Review Cycle	Two Years
SLT member responsible	JM
Committee	Curriculum
Date adopted	23 01 2018
Review Date	2020

Litcham School Online Safety Policy

Writing and reviewing the Online Safety policy

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

- Ofsted inspectors will always make a written judgement under leadership and management about whether or not the arrangements for safeguarding children and learners are effective.
- The school will identify a member of staff who has an overview of Online Safety, this will be the Designated Safeguarding Lead (DSL).
- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior leadership and approved by governors.
- The Online Safety Policy and its implementation will be reviewed annually
- It was approved by the Governors on: 23 01 2018
- Date of next review: 2020

Contents

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Litcham School with respect to the use of technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of Litcham School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school technologies, both in and out of Litcham School.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/staffroom and the shared drive.
- Policy to be part of school induction pack for new staff, including information and guidance where appropriate
- All staff must read and sign the 'Staff Code of Conduct' before using any school technology resource
- Regular updates and training on online safety for all staff, including any revisions to the policy as and when required especially to cover new emerging threats
- ICT Code of Conduct (previously referred to as an Acceptable Use Policy) discussed with staff and pupils at the start of each year. The ICT Code of Conduct/AUP to be issued to whole school community, on entry to the school.

Handling Concerns

- The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE)
- Staff and pupils are given information about infringements in use and possible sanctions.
- Designated Safeguarding Lead (DSL) acts as first point of contact for any safeguarding incident whether involving technologies or not
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE).

- The online safety policy will be reviewed annually **or** when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the Senior Leadership Team (SLT) and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience
- will remind students about their responsibilities through the pupil ICT Code of Conduct/ Acceptable Use Agreement(s)
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights

Staff and governor training

This school:

- makes regular up to date training available to staff on online safety issues and the school's online safety education program
- provides, as part of the induction process, all staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's ICT Code of Conduct/Acceptable Use Agreement

Parent/Carer awareness and training

This school:

- provides information for parents/carers for online safety on the school website
- provides induction and updates for parents which includes online safety
- parents/carers are issued with up to date guidance on an annual basis

3. Incident management

In this school:

- there is strict monitoring and application of the online safety policy, including the ICT Code of Conduct/AUP and a differentiated and appropriate range of sanctions
- support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police, Internet Watch Foundation) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school

- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the LA

4. Managing IT and Communication System

Internet access, security and filtering

In this school:

- we follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision

- School ICT systems security will be reviewed regularly

Critical Security Control	Questions for School Head Teachers, Senior Leaders and Governors
1. Inventory of Authorised and Unauthorised Devices: Actively manage (inventory, track, and correct) **all hardware devices** on the network so that only authorised devices are given access, and unauthorised and unmanaged devices are found and prevented from gaining access.	Access to the Network for data is for Litcham devices only, or those approved by the Network Manager. Effective network security is in place to allow alternative devices connection to the wireless network for internet access only.
2. Inventory of Software	Litcham school uses Spiceworks and Impero to log software installed on machines. Staff are given a position of trust and responsibility to install additional software required in line with their work requirements. All software is scanned for Viruses on access.
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers: Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	Security settings are set by group policy and cannot be changed by the end user. Devices removed from Litcham school have BitLocker USB devices to prevent unauthorised access in the event of theft. Staff are informed to keep the Bitlocker separate from the device. Laptops have a timed out screensaver on them. All machines require a password to access. All software is upgraded and replaced on a costing/productivity basis when required.

4. Continuous Vulnerability Assessment and Remediation: Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.	E-safety is disseminated to staff via INSET, and/or email communications. Students have curriculum, PSHE, and assembly time dedicated to safety. The e-safety curriculum is updated annually, and immediately if emerging threats come to light. Staff are required to carry out operations they know to be safe, and if any matters arise from using the device that they are unsure of, they are required to seek assistance from the network manager.
5. Malware Defences: Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defence, data gathering, and corrective action.	The systems are all under the ultimate accountability of the headteacher. Any staff member found to be using systems in a malicious manner can expect to be dealt with in line with current legislation, and/or DfE teacher standards. Student malicious misuse – the school can impose a sanction from temporary denial of services, up to any appropriate action deemed necessary by the headteacher in line with current guidance.
6. Application Software Security: Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect and correct security weaknesses	Major upgrades to services are generally implemented out of term time to minimise disruption, unless a security update, which is implemented as soon as possible. Familiarisation of services is provided during INSET where required.
7. Wireless Access Control: The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.	Litcham does not currently operate a BYOD system. Access to Wifi is by obtaining the password from the Network Manager. Access for devices to use the internet, will be granted only if the Virus software is up to date.
8. Data Recovery Capability: The processes and tools used to back up critical information properly with a proven methodology for timely recovery.	MIS data is backed up centrally as part of SaaS contract. Litcham in-house data is backed up daily via an automatic system, and weekly to tape devices, which are removed off-site.

