**Respect for All. Learners for Life.**

# Online Safety Policy

May 2019

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2018 (KCSIE) and other statutory documents; it is designed to sit alongside school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

**Development/monitoring/review of this policy**

This online safety policy has been developed by key people:

- Headteacher
- Designated safeguarding lead
- School Online Safety Coordinator
- Teachers
- Support Staff
- ICT Technical staff
- Governors

It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff network/drive
- Available in paper format in the staffroom
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review

There will be an on-going opportunity for staff to discuss with the online safety co-ordinator any issue of online safety that concerns them.

This policy will be reviewed annually and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way or incidents have occurred in school.

This online safety policy was approved on _____

This online safety policy was approved by _____

Signed: _____

Review date: _____

ICT in the 21st century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology (ICT) covers a wide range of resources including web based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using inside and outside of the classroom are:

- Websites
- E-mail and instant messaging
- Chat rooms and social networking
- Gaming- Xbox online, playstation, wii online etc
- Mobiles/ smart phones with text, video/web functionality
- Blogs and wikis
- Podcasting
- Video broadcasting
- Music downloading
- Other mobile devices with web functionality.

We live in a digital age where technology is playing an ever increasing part in our lives; it is changing the way that we do things both inside and outside of school and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents/carers associated with Lister Infant School are able to use technology in a safe and responsible manner. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

This policy applies to all members of the Lister Infant School community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

**Disclaimer*: Due to constant changes taking place within technology, this policy may not contain the most recent developments. We will however, endeavour to add any important issues to the policy on our website***

**Aims**

- Set out expectations for all Lister Infant School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - For the protection and benefit of the children and young people in their care
    - For their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - For the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

**Roles and responsibilities**

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school.

As online safety is an important aspect of strategic leadership within the school, the Head (**JANET DAVIES**) and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named online safety co-ordinator in our school is **RACHEL MANLEY.** All the members of the school community have been made aware of who holds this post. It is the role of the online safety co-ordinator to keep abreast of current issues and guidance through organisations such as Becta, CEOP (Child Exploitation and Online Protection), childnet and the NSPCC.

Senior management and Governors are updated by the Head / online safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: safeguarding, child protection, health and safety, home-school-child agreement, behaviour policy and PHSE.

**Education and training**

As the use of technology and the potential risks associated with the use of the technology change rapidly, it is essential to ensure that the school community know how to use technology safely and responsibly. The school is committed to ensuring that staff receive regular training to keep up to date with new developments and ensure that they are sufficiently confident to educate pupils in the safe and responsible use of technology. The school have designed an online safety curriculum that meets the needs of all pupils and ensure their safety and well-being. The curriculum is reviewed and revised on a regular basis to ensure that it remains current. The school will also endeavour to provide information and training opportunities for parents and carers to raise their awareness of the technologies that their children are potential using and the risks that they potentially face.

**School Website**

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and staff has the responsibility of updating the content of the website.

**Roles and Responsibilities**

**Head teacher**
**Key responsibilities:**

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. technician) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory DfE requirements (see appendices for website audit document)

**Online Safety Lead**

**Key responsibilities** (The DSL can delegate certain online-safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2018):

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with the local authority and work with other agencies in line with Working together to safeguard children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life.
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technician
- Communicate with the designated online safety governor to discuss any current issues
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incidents
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are aware LGfL filtering. see following link- (https://d1afx9quaogywf.cloudfront.net/sites/default/files/Filtering/Monitoring/2017%20LGfL%20Filtering%20integrator%20response.pdf)
- Ensure the 2018 Department for Education guidance on bullying is followed throughout the school and that staff adopt a zero-tolerance approach.

- Facilitate training and advice for all staff: all staff must read KCSIE Part 1 and all those working with children Annex A. It would also be advisable for all staff to be aware of Annex C (online safety)
- work with PSHE/RE lead to- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / RE curriculum, "complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds."

**Governing Body, led by Online Safety / Safeguarding Link Governor**
**Key responsibilities** (quotes are taken from Keeping Children Safe in Education 2018):

- Approve this policy and strategy and subsequently review its effectiveness,
- "Ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety) with the appropriate status and authority [and] time, funding, training, resources and support…"
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and Head teacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction [and] regularly updated, online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach."
- "Ensure appropriate filters and appropriate monitoring systems are in place but be careful that 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding".
- "Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school approach to online safety with a clear policy on the use of mobile technology.

