Title:	E-Safety Policy			
Type:	POLICY			
Review Cycle Frequency:		1 year – Spring		
Lead Staff:	Deputy Head			
Support:	Designated Safeguarding Lead			
VERSION CONTROL:				
Version No	New document or reasons for revision		Agreed by	Date
1	Migration to new document version control system		Office	April 2021
2	Policy review			April 2022
3	Staff update			Sept 2022
LINKED INTERNAL DOCUMENTS:				
Safeguarding & Child Protection policy Staff Use of Social Media for Personal Use Data protection policy Social Media Policy				
LINKED EXTERNAL DOCUMENTS:				

Equalities Statement:

We have carefully considered and analysed the impact of these policies on equality and the possible implications for people with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

If you require this policy in a different format e.g. print or braille please contact
head@lindenlodge.wandsworth.sch.uk

Wellbeing statement of commitment

We are committed to providing a healthy working environment and improving the quality of working lives for all staff and students. The wellbeing strategy aims to support our mission, core values and freedom of thought and expression, freedom from discrimination and the recognition that our community is our greatest asset. For further information on our schools commitment to wellbeing, please see the Mental Health and Wellbeing Policy and Strategy document, or visit our school website.

Introduction

The Governors and the Senior Leadership team recognise the importance that technology has within Linden Lodge in supporting pupil's access to their education, independence and the world around them through the use of specialist technology and the internet. Our pupils use technology and the internet in a variety of different ways including but not limited to supporting them in accessing their education through adapted software, allowing them the opportunity to explore a wealth of information from around the globe through the use of the internet which has an important role for our pupils and one that has a positive impact on their learning and progress. The Governors and Senior Leadership team also understand, that the use of technology needs to be used in a safe and secure way in order to ensure our pupils do not fall victims to the dangers that accompany using the internet. This policy provides advice on how we aim to prevent our pupils coming to harm when using the internet. It also refers to the DFE's guidance on protecting children from radicalisation in line with Keeping Children Safe in Education.

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

Safeguarding

E-Safety forms an important part of our safeguarding offer to our pupils. The Designated Safeguarding Lead has overall responsibility for E-Safety supported by the Deputy Headteacher. The staff team, as part of the regular safeguarding updates and training, receive training within E-Safety delivered to them via external and internal trainers and are updated weekly via team briefings and the school Newsletter by the safeguarding team.

E-Safety: reporting, recording and concerns

All E-Safety concerns are reported to the safeguarding team via MyConcern.

Pupil reporting

We understand that some of our pupils will not be able to communicate their concerns directly to our staffing team and therefore it is vital that our staff teams working with these pupils are able to identify any concerns they have and respond accordingly in line with the safeguarding policy and procedures for reporting concerns.

For our pupils who are able to communicate their concerns, they know and understand what they should do in the event of e-safety concerns and are able to do so with the confidence that the staff team they report to will handle their concerns appropriately.

Staff reporting

Staff are trained to be vigilant within recognising the risks towards our pupils within e-safety. As a result, they are fully aware of the systems in place and the procedures required to report any concerns they have to the safeguarding team using MyConcern.

Escalating concerns

If staff feel there is a need to escalate concerns regarding e-safety they are able to do so via the following pathways:

Concerns regarding the handling of e-safety concerns by:
E-safety coordinator: Escalate to Designated safeguarding lead/Co-Headteacher
Designated Safeguarding Lead (DSL): Escalate to CEO of multi-academy trust
CEO of multi-academy trust: Head of Safeguarding for Wandsworth

Key contacts and who to go to in an emergency for E-Safety

Sarah Norris: Designated Safeguarding Lead for Linden Lodge School
David Shaw: Deputy Headteacher: E-Safety
Linden Lodge Safeguarding team

Our Environment

Linden Lodge is a large campus that includes both day and residential provisions. The site consists of multiple buildings all of which house varying degrees of specialist technology. All buildings have access to the internet. Linden Lodge has its own WIFI which is password protected. Visitors on site have access to the visitors WIFI and are given the password upon arrival.

Online safety awareness: Pupils, parents and staff

Linden Lodge delivers online safety training for everyone involved within the organisation including working closely with parents and carers to raise awareness of online safety within our pupil's home setting. We also ensure appropriate CPD training for staff which includes regular and systematic training that is embedded into the fabric of our school online safety approach.

