Technology Policy

Hardware, Software and Internet ~ Acceptable Use

Lisburne's aim is to provide quality inclusive education for all pupils and access to the full range of National Curriculum subjects in a safe, caring environment where all achievements are valued and celebrated.

Lisburne School is committed to Safeguarding, promoting the welfare of all its pupils and to protecting them from the risks of harm. The Governors expect all staff, students and volunteers to share this commitment by demonstrating their understanding of how each individual adult working on behalf of the school has an active part to play in protecting children from harm and promoting their welfare.

As part of Lisburne's commitment to safeguarding and child protection we fully support the government's Prevent Strategy.

We aim to fulfill the Prevent Duty by protecting our pupils from harm and to ensure they are taught in a way that is consistent with the law and British Values. We aim to: raise awareness, enable learners to make a positive contribution and safeguard the wellbeing of our children.

Policy agreed by GB on	September 20
Policy shared with staff on	September 20
Policy up-dated	March 2022

Aim

To have a clear policy on the acceptable use of computing hardware, software and internet at Lisburne school. Hardware includes mobile phones, portable devices, cameras and wearable technology that is understood and adhered to by all parties concerned without exception. To ensure that this technology can be used safely to improve the quality of learning, by enhancing what is already being done at school and at home

This policy recognises that all digital images of children and individuals and personal information is subject to GDPR regarding the rights of individuals to have information of a personal nature treated in an appropriate way and the privacy of individuals and families is protected.

Lisburne School is committed to safeguard and promote the welfare of children and young people and expects all members of the school community to share in this commitment. This policy will help to define appropriate and acceptable use by both staff and pupils.

Included within this policy you will find definitions and expectations regarding the acceptable use of

0.1 ~ Personal Equipment e.g. mobile phones, wearable devices, portable devices, pupils equipment

0.2 ~ Resources for home learning

0.3 ~ Photography - Cameras and IPads, Class DOJO and Tapestry, School Performances, Photographs of Staff

0.4 ~ IPads

0.5 ~ Internet Usage

0.6 ~ Website

0.7 ~ E-mail

0.8 ~ Social Media

0.9 ~ YouTube

0.1 ~ Personal Equipment

Mobile Phones
Lisburne School allows staff to bring in personal mobile phones for their own use. All staff must ensure that their mobile phones are left inside their bag, staff bags should be placed in a secure place within the classroom or staff room.

Personal mobile phones must not be used within the school building, with the exception of the staff room and office, this includes staff, parents or other professionals.

Mobile phone calls may only be taken at staff breaks or in staff members' own time. If staff have a personal emergency they are free to use the school's phone or make a personal call from their mobile in the office or the staff room. If any staff member has a family emergency or similar and need to

keep their mobile phone to hand, prior permission must be sought from the head teacher or deputy head teacher. It is the responsibility of each member of staff to ensure their families, children's schools etc. have their work emergency contact telephone numbers. Staff also need to ensure that the head teacher/school office has their up to date mobile phone numbers.

All students, volunteers, work experience and parent/carer helpers are required to place their bag containing their mobile phone in a secure area within the classroom or staff room and asked to take or receive any calls in the staff room or office.

During group outings, staff will endeavour to use a mobile phone provided by school. If for any reason this is not possible, staff are permitted to use personal mobile phones for group life-skills, only where another member of staff is also present. Phones must only be used in the case of an emergency and under no circumstances are the cameras on personal phones to be used. If children require toileting while on life-skills, all phones must be left outside the bathroom area. Members of staff should not use their own mobile phone to contact a current pupil or parent/carer during emergencies or at any other time without withholding their number by dialling 141 before calling.

Users bringing mobile phones and portable devices into school must ensure there is no inappropriate or illegal content on the device. It is the responsibility of all members of staff to be vigilant and report any concerns to the head teacher. The class teacher, in the absence of the head teacher reserves the right to check the image content of a member of staff's mobile phone or portable device. Concerns will be taken seriously, logged and investigated. Should inappropriate material be found then the Child Protection Officer will be contacted immediately. We will follow the guidance from the Local Authority as to the appropriate measures for the staff member's dismissal.

Wearable Devices
Lisburne School allows the wearing of 'wearable devices' e.g. Smart Watches that have the capacity to take photographs, however, it is the expectation that whilst in contact time with Lisburne children both within and outside of the school environment this facility be disabled. This also applies to apps on their 'wearable devices' that could compromise the safety of the children e.g. 'Walkie Talkie' that allows others to pinpoint exact locations and listen in to conversations.

