Lovers' Lane Primary and Nursery School

Online Safety Policy

Agreed: December 2023
Review date: September 2024

Lovers' Lane Primary and Nursery School
Online Safety Policy

Introduction

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

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 understand their obligations under the Keeping Children Safe in Education statutory guidance
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problems to the Headteacher or DSLs for investigation.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- they monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- they recognise the warning signs of children at risk of radicalisation or extremism and report in line with Prevent Duty (1st July 2015)
- in lessons where internet use is pre-planned pupils 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.

Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- 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's 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. Parents and 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 / Learning Platform and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils 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. 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 should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils 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.
- Pupils 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.
- Pupils should be helped to understand the need for the pupil 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

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, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference: https://www.gov.uk/government/publications/education-for-a-connected-world

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:

- 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 Online Safety Policy and Acceptable Use Agreements.
- Participation in school / academy training / information sessions for staff or parents
- Staff to be trained to identify behaviour that causes concern that the child is at risk of radicalisation or extremism.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to 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
- 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 IT Co-ordinator who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet
- 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.
- Filtering and monitoring is in place to ensure that children are kept safe from terrorist and extremist material when accessing the internet in school in line with current guidance of the Prevent Duty (1st July 2015)

Filtering and monitoring is managed by Atom IT, who send a 'Safeguarding Daily Internet Blocked Categories Report' to the Headteacher on email each day. This alerts the headteacher to any internet searches which relate to categories relating to KCSIE guidelines. Should a concern arise, it is possible from the report for the Headteacher to identify which class were using the machine at the time and to investigate. This is also the case for staff laptops/ ipads. This is something all children, staff and families (especially during remote learning) are made aware of as part of our safeguarding strategy. All laptops leant to families during remote learning have this filtering and monitoring applied.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.
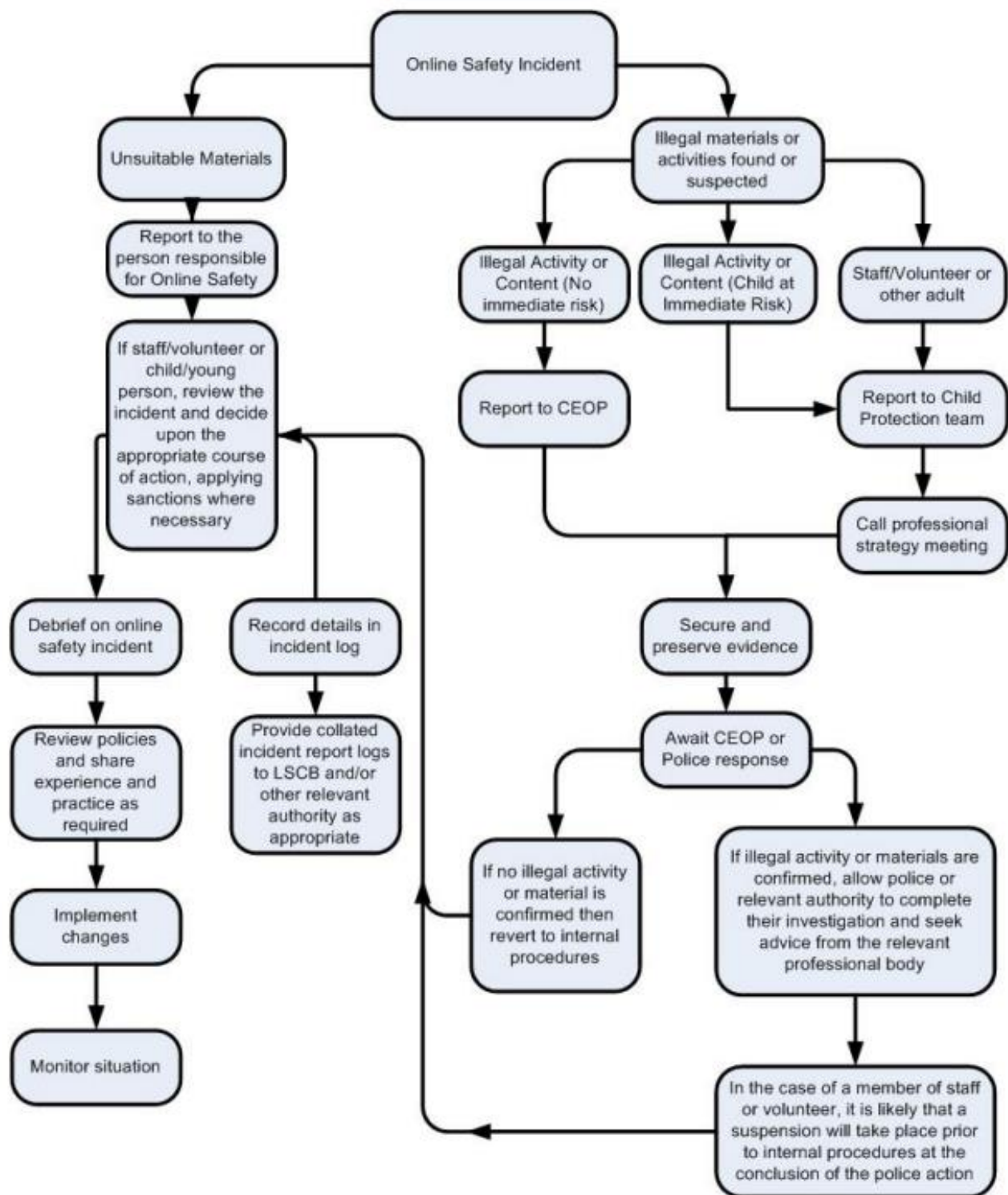
The school allows:

	School Devices		Personal Devices		
	School owned for single user	School owned for multiple users	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes *(locked away during the school day)*	Yes *(subject to acceptable use)*	Yes
Full network access	Yes	Yes	No	No	No
Internet only		Yes	No	Yes	No

Use of digital and video images

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

- When using digital images, staff should inform and educate pupils 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 or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school academy 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Responding to incidents of misuse – flow chart

```
                        ┌─────────────────────┐
                        │ Online Safety Incident │
                        └─────────────────────┘
          ┌──────────────────┘           └────────────────────┐
          ▼                                                    ▼
┌──────────────────┐                              ┌──────────────────────┐
│ Unsuitable Materials │                          │ Illegal materials or   │
└──────────────────┘                              │ activities found or    │
          │                                       │ suspected              │
          ▼                                       └──────────────────────┘
┌──────────────────┐              ┌───────────────┼─────────────────────┐
│ Report to the      │            ▼               ▼                     ▼
│ person responsible │   ┌──────────────┐ ┌──────────────┐ ┌──────────────┐
│ for Online Safety  │   │ Illegal Activity │ │ Illegal Activity │ │ Staff/Volunteer or│
└──────────────────┘   │ or Content (No   │ │ or Content (Child │ │ other adult      │
          │            │ immediate risk)  │ │ at Immediate Risk)│ └──────────────┘
          ▼            └──────────────┘ └──────────────┘        │
┌──────────────────┐          │               │                ▼
│ If staff/volunteer │         ▼               │        ┌──────────────┐
│ or child/young     │  ┌──────────────┐        └───────▶│ Report to Child│
│ person, review the │  │ Report to CEOP │               │ Protection team│
│ incident and decide│  └──────────────┘               └──────────────┘
│ upon the           │         │                               │
│ appropriate course │         │                               ▼
│ of action, applying│         │                       ┌──────────────┐
│ sanctions where    │         │                       │ Call professional│
│ necessary          │         │                       │ strategy meeting │
└──────────────────┘         │                       └──────────────┘
     │           ▲            │                               │
     ▼           │            ▼                               ▼
┌──────────┐  ┌──────────┐  ┌──────────────┐       ┌──────────────┐
│ Debrief on │  │ Record    │  │ Secure and    │       │ Secure and    │
│ online     │  │ details in │  │ preserve      │       │ preserve      │
│ safety     │  │ incident   │  │ evidence      │       │ evidence      │
│ incident   │  │ log       │  └──────────────┘       └──────────────┘
└──────────┘  └──────────┘         │
     │           │                 ▼
     ▼           ▼          ┌──────────────┐
┌──────────┐ ┌──────────┐   │ Await CEOP or │
│ Review     │ │ Provide   │  │ Police response│
│ policies   │ │ collated  │  └──────────────┘
│ and share  │ │ incident  │    ┌────┘    └────┐
│ experience │ │ report    │    ▼              ▼
│ and        │ │ logs to   │ ┌──────────┐ ┌──────────────────┐
│ practice as│ │ LSCB and/or│ │ If no     │ │ If illegal activity │
│ required   │ │ other     │ │ illegal   │ │ or materials are    │
└──────────┘ │ relevant  │ │ activity  │ │ confirmed, allow    │
     │       │ authority │ │ or material│ │ police or relevant  │
     ▼       │ as        │ │ is        │ │ authority to        │
┌──────────┐ │ appropriate│ │ confirmed │ │ complete their      │
│ Implement  │ └──────────┘ │ then revert│ │ investigation and   │
│ changes    │             │ to internal│ │ seek advice from    │
└──────────┘             │ procedures │ │ the relevant        │
     │                   └──────────┘ │ professional body   │
     ▼                                └──────────────────┘
┌──────────┐                                    │
│ Monitor    │                                    ▼
│ situation  │                          ┌──────────────────┐
└──────────┘                          │ In the case of a   │
                                        │ member of staff or │
                                        │ volunteer, it is   │
                                        │ likely that a      │
                                        │ suspension will    │
                                        │ take place prior   │
                                        │ to internal        │
                                        │ procedures at the  │
                                        │ conclusion of the  │
                                        │ police action      │
                                        └──────────────────┘
```