In addition, Linden Lodge School, as part of the safer requirement for staff, supports the development of staff within the following areas:
Regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding

Online safety training in relation to Keeping Children Safe in Education
Annual training provided by our external provider/ advisor Child Net.
Use of technology for Children and Young People with SEN at Linden Lodge
At Linden Lodge we understand the importance of technology for our pupils and how is positively impacts their education. However, it is important that our staff understand the importance of the following:

- Our pupils, due to their need, are more vulnerable and more at risk than others when using computing equipment:
- Our pupils may make literal interpretations of content which will affect how they respond.
- Our pupils may not understand some of the terminology used.
- Our PMLD, SLD and MLD do not always understand the concept of friendship and therefore trust everyone implicitly.
- Our pupils do not always know how to make judgements about what information is safe to share. This leads to confusion about why you should not trust others on the internet.
- Our pupils may be vulnerable to being bullied through the internet.
- Our pupils may not understand or recognise that they are being bullied.
- Our pupils may not appreciate how their own online behaviour online may be interpreted by others as bullying.

E-Safety and our curriculum

Our curriculum pathways all aim to create engaged and active citizens in the wider community in the 21st century. A huge part of accessing society in its current form is through the internet and specialist technology and we need to ensure and embed e-safety into their day to day learning within school, residential and within their home environment. E-Safety awareness is delivered to our pupils through taught sessions within computing and PSHE.

Acceptable use of technology within school

Our intention is to ensure that our children and young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use while on site with us during the day and within residential. Through our online security platforms, we hope to ensure that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk and in addition we support our parents within the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

Staff use of technology at Linden Lodge School/ Professional boundaries
Staff receive regular information within e-safety and are fully aware of the importance of e-safety across the campus. Key considerations for our staffing team is the use of personal technology across the campus during the day and evening. Across our campus we are a non-personal technology site and staff are only able to use their personal technology within designated safe zones where no pupils have access to. As a school we are fully aware that staff are able to access content through the

cellular networks which bypass our own security measures and our staff are continually briefed to be vigilant in these circumstances and to report any concerns they may have within this to the safeguarding team. In addition to this, our entire staff group has access to our computer network through personal logins. Our school computers are protected by our onsite security settings.

How will information systems security be maintained?

At Linden Lodge we have an IT team that monitor and maintain the systems in place. The team are responsible for the safety of our pupils by ensuring our security systems are up to date and working.

The team ensure safety by:

- Monitoring and maintaining the server and ensuring the security is in place to protect it from harm
- Ensuring the virus protection is up to date and ready to protect the school from any potential harm
- Ensuring the firewall is robust and in place
- Ensuring the safety of the servers and securing them in a place that cannot be accessed by staff or pupils
- Ensuring the internet is protected by robust firewalls that prevent our pupils or staff downloading any inappropriate materials
- Ensuring the storage of school data is protected and able to be retrieved from back up files if needed
- Provide regular updates and checks for security systems

Provide pupils and staff with secure logins and maintain their systems regularly

Provide an encrypted email service for staff (EGRESS)

Social networks

- Linden Lodge School's filtering system blocks any access to social media platforms through its internet/ WIFI.
- Pupils are taught through structured lessons the appropriateness of internet use and are taught how to access the internet safely
- Pupils are taught to understand the risks posed by the internet and how to keep themselves and others safe
- Staff are trained to understand the risks posed by those who use the internet in order to bully, groom, radicalise or abuse pupils
- School leaders are expected to oversee the safe use of technology in school and act immediately where there are concerns about bullying or a pupil's wellbeing
- All staff has a shared responsibility to ensure that children are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all adults working with children are bound.
- Following the Keeping Children Safe in Education guidelines, it is the responsibility of all staff to ensure that all children that are accessing the internet in school are doing so through the school's internet and not 3G, 4G or

5G domains. This insures that block and filter access is in place when pupils are using the World Wide Web.
- Linden Lodge School offers training to parents in partnership with Child Net as to how to keep their children safe at home when using the internet.

Unintentional exposure to children of undesirable materials

Linden Lodge School takes every reasonable step in order to prevent exposure of pupils to undesirable materials on the internet.

It is recognised that this can happen not only through deliberate searching for such materials but also unintentionally when a justifiable internet search yields unexpected results.

To prevent such occurrences the school has adopted the following position:
- Internet filtering systems blocking access to inappropriate sites
- Adult supervision
- Training and educating our pupils in internet safety
- All staff attending Prevent training as part of our Prevent strategy

In the event of a young person accessing inappropriate materials, the Headteacher is immediately informed and safeguarding measures are put in place.

New technologies

Linden Lodge School is a place for innovation within specialist technology to ensure we continually meet the access needs for our pupils. Any new technology that enters onto school site is assessed and set up accordingly by our IT team before it is distributed to our pupils/ staff.