Portable Devices
Lisburne school allows staff to bring in portable devices (e.g. iPads and other tablets) for their own use and may be used within school for personal use related to work e.g. as a diary. Portable devices must not be used as a camera within or outside the school working environment during contact time with Lisburne children. Portable devices must not be used to access social media within the school environment or when taken out of the school during contact time with Lisburne children.

Pupils Equipment
In some cases pupils may bring personal portable devices into school to support the transition from home to school, or for communication and learning.
In the case of transition aids, on arrival at school devices should be stored safely within the classroom and should remain stored until the children are transitioning home at the end of the day.
As a communication/learning aid, devices must only be used for the specified purpose.

0.2 ~ Resources for Home Learning

Where children's learning has been affected by COVID 19 and children are required to learn from home, the school has access to 5 laptops and 18 IPads which can be sent home for individuals to support home learning.

Before any device is sent home, a 'Home User Agreement for Online Devices' must be read and signed by a parent or carer. Devices are to be used for educational purposes only must not be used to access content that is deemed to be inappropriate.

0.3 ~ Photography

Cameras/iPads
As a school we recognise that images of children can increase motivation, moral and help parents and the local community celebrate the life of the school. Photographs are also used as part of the assessment process within school. We also recognise that to protect the rights of children and to safeguard them, photographs and digital images must be used in a responsible way.

School Cameras/iPads must be used at all times both within and outside of the school environment for the purposes or recording evidence of a child or children. Photographs are taken for the purpose of recording evidence of children participating in activities, showing progress made or celebrating achievements. At no time will staff use personal devices to take photographs of children. Parents/carers will be given permission to take photographs of their own child at e.g. school performances or sports day, this will be granted by the head teacher or deputy head.

If there is a need to take photographs in toilets, e.g. photographs of the children washing their hands, then the class teacher must be informed and the activity will be carried out with two members of staff present.

All staff are responsible for the location and maintenance of the cameras/iPads ensuring that they are stored appropriately and downloaded regularly. All photographs must be stored appropriately on site. Images will be stored until children leave the school. At the end of the summer term photographs will be removed from the server and saved on secure hard drive on site.

Parental consent will be obtained when children join the school and on an annual basis after this as part of the September record update. Parents will be advised that they can change their decision about the use of photographs at any time. Where children are subject to a court order or where parents have refused permission images will not be taken.

Images of children will always be in suitable dress. Where photographs are taken of children in PE kit the focus will be on the activity and not the children.

Class DOJO and Tapestry
Photographs are used on Dojo and Tapestry to share pupil progress with parents and carers, these apps are password protected. Parents and carers will sign an agreement with the school, prior to

accessing Tapestry or Dojo, to confirm that images will be accessed for personal use only, images will not be downloaded or shared on any social media website or any other public forum.

<u>School Performances</u>
Parents are not permitted to take any photographs or videos of school productions/assemblies/ performances. Only when full permission has been obtained for all children may photographs or videos be taken of school productions. The school will make a copy of school productions and make this available for parents. Parents are invited to stay after the performance/ assembly to take photographs of their own children.

<u>Photographs of Members of Staff</u>
All members of staff must wear an ID badge with a recent photograph as part of the school security system. The school respects the rights of members of staff who do not wish their photograph to be used on the school web site, for publicity or as part of displays.

0.4 ~ IPads

IPads must be treated with care. Screens are made of glass and therefore can be cracked or broken by misuse. IPads must remain in the case provided at all times. Staff should avoid placing other items on top of the iPad or dropping it.   IPad's must be kept away from food, drink or other liquids. Screens cleaned with a soft cloth. IPads should not be subjected to extremes of high or low temperatures. When charging the iPads, staff must take care inserting and removing the cable to avoid damaging it or the iPad.   All iPads are monitored and can be tracked and remotely locked/wiped by the school.

0.5 ~ Internet Usage

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught the importance of cross-checking information before accepting its accuracy, as well as how to report unpleasant Internet content. Parental permission will be sought before any pupils are allowed Internet access

The class teacher will take responsibility for developing pupil research skills including the effective, reasonable and legal use of information retrieved i.e. copyright and for moving the children in their class on to their next target as they develop and refine these skills. The Internet will be integrated into learning activities in all subject areas at Key Stage 1 and Key Stage 2. The staff will monitor Internet use through planning and assessment. The school is able to block any site they don't want accessed.

