobile phones should be turned off or switched to silent. Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and should only use work-provided equipment for this purpose.

There are dangers for staff if personal phones are used to contact pupils and or parents. School owned mobile phones will be issued to staff to take on school trips and residential trips. Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or without the school in a professional capacity. The school telephone system should be used for such communication whilst onsite. Staff who are on offsite school activities may use their own mobile phones to contact the school office or other members of staff as long as they are without children.

Electronic devices of all kinds that are brought into the school are the responsibility of the user and the school accepts no responsibility for the loss, theft or damage of such items.

Issuing of the policy

This E-Safety policy has been drawn up in consultation with Computrad and the Acceptable Use Policy (AUP) was implemented as part of this process. All staff must sign the AUP and new staff are asked to sign the AUP upon joining the school. The signed copies are kept in the Safeguarding folder. The AUP is revised in line with new safeguarding legislation and updated accordingly. Staff are aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute or if something is felt to have undermined confidence in their professional abilities. Staff are aware that internet traffic can be monitored and traced to the individual user.

All school laptops and devices issued to staff by the school are covered by this E-Safety policy and should not be used by third parties. Staff know of their responsibilities to maintain confidentiality of the school information.

Parent support

Parents' attention will be drawn to the school E-Safety Policy in newsletters and on the school website. Parents will be requested to read the school Acceptable Use Policy for pupils and discuss its implications with their children.

Guidelines For Staff on Social Networking

Principles for Staff
When networking– **BE PROFESSIONAL, RESPONSIBLE AND RESPECTFUL**

1. You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for Le Hérisson and your personal interests.
2. You must not engage in activities involving social media which might bring Le Hérisson into disrepute.
3. You must not represent your personal views as those of Le Hérisson on any social medium.
4. You must not discuss personal information about pupils, Le Hérisson and other professionals you interact with as part of your job on social media.
5. You must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations, or Le Hérisson.
6. You must be accurate, fair and transparent when creating or altering online sources of information on behalf of Le Hérisson.
7. Staff members must not identify themselves as employees of Le Hérisson or service providers for the schools in their personal webspace. This is to prevent information on these sites from being linked with Le Hérisson and the schools and to safeguard the

privacy of staff members, particularly those involved in providing sensitive frontline services.

8. Staff members must not have contact through any personal social medium with any pupil, whether from Le Hérisson or any other school, unless the pupils are family members.
9. Staff members must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.
10. On leaving Le Hérisson, staff members must not contact parents by means of personal social media sites.
11. Information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues and other parties and the school must not be discussed on their personal webspace.
12. School e-mail addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.
13. Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.
14. Le Hérisson's corporate, service or team logos or brands must not be used or published on personal webspace.
15. Le Hérisson does not permit personal use of social media while at work. Staff members are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the internet should not be on the school's time.
16. Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.
17. Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate e-mail address just for social networking so that any other contact details are not given away.

Written : November 2016 **Review Date : March 2018**

Last reviewed: 20/11/2017

Le Hérisson | Rivercourt Methodist Church, Rivercourt Rd, London, W6 9JT | 020 8563 7664
Administration@leherissonschool.co.uk | www.leherissonschool.co.uk

Acceptable Use Agreement/Code of conduct

ICT and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Proprietor.

- I will only use the school's e-mail / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Proprietor
- I will comply with the ICT system security and will not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Proprietor.
- I will not use or install any hardware (including USB sticks) or software without permission from the Proprietor.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or the Proprietor.
- I understand that all my use of the Internet and other related technologies can be monitored and logged.
- If a password may have been compromised or someone else has become aware of my password I will report this immediately to the Proprietor.
- I will ensure that workstations are not left unattended and unlocked.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, including my use of any social networking site will not bring my professional role 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.
- I will ensure that only children whose parents have given permission for them to use the Internet and ICT are enabled to do so at school.

By signing this Acceptable Use Agreement I am demonstrating that I have read, understood and agree to be bound by Le Hérisson's E-Safety Policy.

FULL NAME		DATE	
SIGNATURE		JOB TITLE	

Le Hérisson | Rivercourt Methodist Church, Rivercourt Rd, London, W6 9JT | 020 8563 7664
Administration@leherissonschool.co.uk | www.leherissonschool.co.uk