9. Security Skills Assessment and Appropriate Training to Fill Gaps: For all functional roles in the organization (prioritizing those mission--critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defence of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.	The network manager is up to date on training needs, and independently proactive in ensuring his skills are up to the level required to manage the network.
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches: Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	Our ISP manage the Proxy, Router interface to the WAN, including upgrades, maintenance and uptime. LAN side access to all network devices is protected by password.
11. Limitation and Control of Network Ports, Protocols, and Services: Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.	In the event of network changes affecting users, the users will be emailed in advance by the network manager. Litcham does not have access to port management on the interface routers.
12. Controlled Use of Administrative Privileges: The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.	Litcham monitors and modifies its network and password policies regularly to ensure the smooth running of the network.
13. Boundary Defence: Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.	VPN software is provided by FortiNet for staff access, and follows all required encryption levels. Firewall and routers protected via ISP provider schools broadband.
14. Maintenance, Monitoring, and Analysis of Audit Logs: Collect, manage, and analyse audit logs of events that could help detect, understand, or recover from an attack.	Audit logs on web access for staff and students.

15. Controlled Access Based on the Need to Know: The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.	Students are reminded of their responsibilities in lessons, Assembly and Impact days. Staff are reminded annually via the policy, and when new threats emerge.
16. Account Monitoring and Control: Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.	User Data and User Accounts are kept (however disabled from use) for 2 years.
17. Data Protection: The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information (exfiltration: the unauthorized release of data from within a computer system or network)	The school operates and expects its staff to operate in accordance with the Data Protection Act 1998, Information Commissioner's Office and the Teacher Standards.
18. Incident Response and Management: Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.	Isolation can separate network sections that are broadcasting and preventing network access. Other systems to detect problems tend to be reactive rather than proactive.
19. Secure Network Engineering: Make security an inherent attribute of the enterprise by specifying, designing, and building--in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.	Litcham have a team of staff, including School SIG, which work together in partnership with the network manager to consistently improve the services offered to the school. INSET is provided where required to help users with ICT issues.

E-mail

This school

- Provides staff with an email account for their professional use, e.g. @litchamschool.net and makes clear personal email should be through a separate account
- We use anonymous e-mail addresses, for example head@, office@
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law
- Will ensure that email accounts are maintained and up to date

Pupils email:

- We use school provisioned pupil email accounts that can be audited
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home

Staff email:

- Staff will use LA or school provisioned e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff should never use email to transfer staff or pupil personal data unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption

School website

- The school web site complies with statutory DfE requirements
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- Photographs of pupils published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website

Cloud Environments

- All staff and pupils have Office 365 accounts and shared content is managed by the school
- Office 365 documents and VPN access to confidential school documents must have their integrity and security respected. Laptop access must be for designated personnel only, and communications to data remain the responsibility of the employee.

Social networking

- Staff are encouraged to use social media for educational purposes where appropriate, such as Edmodo, YouTube etc. This social media usage must be open and transparent, professional and communications must be in line with this policy, other DfE guidance and Teachers Standards.

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- The use of any school approved social networking will adhere to ICT Code of Conduct/AUP

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our age appropriate pupil ICT Code of Conduct/AUP
- The use of mobile phones is not permitted in school unless specific permission is given by a member of staff for a curriculum activity.

.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through our parental ICT Code of Conduct/AUP and additional communications materials when required.

5. Data Security

Management Information System access and data transfer

- The Litcham School follows guidance from the Information Commissioner's Office to ensure that it complies with its responsibilities to information rights in school

6. Equipment and Digital Content

Bring Your Own Device Guidance for Staff and Pupils

- At present Litcham School does not facilitate a Bring Your Own Device policy.

Digital images and video

In this school:

    - We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school
    - We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs
- Staff sign the school's ICT Code of Conduct/AUP and this includes a clause on the use of personal mobile phones/personal equipment
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use