Some of the information to be found on the Internet may be inappropriate for pupils. Management has a duty to ensure that before using the Internet with pupils, the staff have had the opportunity to discuss how they will deal sensitively with inappropriate use. Children must be supervised when they

are using the Internet by a member of staff. All users of the Internet must be authorised by the Headteacher. Authorised users will not be allowed to access the Internet through the school Network for personal financial gain or advertising any business or service they might personally be involved in for financial reward. The school will use Stockport LEA as their Internet Service Provider (ISP). This will be reviewed annually in terms of service / reliability / filtering and cost involved in changing their Internet Service Provider.   The school will use the filtering software provided by Stockport LEA.

Every user of the schools' network can have access to a class email address. In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission. Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. All email accounts held on the school network can be accessed at any time by the Headteacher to check on appropriate use. The Network is installed with virus checking software both on the server and the workstations, this software is updated each term.

Pupils will be educated to follow sensible rules for personal safety and will be encouraged to report if they feel uncomfortable about material or messages they encounter when using the Internet to the member of staff supervising. If the member of staff, after investigation, agrees with the child they must pursue the following action.
• 	Arrange for the site, or area visited, to be blocked or the email traced and the police informed if necessary.
• 	Inform the parents of the child in writing.
• 	Complete the Internet incident log in the office
Pupils will be encouraged to report any intentional access of unacceptable material by any user of the school network. The member of staff in charge of the session would take the following action:
• 	Implement the school discipline procedure.
• 	Inform the parents of the pupils in writing
• 	Complete the Internet incident log
• 	Check that the site that the pupil was trying to visit is blocked. If it is not, arrange for it to be blocked.
Staff will be asked to sign an acceptable use statement. Any person not directly employed by the school will be asked to sign an agreement for acceptable use of school ICT resources, before being allowed to access the Internet from the school site. If a member of staff or volunteer is reported to any member of staff. The following action would be taken by the member of staff:
• 	The staff member would ensure that pupils aren't at risk.
• 	They would inform the Head teacher or Deputy
The following action would be taken by the Head teacher:
• 	Implement the school discipline procedures
• 	Remove access as appropriate
• 	Record the incident in the confidential Internet Incident Log

Parents will be kept informed of the school's policy and ongoing issues raised by the Internet by Information Leaflets sent home. The school will work with parents to encourage appropriate use outside school.

All pupils are entitled to equal access to the Internet regardless of learning need, disability, gender, creed, ethnic or social background. Any Web Sites that undermine this principle will be blocked from the school Network.

0.6 ~ Website

The school will develop and maintain its own Website. The Computing SIG (School Improvement Group) will update the website and ensure that content is accurate and appropriate. The Head Teacher will have overall editorial responsibility. The Head teacher may delegate tasks to either a member of staff or a supporting company / organisation with specialist skills. If the school is approached to publish work or photographs on other Web Sites individual letters of permission will be sought from parents.

Photographs of children will only be used on the school website if they are able to remain anonymous and the school has received parental consent.

Staff or pupil personal contact information will not be published. The contact details given online will be the school office.

0.7 ~ E-mail

All email communication between staff and members of the school community on school business must be made from an official school email account. Staff should not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the head teacher. The official school email service may be regarded as safe and secure and is monitored. Users must immediately report, to the to the E-safety coordinator – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

0.8 ~ Social Media

The widespread availability and use of social media applications bring opportunities to understand, engage and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation e.g. our duty to safeguard children, young people and vulnerable adults. Social networking applications include, but are not limited to: Blogs, Online discussion forums, Collaborative spaces, Media sharing services, 'Microblogging' applications and online gaming environments. Examples include Twitter, Facebook, Windows Live Messenger, YouTube, Flickr, Xbox Live, Blogger, Tumblr and comment streams on public websites such as newspaper sites.

All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the school's Equalities, Child Protection and the Technology Policy.