Appendices

Staff (and Volunteer) Acceptable Use Policy Agreement

Acceptable Use Policy Agreement

- I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.
- I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology.
- I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
- When I use my personal mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use.
- I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I understand that I may not use personal electronic devices when children are present and I must never take or store images of children on a personal device.
- I will not use personal email addresses on the school / academy ICT systems.

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of the school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology
- equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name:

Signed:

Date:

Pupil Acceptable Use Agreement KS1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computing equipment in school (this includes laptops and iPads).
- I will only use websites, applications (apps) and software that a teacher or suitable adult has told or allowed me to use.
- I will follow all instructions given to me by a teacher or responsible adult.
- I will take care of the computing equipment so that it is available for others to use.
- I will ask for help from a teacher or suitable adult if I am not sure what to do.
- I will ask for help from a teacher or suitable adult if I think that there is something wrong or I have accessed something by mistake.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I will treat everyone fairly and with respect when communicating with them online
- I understand that people I do not know are strangers on the internet and I must not share my own, or anybody else's personal information (this includes names, date of birth, email, address, school name).
- I will keep all passwords safe and not share them with anyone else.
- I know that if I break the rules I may not be allowed to use the computer equipment and if necessary further action may be taken.

Pupil Acceptable Use Agreement KS2

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computing equipment in school (this includes laptops and iPads).
- I will only use websites, applications (apps) and software that a teacher or suitable adult has told or allowed me to use.
- I will follow all instructions given to me by a teacher or responsible adult.
- I will take care of the computing equipment so that it is available for others to use.
- I will ask for help from a teacher or suitable adult if I am not sure what to do.
- I will ask for help from a teacher or suitable adult if I think that there is something wrong or I have accessed something by mistake.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I will treat everyone fairly and with respect when communicating with them online and understand that cyberbullying is not acceptable.
- I understand that people I do not know are strangers on the internet and I must not share my own, or anybody else's, personal information (this includes names, date of birth, email, address, school name).
- I will keep all passwords safe and not share them with anyone else.
- I understand that the use of computers in school is digitally monitored and any attempts to access websites, software or applications will be reported.
- I understand that I must only download digital content that I have permission to use this includes pictures and videos from websites.
- I know that if I break the rules I may not be allowed to use the computer equipment and if necessary further action may be taken