Lincoln Christ's Hospital School

Online Safety Policy

SLT link member of staff:	**Paul Fragle**
Date presented to SLT:	**September 2022**
Review date:	**September 2023**

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. This policy should be viewed in conjunction with:

- ICT Code of Conduct/Acceptable Use Policy (AUP);
- Social Media Policy;
- Photographic Images of Children Policy;
- Data Protection Policy Incorporating GDPR;
- Freedom of Information Policy.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

<u>Governors</u>
Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor.

The role of the Online Safety Governor will include:

- Regular meetings with the Online Safety Co-ordinator/Officer;
- Attendance at Online Safety Group meetings;
- Regular monitoring of online safety incident logs;
- Reporting to relevant Governors.

<u>Headteacher</u>
The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.

The Headteacher and Designated Safeguarding Lead should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

The Headteacher is responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
The Senior Management Team will receive regular monitoring reports from the Online Safety Officer.

Online Safety Officer

- Leads the Online Safety Group;
- Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents;
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- Provides training and advice for staff;
- Liaises with the Local Authority/relevant body;
- Liaises with school technical staff;
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments;
- Reports regularly to Senior Leadership Team.

Network Manager/Technical staff
The Network Manager is responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack;
- The school meets required online safety technical requirements and any Local Authority Online Safety Policy/Guidance that may apply;
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-and-monitoring).
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- The use of the network is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Officer for investigation;
- Monitoring systems are implemented and updated.

Teaching and Support Staff
Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices;
- They have read, understood and signed the Staff Acceptable Use Policy (AUP). This is displayed and agreed each time a user logs into a PC;
- They report any suspected misuse or problem to the IT Systems Manager who will investigate and inform the Online Safety Coordinator/Officer for further investigation if required;
- All digital communications with students/parents/carers should be on a professional level and only carried out using official school systems;

- Online safety issues are embedded in all aspects of the curriculum and other activities;
- Students understand and follow the Online Safety Policy and acceptable use policies;
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

Designated Safeguarding Lead

Designated Safeguarding Lead should be trained in Online Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data;
- Access to illegal/inappropriate materials;
- Inappropriate on-line contact with adults/strangers;
- Potential or actual incidents of grooming;
- Cyber-bullying.

Students:

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement;
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying;
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will endeavour to help parents understand these issues through various means, which could be parents' evenings, newsletters, letters, the school website, social media channels and information about online safety campaigns. Parents/carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events;
- Access to parents' sections of the website and on-line student/pupil records;
- Their children's personal devices in the school.

Community Users

Community users who access school systems as part of the wider school provision will be expected to follow the AUP before being provided with access to school systems.

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is

therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of SMSC and is regularly revisited;
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities;
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information;
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making;
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school;
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices;
- In lessons where internet use is pre-planned, it is best practice that students 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 students are allowed to freely search the internet, 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 (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities;
- Letters, newsletters, web site, social media;
- Parents/Carers evenings/sessions;
- High profile events/campaigns e.g. Safer Internet Day;
- Reference to the relevant web sites/publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers.

Education – The Wider Community

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents;
- The school website: providing online safety information for the wider community;
- Support for community groups e.g. Early Years Settings, Childminders, and youth/sports/voluntary groups to enhance their Online Safety provision.

Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- LCHS has registered a subscription with National Online Safety. Throughout the year staff, governors and parents will have access to complete a number of online safety courses, webinars and essential and certified training with a national online organisation.
- LCHS is committed to becoming a certified school for online safety through the National Online Safety programme.
- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly;
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school/academy Online Safety Policy and Acceptable Use Agreements;
- It is expected that some staff will identify online safety as a training need within the performance management process;
- The Online Safety Officer will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations;
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings or in INSET sessions;
- The Online Safety Officer will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any subcommittee/group involved in technology/online safety/health and safety /safeguarding. This will be offered in two ways:

- Attendance at training provided by the National Governors Association/or other relevant organisation;
- Complete a range of essential and certified online courses through the National Online Safety programme.
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring

The school is responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements;
- There will be regular reviews and audits of the safety and security of school technical systems;

- Servers, wireless systems and cabling must be securely located and physical access restricted;
- All users will have clearly defined access rights to school technical systems and devices;
- All users will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password;
- An Administrator account will be provided upon request when required. In the event that the IT Systems Manager is unavailable, then the IT Technician can provide the account. In the event that Both IT staff are unavailable (and it is an emergency) F1Group of Lincoln should be contacted.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs);
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the school's web filtering software which uses the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. The Web Filtering system allows users to request an unblock for a site. The unblock request is received by the IT Systems manager and validated. If appropriate, the site is allowed;
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet;
- The school has provided differentiated user-level filtering (allowing different filtering levels for different ages and different groups of users – staff/6th Form students, other students etc.);
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement;
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person. These incidents are reported to the IT Systems Manager who will carry out an initial investigation. If of a serious nature, then this will be passed to the Online Safety Officer for further action;
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software;
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems;
- An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school;
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices. This is done by system administration;
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

<u>Use of digital and video images</u>

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students to instantly use images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for

cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

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

- **Written permission from parents/carers will be obtained before photographs of students are published on the school website/social media/local press** (may be covered as part of the AUA signed by parents/carers at the start of the year - see Parents/Carers Acceptable Use Agreement in the appendix);
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases for protection, these images should not be published or made publicly available on social networking sites, nor should parents/carers comment on any activities involving *other students* in the digital/video images;
- Staff and volunteers are allowed to take digital/video images to support educational aims, 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 when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;
- Students must not take, use, share, publish or distribute images of others without their permission;
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images;
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs;
- Student's work can only be published with the permission of the student and parents/carers.

