Online Safety Policy

Statement of intent
This policy is intended to ensure pupils at Livingstone Primary School are protected while using digital technologies at the school. The school is committed to including digital technologies, in particular, internet use, in our curriculum. In so doing we recognise the inherent risks posed by this useful learning tool. Full compliance with this policy will mitigate these risks and help to ensure pupils are safe online.

Introduction
New technologies have become integral to the lives of children at our school and young people in today's society, both within schools and in their lives outside school. While digital technology and the internet provide an exciting opportunity for children to learn and interact with various subjects, they also pose a risk for children, with the potential for exposure to inappropriate content and inappropriate contact from other children and adults. Digital technology also provides an opportunity for pupils to engage in unacceptable behaviour, both online and offline.

In order to keep pupils safe online, and for them to learn how to keep themselves safe online, all pupils and teachers should be aware of relevant skills and strategies needed to ensure online safety. (This may range from knowing to only use the internet with adult supervision for younger pupils, to strategies for identifying appropriate links for older children.)

Mitigating the risk to children created by digital technology and the internet will be ensured through specific safety lessons and will also be embedded within the general curriculum. We consider that the advantages far outweigh the risks involved so long as users are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.

Online safety will depend on policies being properly implemented at all levels of the school community: from published policies, to a secure school network design, the effective management of school broadband and filtering and monitoring systems, parental awareness of the dangers of online use and effective teaching about digital-technology use.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This policy is to work in conjunction with our behaviour and anti-bulling policy, child protection and safeguarding policy, Prevent Duty policy and Acceptable Use Procedures.

Aims
At Livingstone Primary School, we are committed to using the internet and other digital technologies to:

- Make learning more exciting and interactive.
- Make lessons more varied.
- Enable pupils to gain access to a wide variety of knowledge in a safe way.
- Raise educational standards.
- Support children to develop their reading and research skills.
- Prepare our pupils for using the internet safely outside of school and throughout their education.
- Equip children with skills for the future.
- Foster good social and communication skills.
- Teach computing skills as required by the curriculum

Definition
Digital safety encompasses a number of technologies such as computers, tablet computers, internet technologies and mobile devices.

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils 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 out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate online behaviour that take place out of school. We will also deal with any matters that could be seen as involving sexual harassment or sexual violence. Livingstone School is proactive in the education of pupils in regard to establishing what bullying is and providing advice and guidance to parents, encouraging them to take responsibility for their children's online activities**.** We also ensure that teaching about child-on-child abuse or harassment is part of our online safety and PSHE curriculum in order to give children an understanding of how to act and what to do if something makes them feel uncomfortable.

Access to inappropriate websites, blogs and forums are a child protection issue and any staff who believe children have had access to these (whether this is linked to CSE, radicalisation and extremism or any other safeguarding issue) will inform the lead safeguarding professional (the Headteacher).

Roles and Responsibilities
Governors:

- 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 where necessary.
- Governors are responsible for ensuring that there are appropriate filtering and monitoring procedures in place to block access to inappropriate sites and harmful content
- Governors will ensure that the appropriate staff training is delivered and that the schools' approach to online safety is reflected in all relevant policies and procedures.
- Governors will sign the Acceptable Use Policy / Agreement (AUP) on joining the Governing Body as they use a school email account to access Office 365.
- If Governors have a device stolen on which they normally access Governing Body paperwork and emails, they are expected to inform school immediately who will reset their password thus blocking unauthorized access on the device.
- In extreme circumstances, the contents of the shared Office 365 drive can be deleted by the ICT SLA provider.

Headteacher and Senior Leadership Team:

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community whilst in school, though the day to day responsibility for online safety will be delegated to the ICT SLA provider / Computing Leader.
- The Headteacher is responsible for ensuring that the ICT SLA provider / Computing Leader and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant

- The Headteacher and 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.
- In the case of an allegation against the Head or the Safeguarding Lead, another member of the Senior Leadership Team will be asked to follow procedures. Please see policy on Managing Allegations of Abuse Against Staff for further guidance.
- The SLT must be aware of the procedure to be followed when there has been an online safety incident reported to school that has happened at home.
- The SLT are responsible for procuring appropriate filtering and monitoring software to ensure that access to harmful and inappropriate content is blocked whilst not interrupting teaching and learning.
- The SLT are responsible for documenting the sites and areas that are blocked and why.
- The SLT are responsible for reviewing the effectiveness of the filtering and monitoring at least annually and making changes as deemed necessary.
- The Headteacher is responsible for providing reports to the Governing Body on the effectiveness of filtering and monitoring.
- The Headteacher is responsible for ensuring staff understand their role in implementing the online safety (including filtering and monitoring) procedures

ICT SLA provider:

- take day to day responsibility for online safety issues
- provides training and advice for staff
- liaises with the Local Authority and filtering providers
- Maintain and monitor filtering systems
- Advise and support the DSL when an alert has been received to support them as to appropriate action and identification of the user.
- Test the filtering system on a termly basis
- Advise the DSL and computing lead when changes are needed to the filtering and monitoring system in place.

