E-safety Policy

Last revised: November 2018
Policy Owner: Head of Computing

Policy Statement

This is a whole school policy.

This policy has been prepared with reference to Surrey County Council's E-safety Policy Template (revised 2014) and the CEOP Way Forward documentation (2010).

Associated Policies and Documents

- Lyndhurst School Safeguarding Policy
- Lyndhurst School Staff Code of Conduct
- Lyndhurst School Anti-Bullying Strategy
- Lyndhurst School Behaviour and Sanctions Policy

Introduction

The e-safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.

The e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

The school will use a recognised internet service provider or regional broadband consortium.

The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.

The school will ensure that its networks have virus and anti-spam protection.

Access to school networks will be controlled by personal passwords.

Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform e-safety policy.

The security of school IT systems will be reviewed regularly.

All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.

The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

There will be pin codes needed for the use of any iPads and other handheld devices.

All staff, governors and external companies affiliated with Lyndhurst School must be aware of GDPR guidelines and how to safely handle private data.

Internet Use

The school will provide an age-appropriate e-safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

All communication between staff and pupils or families will take place using school equipment and/or school accounts.

Pupils will be advised not to give out personal details or information which may identify them or their location

As part of being able to use the internet safely and securely, children will have a dedicated lesson focussing on strategies that will keep them safe while using the internet.

E-mail

Pupils and staff may only use approved e-mail accounts on the school IT systems.

Staff to pupil email communication must only take place via a school email address or from within the learning platform.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

If there are any doubts about and inbound or outbound email staff should immediately speak to a member of SLT.

Published content

The contact details for published content e.g. school web site, school social media accounts will be the school address, email and telephone number. Staff or pupils' personal information will not be published.

Publishing pupils' images and work

Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media.

Use of social media

The school will control access to social networking sites. This control may not mean blocking every site; it may mean monitoring and educating students in their use.

The school will educate its children on the safe usage of social media sites via modelling and frank discussion, with the ability for children to use a dummy account.

Use of video services such as Skype, Google Hangouts and Facetime will be monitored by staff. Pupils must ask permission from a member of staff before making or answering a video call.

Staff and pupils should use ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

Pupils will have a dedicated E-safety lesson each term lead by the Head of Computing that will cover a range of topics, including but not limited to cyber bullying and staying safe online.

Use of personal devices

Personal devices may not be used by staff or pupils whilst on the school premises. Staff and/or pupils may access the school IT systems remotely, provided their use complies with the e-safety policy and the relevant AUP.

Staff must not store images of pupils or pupil personal data on personal devices.

The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Authorising access

All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff AUP' before accessing the school IT systems.

The school will maintain a current record of all staff and pupils who are granted access to school IT systems.

In the Lower School, Pupil's access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials. In the Upper School, access to the internet will be with teacher permission with increasing levels of autonomy.

People not employed by the school must read and sign a Guest AUP before being given access to the internet via school equipment.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access.

Handling e-safety complaints

Complaints of internet misuse, within school or without, will be dealt with according to the school behaviour policy.

Complaints of a child protection nature must be dealt with in accordance with school's child protection procedures.

Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behavior policy.

Community use of the internet

Members of the community and other organisations using the school internet connection will have signed a Guest AUP so it is expected that their use will be in accordance with the school e-safety policy.

Communication of the Policy

To pupils

Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet

Pupils will be reminded about the contents of the AUP as part of their e-safety education

To staff

All staff will be shown where to access the e-safety policy and its importance explained.

All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet

Statement of acceptable use of ICT and related technology (staff)

ICT and the related technologies such as email, 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 to its contents at all times. Any concerns or clarification should be discussed with Andrew Friend, Head of ICT.

- I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email, internet and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Headmaster.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that all electronic communications with parents, pupils and staff, including email and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- 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 Headmaster.
- I will only take images of pupils and/or staff for professional purposes in line with school policy. I will not distribute images outside the school network without the permission of the Headmaster.
- Images will be taken using a school assigned camera or a school assigned iPad.
- Under no circumstances are personal devices (phones, tablets etc) to be used within school unless within the staff room area.
- I will not install any hardware or software without the permission of the Head of Computing.
- I will not download applications for the iPads without the consent of the Head of Computing.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or the Headmaster.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support the school's e-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the e-safety Coordinator, the Designated Safeguarding Lead or Headmaster.
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serous infringements may be referred to the police.

User Signature

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

Full Name…… (Printed)

Job title……

Signature…… Date……

E-safety: Acceptable Use of Computers (Lower School)

These rules help me to stay safe on the internet

I will take care of the school computers and iPads

I will only use the internet when I have been given permission by an adult

I will tell an adult if I see something on the internet that upsets me.

I will not tell other people my personal things about me.

I will always be polite and friendly when I write messages on the internet

NAME: _____

E-safety: Acceptable Use of Computers (Upper School)

Contract for using the school computers

These rules will help to keep everyone safe and help us to be fair to others.

- I will only use the school's computers and iPads for schoolwork and homework
- I will not let the use of iPads, or others using iPads, distract me from my learning
- I will not tell anyone any of my logins and passwords
- I will only login to the school systems as myself
- I will only edit or delete my own files
- I am aware that some websites and social networks have age restrictions which mean that I should not go on them
- I will only visit internet sites that are appropriate for my age
- I will only communicate with people I know, or that a responsible adult has approved
- I will only send polite and friendly messages
- I will not open an attachment, or download a file, unless I have been given permission by an adult
- I will not tell anyone 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 a trusted adult has given permission.
- If I see anything I am unhappy with or I receive a message I do not like, I will show a responsible adult.

My name: . . . . . Date: . . . . . .