School staff will not invite, accept or engage in communications with parents/carers or children from Lisburne School. When there are exceptional circumstances, permission must be sought from the head

teacher or member of the senior management team. Any communication received from children on any personal social media sites must be reported to the Designated Safeguarding Lead. Staff should not accept any current pupil of any age or any ex-pupil of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account. If any member of staff is aware of any inappropriate communications involving any pupil in any social media, these must immediately be reported.

School staff should ensure that
- No reference is made in social media to pupils, parents / carers or school.
- 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 or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- The school's use of social media for professional purposes will be checked regularly by the e-safety coordinator.

Members of the school staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts. Staff are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts. Staff are also advised to consider the reputation of the school in any posts or comments related to the school on any social media accounts. Staff are not to use the school system for any social media activities. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. We appreciate that parents may choose to expose their children to social networking.

0.9 ~ YouTube

In line with LEA guidance, use of YouTube in school must be reasonable and users must be held responsible for the chosen content being streamed within school. Specific school computer users may access the video sharing site to provide ease of access to videos which have the potential to enrich and stimulate the education of Lisburne School Pupils.

To access YouTube at Lisburne School users must:
- Be a teacher or member of SLT
- Only connect to YouTube through their own personal Lisburne computer login
- Teachers/SLT must be in the room while YouTube is being used.
- All videos must be scrutinized from start to finish before being shared for appropriate content.
- YouTube is not for personal use, strictly for relevant educational purposes.
- Be aware that all usage is being monitored.
- Users are using the same internet browser for work emails and YouTube they will be automatically logged into YouTube with their work email account.
- Never download any content from the website to be stored.
- Never upload their own videos to the site using their Lisburne School email address.
- Content can be deleted by the video uploader or YouTube themselves
- Lisburne School and SMBC are not responsible for the content of the website.

Any failure to comply with the above regulations will result in the immediate termination of YouTube access.

<u>0.9 ~ E-Safety</u>

Pupils must be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school:
- Training to include: acceptable use, social media, data protection, reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions including legal risk

Training will be received by staff, parents, governors and the wider community on e-safety. All staff must read and sign the Staff Code of Conduct for ICT before using any school ICT resource. The Business Manager, in conjunction with the Headteacher, will maintain a current record of all staff, governors and pupils who are granted access to school ICT systems.

Should an incident arise outside of school with regards to e-safety, this will be reported to the Headteacher and e-safety coordinator, who will discuss the incident with parents. The incident will also be discussed with the pupil. As a follow up – discussions will take place, for example during circle times within class, as an assembly and lessons on e-safety through ICT and PSHE lessons.

<u>Assessing risks</u>
The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Stockport Council can accept liability for any material accessed, or any consequences of Internet access.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The senior management team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

The Computing SIG will audit ICT use to establish if the current policy is adequate and that the implementation of the policy is appropriate and effective.

<u>Handling e-safety complaints</u>
- Complaints of Internet misuse will be dealt with by the E-Safety coordinator and members of the Senior Management team.
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Out of school incidents must be reported to the Headteacher and E Safety Coordinator who will follow the same incidents of misuse (see appendix A – flowchart).
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- An e-safety report log is kept in the school office to report e-safety incidents.

E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly. Pupils will be informed that network and Internet use is monitored and appropriately followed up.

E-Safety training will be embedded within the Computing progression of skills and/or the Personal Social and Health Education (PSHE) curriculum. Pupils will be made aware that E-Safety incidents can take place outside of school. They will be taught that the same rules apply inside and outside of school.

Staff must be made aware that network and Internet traffic is monitored and traced to the individual user. Staff who manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Staff will always use a child friendly safe search engine when accessing the web with pupils.

The school will maintain a list of E-safety resources for parents/carers via the school website.

Lisburne has a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities may be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party.

Responding to incidents of misuse – (Appendix A)

Incidents to be reported to: Headteacher and E Safety Coordinator or another member of the Senior Management Team.