Internet Provider

- Maintains internet filtering and blocking of inappropriate websites
- Screens the blocked websites and contacts school urgently if anyone has attempted to access a concerning site.

DSL / Safeguarding team

- receives reports of online safety incidents and creates a log of incidents, should they occur, to inform future online-safety developments eg. Websites that need to be blocked
- Responds to notification from the internet provider that an inappropriate website has been attempted to be accessed.
- Liaises with IT SLA provider to deal with the notification which may include working out next steps, identifying the user and discussing the issue with the staff member or child.
- Dealing with and supporting staff when incidents of child-on-child abuse, sexual harassment, and sexualised language are reported.
- Dealing with online safety incidents that have a safeguarding element that have happened at school or at home.
- should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials (including those expressing extremist views)
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming
    - cyber-bullying
    - Sexual harassment and sexual language

- Child-on-child abuse

Computing Lead

- Liaises with the DSL. HT and ICT SLA provider about the filtering and monitoring procedures.
- Plans the teaching of online safety across the school.
- Supports and trains classroom staff to deliver the online safety sessions in the classroom.
- Attends training to ensure that they are aware of the up-to-date risks and harms
- Receives the weekly monitoring reports and checks them, liaising with the HT and the ICT SLA provider if there is something of concern.

Office

- Requests sites to be unblocked if access is appropriate and is needed.
- Responds to notification from the internet provider that an inappropriate website has been attempted to be accessed from a pupil login if the DSL is not available – takes down the information to pass on at the soonest possible opportunity.

Teaching and Support Staff are responsible for ensuring that:

- report any suspected misuse or problem to the Headteacher / Senior Leader / Computing Leader / Class teacher for investigation as appropriate.
- Report any attempt to access extremist material to the DSL as a safeguarding issue
- Ensuring that Chrome book users are allocated a chrome book and the number they use is always the same and recorded so that the user responsible for attempting to access harmful or inappropriate material can be identified.
- Monitoring Chromebook usage in lessons and co-curricular activities
- Responds if the office / DSL contacts them with notification of an inappropriate site being accessed by tracing which child has attempted this and taking further action as needed.
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they have an up-to-date awareness of online safety matters and of the current school online safety policy
- digital communications with students / pupils (email / blogging / messaging / voice) 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 school activities
- Online safety lessons are taught as planned by the computing lead
- Dealing with any online safety issues that have been brought to their attention that do not require the DSL / SLT. This may include any reports of child-on-child abuse, sexual harassment or sexual language
- Logging all online safety incidents in the online safety file including actions taken and the resolution provided where appropriate. It may include advice given to parents on digital safety.
- Ensuring appropriate search engines are used as advised by the computing lead and appropriate to the age of the children.
- Reminding children of the filtering and monitoring in place and that they will be identified if they attempt to access inappropriate content
- Ensuring all mobile devices belonging to children are signed in and locked away during the school day.
- Ensuring that they themselves meet the guidelines of the online safety policy (which includes the use of mobile phones, cameras and other hand held devices) and ensuring that their activities outside of school do not bring the reputation of the school or individuals within the school into disrepute.
- Not connecting their personal devices to the school network.

Students / pupils: pupils understand and follow the school e-safety and acceptable use policy

- pupils have a good understanding of research skills and how to stay safe on the internet
- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy.
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying (in particular KS2).
- 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

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings / information sessions, newsletters, letters, website and information about national / local e-safety campaigns / literature.

Parents and carers will be responsible for:

- endorsing the Student / Pupil Acceptable Use Policy
- accessing the school website in accordance with the relevant school Acceptable Use Policy.
- Acting on the advice and information provided by school to have discussions about online safety with their children

OnlineSafety Education – students / 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 provision. Children and young people need the help and support of the school to recognise and avoid online risks and build their resilience.

Online Safety education will be provided in the following ways:

- Online safety should be provided as part of Computing / PHSE and other relevant lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Pupils should be taught in 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 helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Curriculum:

Online safety should be a focus in all areas of the curriculum and staff should reinforce messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use
- Where pupils are allowed to freely search the internet, eg using search engines, they are actively taught safe practice on internet search engines before use.

Search engines selected should be appropriate to the age of child according to the plan for progression.

- Pupils should be taught in lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils are taught about appropriate and not appropriate behaviour online. This occurs via planned series of lessons and also as impromptu learning if and when incidents occur.

Online safety Education – parents / carers

Many parents 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 online experiences.

Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The school will therefore seek to provide information and awareness to parents and carers through:
- Letters, newsletters, and website
- Parents' evenings / parent information sessions
- Reference to the CEOP / childnet / other internet safety materials

Online safety Education & Training – Staff
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 online safety training will be made available to staff through formal INSET and staff meetings.
- All new and existing staff should sign to agree they fully understand the school online safety policy and Acceptable Use Policies

Online safety measures
- The school's internet system, and access to it, is specifically designed for staff and pupil use and, as such, includes filtering appropriate for primary age children. This filtering system is applied to the school network to stop any user accessing inappropriate websites. Staff have all been trained in the Prevent Duty and regard potential radicalisation as a safeguarding issue. As with all safeguarding issues, if they become aware of children accessing websites which contain an extremist point of view (wherever this has happened), they should report the matter to the designated safeguarding professional (the Headteacher).
- Pupils will have clear objectives about why they are using the internet whenever the internet is incorporated into lessons.
- Lessons using the internet will be carefully planned and the 'access levels' classes and pupils are afforded will be fully considered, taking into account pupil age and curriculum requirements. The search engines will be chosen appropriately for the age of child.
- Children using the internet will do so in classrooms (or other appropriate shared areas of the school) during lesson time only and with teacher supervision.
- Classroom staff will monitor all use of the Chromebooks.
- Pupils will be taught what internet use is acceptable / unacceptable and teachers should be vigilant during internet based lessons.
- Online safety is a planned part of the computing curriculum as well as pupils being regularly reminded about procedures.
- Before allowing children to search on line as part of a lesson, staff should know which results are likely to come up in a search and be familiar with the content of the websites.

Procedures for Use of a Shared School Network
- Users must access the school network using their logons and passwords. These must not be disclosed or shared.
- Children using the Chromebooks must be allocated a numbered device and always use the same one so that users can be identified. Classes must log on with the correct colour log in
- Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.
- Software installed or programmes downloaded from the Internet should only be installed or downloaded from a respected source and after consultation with the ICT SLA provider.
- Removable media are not to be used. Instead staff can use Hamachi or the One Drive to be able to work remotely.
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer'). Machines must be 'logged off' correctly after use. Children must be taught to close all tabs and log off correctly at the end of a lesson.

Procedures for Use of the Internet and Email

- Pupils, governors and staff must sign an Acceptable Use Agreement before access to the Internet and email is permitted in the establishment.
- The school's internet system has a firewall and all appropriate filters that are maintained by the internet service provider. Staff have all been trained in the Prevent Duty and regard potential radicalisation as a safeguarding issue. As with all safeguarding issues if they become aware of children accessing websites which contain an extremist point of view (wherever this has happened), they should report the matter to the designated safeguarding professional (the Headteacher).
- The security of the school's information systems and ICT system capacity will be reviewed regularly.
- Users must access the Internet and email using their own logon / password and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's email account.
- The Internet and email should only be used for professional or educational purposes in directed time. Only approved school email accounts may be used at school / via the school network. Any other use, for example, the use of school email for personal reasons in an emergency, must be discussed and agreed with the Head Teacher.
- Children must be supervised at all times when using the Internet.
- Pupils should be taught about the dangers involved in online communications. They should be taught:
    - Not to reveal personal details about themselves or others. This will generally include full names, addresses, mobile or landline phone numbers, school name, IM (instant messenger) address, e-mail address, names of friends, specific interests and clubs etc.
    - Never to arrange to meet someone they have 'met' online without appropriate safeguarding measures (e.g. the presence of a parent or responsible adult).
    - That online communications are 'real' and as such require the same respect for others as face-to-face interactions.
- Accidental access to inappropriate, abusive or racist material is to be reported without delay to the technician or Headteacher and a note of the offending website address (URL) taken so that it can be blocked.
- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly.
- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- If users are bullied, or offensive emails are received, this must be reported immediately. Emails received should not be deleted, but kept for investigation purposes.
- Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.
- All email attachments must first be scanned before they can be opened. Attachments received from unknown senders or attachments whose content is not outlined in the body of an email should be deleted.
- Teachers should only download files from a reliable source; pupils should <u>never</u> download files from the Internet.
- All users will be made aware of copyright law and will acknowledge the source of any text, information or images copied from the Internet.

Procedures for the use of Office 365

- Office 365 is predominantly used by the Governing Body or the Senior Leadership Team to work jointly on documentation and store paperwork for meetings.
- Teachers can also store their files on One Drive so that they can access them from home.
- This is accessed through logging on with a school email address.

- In the event of devices being lost / stolen, the IT SLA provider is able to reset the login to Office 365 and thus prevent unauthorized access.
- If a Governor loses or suffers the theft of a device on which they have been accessing their school emails and documents, they are expected to notify the school immediately.