<u>Social Media - Protecting Professional Identity</u>

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority / MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school:

- Ensuring that personal information is not published;
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues;
- Clear reporting guidance, including responsibilities, procedures and sanctions;

- Risk assessment, including legal risk.

School / academy staff should ensure that:

- No reference should be made on personal social media accounts to students, parents/carers or school staff;
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established, there should be:

- A process for approval by senior leaders;
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff;
- A code of behaviour for users of the accounts, including;
- Systems for reporting and dealing with abuse and misuse;
- Understanding of how incidents may be dealt with under school / academy disciplinary procedures.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy;
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

The school permits reasonable and appropriate access to private social media sites.

Monitoring of Public Social Media

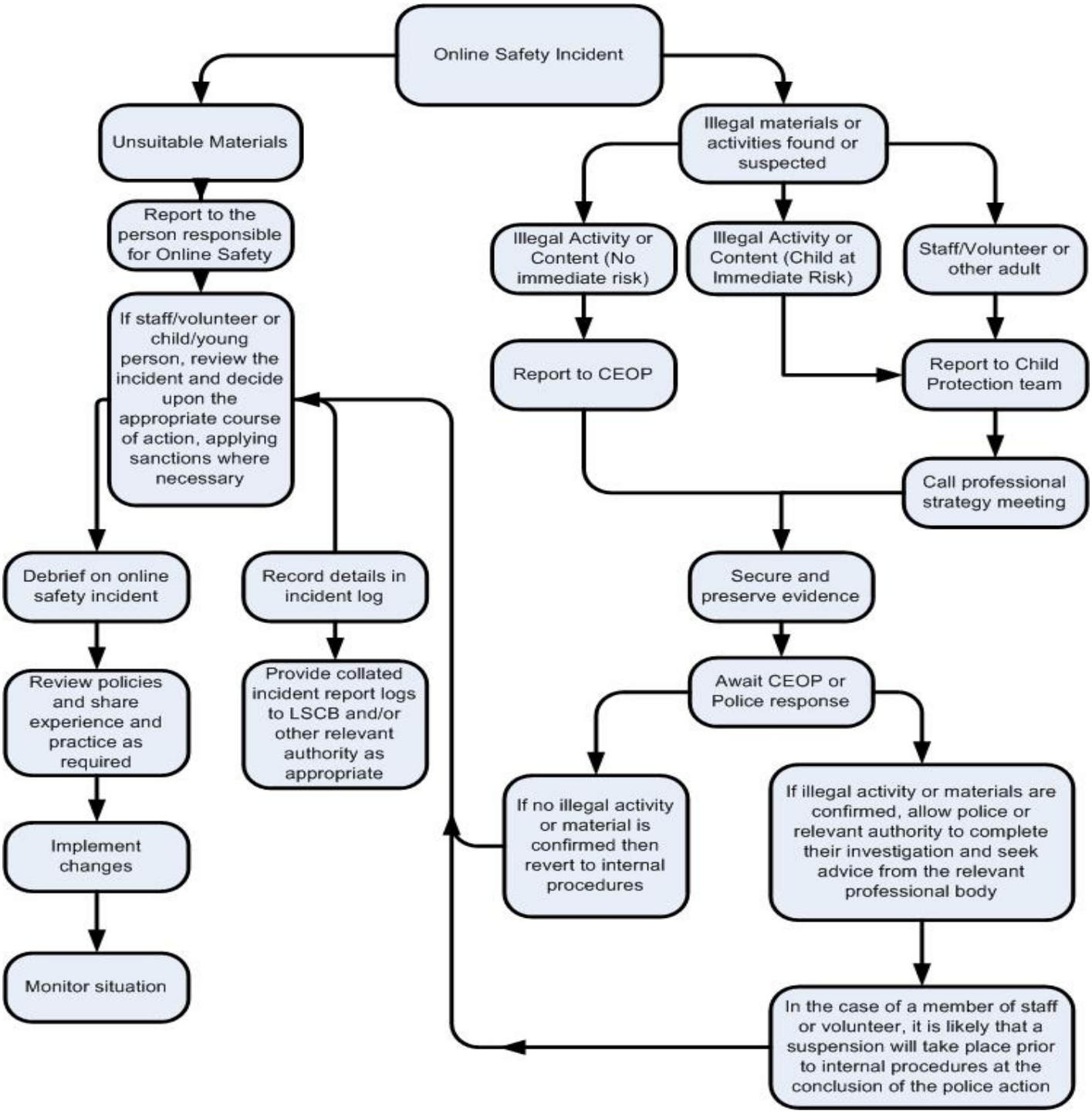
- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school;
- The school should effectively respond to social media comments made by others according to a defined policy or process.

The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Useful Websites:
www.thinkuknow.co.uk
www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org
www.pshe-association.org.uk

educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Reporting Log Group:						
Date	***Time***	***Incident***	***Action Taken***		***Incident Reported By***	***Signature***
			What?	***By Whom?***		