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: Particular care should be taken if any apparent or actual misuse appears to involve illegal activity. The following are examples of such illegal online activities:
• Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978
• Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
• Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to Sections 63(1), (7)(d) and 67(3) of the Criminal Justice and Immigration Act 2008

• Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986
• Other criminal conduct, activity or materials

Flowchart for responding to online safety incidents:

Polite

I will report any form of bullying, intimidation or nastiness towards others.
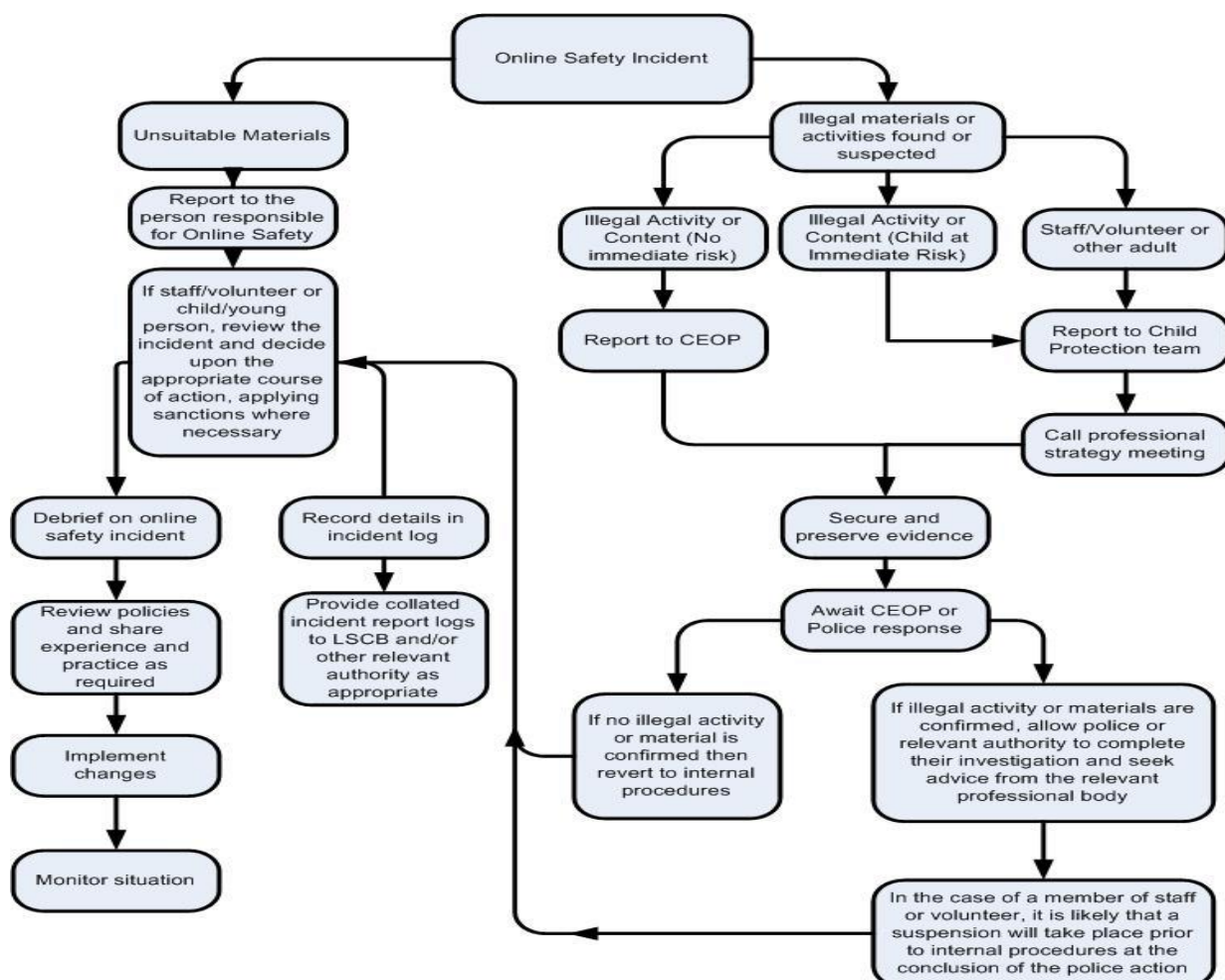
Responsible

I will look after the iPad and never leave it unattended.

I will bring the iPad to school when asked in its case, within my school bag.

iRule

Respectful

I will not tamper with the iPad to get round restrictions.

I will not mark the iPad, or its case, in any way.

Kind

I will ask people's permission before taking a photo, video or audio of them.

I will not try to guess other people's password

Safe

I will only use the iPad at home or at school, not on the way.

I will protect the iPad with a 4-digit code (password).

I will not use the iPad to access inappropriate content.

Honest

I will tell the school as soon as possible if I lose the iPad or if it gets broken.

I will not use the iPad for illegal downloads.