Procedures for Use of Instant Messaging (IM), Chat and Weblogs

- The use of Instant Messaging (e.g. MSN messenger) is not permitted by any user, whether pupil or staff.
- Use of Social Networking websites, such as Bebo, MySpace, Facebook, Habbo, and Piczo is not permitted by any user, whether pupil or staff.
- Staff or pupils using social networking sites outside school hours should be aware that the posting of any defamatory or inappropriate comments could lead to disciplinary action. Disciplinary action can also result from the sending of inappropriate text messages or from sending repeated messages which could cause disturbance or harassment.
- Parents and pupils alike should both be informed of the risks inherent in using social media.

Procedures for Use of Cameras, Video Equipment and Webcams

- Any photographs or video footage stored must be deleted immediately once no longer needed.
- School devices are the only ones that may be used to take images of children. These images must be downloaded onto the server as soon as possible and deleted from the device. Images taken to evidence practical learning should be printed as soon as possible and deleted from the device. All images should be taken for educational purposes or wider school use.
- Video conferencing equipment and webcams must be switched off (disconnected) when not in use.
- Webcams must not be used for personal communication and should only be used with an adult present.
- Children and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

The school website

- The headteacher has overall responsibility for the content of the school website. This includes ensuring all content is appropriate and accurate. Procedures should be in place for authorising the uploading of any content onto the school's website.
- No personal information or the contact details will be published on the school's website. This extends to the use of pupil's full names. The school address, email and main telephone number should be the only contact information available to website visitors.
- The uploading of any images or photographs of pupils onto the school website requires parental permission in writing. Any images should be carefully chosen with safeguarding in mind. Pupil's names should never be used in conjunction with their photograph on the website. Parents can request at any point that images of their child are removed.
- The school website should be subject to frequent checks by the Head teacher to ensure that no material has been inadvertently posted, which might put children / young people or staff at risk.
- Copyright and intellectual property rights must be respected.
- When photographs of children for the website are saved, names of individuals portrayed therein should not be used as file names**.**

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary

- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Do not use removable devices such as USB sticks.

Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Then the incident will be referred to the police.

If any apparent or actual misuse appears to involve activities which involve access to extremist or terrorist views and potential radicalisation then the incident must be referred to the Designated Safeguarding Lead (the Headteacher). From 1 July 2015 all schools, registered early years childcare providers and registered later years childcare providers are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent duty. It applies to a wide range of public-facing bodies. Bodies to which the duty applies must have regard to the statutory guidance. The headteacher will work with the LSCB as appropriate and may make a referral to the Channel programme. Channel is a programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. It provides a mechanism for schools to make referrals if they are concerned that an individual might be vulnerable to radicalisation. An individual's engagement with the programme is entirely voluntary at all stages.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

- Complaints regarding pupil misuse of the school's internet / digital devices will be dealt with by the headteacher and an appropriate, senior member of staff. Sanctions for misuse may include:
  - Revocation of internet use privileges.
  - Communication with the pupil's parents / carers.
  - Detention or other usual sanctions.
  - Details may be passed on to the police in more serious cases.
  - Legal action may be taken in extreme circumstances.
- Staff misuse of the internet or digital technology should be referred to the headteacher. This may be logged as a 'low-level concern' if it is not deemed to reach the safeguarding threshold. If more serious it could be investigated and lead to disciplinary action.
- Any issues or complaints of a child protection nature should be dealt with according to the school's child protection / safeguarding policy procedure.

- Information on the complaints procedure should be published on the school's website and parents should be informed about this.
- Cases of misuse will be considered on an individual basis by the Head Teacher and sanctions will be agreed and imposed to 'fit the crime.'

Digital technology/internet use outside of school

- Parents should be informed of the inherent risks of internet use.
- The school will be aware of and responsive to any issues pupils experience via their use of the internet or digital technology outside of school. The school's bullying policy may also be relevant in such instances.
- The school will have a zero tolerance approach to any reports of sexual harassment or peer on peer abuse and will deal with each matter thoroughly and as appropriate to each matter.

Use of online learning platforms

The school uses the Seesaw app to set homework online or to share home activities and wow moments in the EYFS. We expect children and parents to respond on the online learning platform appropriately at all times.

Monitoring

- This policy should be monitored and updated to account for changes in the legal landscape such as amendments to the outlined laws. The headteacher is responsible for updating this policy and ensuring the school remains in compliance with its legal obligations.

Concluding Statement

The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into the school and therefore this policy will not remain static. It may be that staff/children might wish to use an emerging technology for which there are currently no procedures in place. The use of any emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates.

Because of the frequently changing nature of this area, this policy will be reviewed annually.

Simon Wilde
Vice-chair of Governors
25th September 2023