Residential

Linden Lodge School recognise that during our pupil's time within the residential unit they will be accessing technology including the use of mobile phones and tablets. We also recognise that these times may not always be supervised by the staff members working on the units. Therefore, we have initiated the following in order to support our pupil's safe access to the internet:

- Timed blocks on websites that can offer access to inappropriate materials
- Internet and e-safety lessons based on Google's framework of Sharp, Alert, Secure, Kind, Brave, Be internet legends, on the following areas: Think before you share/ Check it's for real/ Protect your stuff/ Respect each other/ When in doubt, ask.
- Robust firewall and filtering systems in place
- Staff awareness/ supervision of pupil spaces such as lounge/ kitchens

Assessing risks

Linden Lodge will monitor, through our security systems in place, all computer access by both staff and pupils. Any inappropriate content will be reported directly to the Head Teacher. Linden Lodge will take all reasonable precautions to ensure e-safety.

However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

The school will regularly audit its IT provision to establish if the e-safety policy is adequate and that its implementation is effective.

The E-Safety policy will be regularly updated in line with current legislation when needed and updated annually as part of regular review.

School security

Internet

Bandwidth	300Mbps
Model of firewall	Cisco ASA 5508 running FTD software
Model of CPE	Cisco ISR 4431

Filtering:

LGFL Webscreen – Managed Service by LGFL (latest declaration LGFL/ Adept (2020) that proves that LGFL Websreen complies with KCSIE and counter terrorism law requirements (https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring/provider-responses-0)).

The WebScreen filter system is intended to address the 'Keeping Children Safe In Education' statutory guidance published by the Department for Education, and issued under Section 175 of the Education Act 2002.

Webscreen also addresses the 'Revised Prevent duty guidance: for England and Wales' statutory guidance published by the Home Office, and issued under Section 29 of the Counter Terrorism Act 2015.

Internet access logs are retained for the period of 1 year after the end of the academic year and then disposed of.

Testing

You can check any device is being filtered by visiting http://wsblock.co.uk/ - If you can access this site then the device is not filtered.

Google Safe search: https://www.google.com/safesearch - This can be tested on any computer in the school.

YouTube – . https://www.youtube.com/check_content_restrictions You can check the restrictions forced via IT from any school computer.

Anti-Virus
Sophos Cloud
Sophos cloud is used to provide anti-virus across all our PC, it scans downloaded files and blocks high risk files from being downloaded.

Linden Lodge Virtual School - Staying Safe Online

As part of our Virtual Education offer, we use video and audio-conferencing technology to connect with our students and families. The aim of using this resource is as a professional tool to establish and strengthen levels of engagement, and be used as a method for delivering teaching, learning and holding remote meetings.

Our advice to parents

We advise our parents to ensure a suitable environment is readied for our pupils to undertake the video call, without distractions where possible. We advise our parents to support their child to communicate in an appropriate way during the Skype/Teams/Google Classroom sessions. We state that under any circumstances the communication should not be recorded or distributed. We advise where possible for our families to speak with their child about how to stay safe online using child/young person friendly language. We support our families within this if needed.

Advice to staff using our virtual school

Before the virtual call, we inform the parent/carer of the required information (time, username etc.) and state the nature of the call (e.g. Sensory Story session, Maths session).

During the first session, the member of staff leading the video call will go through the agreement and how to remain safe online with either the child/young person or the adult parent/carer who is working with them. This is referred to at the start of each call to promote e-safety.

There is always more than one member of staff present during any video call. Parent/Carers are also present. The second person introduces themselves on the video call but is only required to observe the session and not interact.

Our staff do not, under any circumstances, record or distribute the online sessions.

If a safeguarding concern is raised during the session, staff have a duty to report it to the Designated Safeguarding Lead immediately.

If anyone in the home is improperly dressed, staff need to alert the parent/carer to this fact and terminate the call until a later time.

After the call, our staff record the contact as appropriate for attendance, content, etc. and email the script to the home learning email address.

Security rules for home working

We understand that there are risks associated in home and remote working that could lead to harm or distress to individuals and cause reputational damage to the school.

As a school we will need to:

- Try not to take hard copy paperwork home unless necessary
- Make a record/log of any paperwork you are taking home
- Email a list of any data (types) are kept of what you take and notify when brought back or shredded/destroyed to colleen.grove@lindenlodge.wandsworth.sch.uk
- Do not take any originals of documents
- If work is taken home, it should be transported securely, i.e.
    - using an encrypted USB or portable hard drive
    - in a locked briefcase
    - not left unattended – even hidden from view - in a car

- Use strong passwords and do not share them with anyone. Our IT team will not ask you for them, so do not share.
- If a password needs to be replaced, this will only be done to school emails or a verified personal contact number/email that we already have on file for you.
- If equipment is taken home that has remote connectivity to the school system, we advise our teams to use log in details that are separate from the machine and teams log off whenever they are not using it
- We advise our teams not leave your computer equipment logged in and unattended
- We advise our teams not connect to a public or unsecured broadband connection to access your school accounts

Home working should be set up:

- In a physical space where family members and visitors cannot see confidential information

- Work that involves data should be locked away securely when not in use