**Role of all staff**

**Responsibilities:**

- Understand that online safety is a core part of safeguarding and know who Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are
- To embed online safety in the curriculum, identifying opportunities to thread online safety through all school activities. Including both outside the classroom and within the curriculum, making the most of unexpected learning opportunities as they arise
- They have an up to date awareness of online safety matters and of the current school online safety policy and practices, attending whole school training
- They have read, understood and signed the Staff Acceptable Use Agreement.
- 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.
- They report any suspected misuse or problem to the Headteacher/ online safety Coordinator/Designated Senior Person for investigation/action/sanction.
- Whenever overseeing the use of technology (devices, the internet, new technology) in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Encourage pupils to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem. Be aware that you are often most likely to see or overhear online-safety issues- let DSL/OSL know
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff

**Role of Pupils**

**Responsibilities:**

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology

- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

**Computing lead**
**Responsibilities:**

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

**Role of ICT Technician**
**Responsibilities:**

- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / LGfL TRUSTnet nominated contact to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of school technology and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- To ensure appropriate backup procedures and disaster recovery plans are in place
- Ensure that anti-virus is up to date on all computers and staff laptops. This automatically updates.

**LGfL TRUSTnet Nominated contacts – (Janet Davies, Kirsty Gordon, Rachel Manley, Paula McFadden and Ashley Haynes)**
**Responsibilities:**

- To ensure all LGfL TRUSTnet services are managed on behalf of the school in line with school policies, following data handling procedures as relevant
- Work closely with the DSL and DPO to ensure they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications of all existing services and changes to settings that you might request – e.g. for YouTube restricted mode, internet filtering settings, firewall port changes and sharing settings for any cloud services such as Microsoft Office 365.
- Ensure the DPO is aware of the GDPR information on the relationship between the school and LGfL TRUSTnet at gdpr.lgfl.net

**Parent's/Carers role**

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their children's online 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.

**Responsibilities**

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

**Education and Curriculum**

**Managing the school's online safety messages**

- Policy to be posted on the school website, kept in all staff/classroom policy folders and in the staffroom.
- The online safety policy is introduced to the pupils at the start of each school year and pupils sign their name to agree the rules.
- We endeavour to embed online safety messages across the curriculum whenever the Internet and/or related technologies are used. Online safety has been included in our PSHE curriculum.
- Online safety displays and key messages (posters and top tips).
- Internet and iPad rules are displayed by each class computer and technology areas.
- All year groups take part in workshops on Safer Internet Day

**Online safety in the curriculum**

- Every year the school celebrates National Safer Internet Day, teaching the children the advantages and disadvantages of working online and how to stay safe through age related online safety messages/themes.
- The school provides opportunities within a range of curriculum areas to teach about online safety, especially PHSE and Computing.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the online safety curriculum.
- Pupils are taught about respecting other people's information, images etc through discussion and modelling.
- Pupils are aware of the impact of on-line bullying and know how to seek help if they are affected by these issues. Pupils are also aware where to seek advice or help if they experience problems when using the internet and related technologies i.e. parent/carer/teacher/trusted staff member or an organisation such as childline/CEOP report abuse button.
- Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying
- School procedures for dealing with on Online safety will be mostly detailed in the additional policies

This school commits to take all reasonable precautions to ensure online safety recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF).

**Data Security and Protection**

The accessing of the school data is something that the school takes very seriously.

- All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements,
- Rigorous controls on the LGfL TRUSTnet network, USO sign-on for technical services, firewalls and filtering all support data protection.
- The headteacher/principal, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

**All school staff will ensure that:**

- Care is taken to ensure the safe keeping of data, minimising the risk of its loss or misuse.
- Data is used or processed on only secure password protected computers and other devices, and these devices are properly "logged-off" at the end of any session in which they are using personal data.
- Data is transferred securely using encryption and secure password protected devices and email solutions.

**Encrypted USB sticks:**

- The device must be password protected
- The data must be securely deleted from the device once it has been transferred or its use is complete

**Password policy**

- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems including ensuring that passwords are not shared and are changed periodically. Passwords should be on iPads, laptops and memory pens holding confidential data.
- Staff are not to save passwords or ask computers to remember passwords.
- Staff teach pupils and discuss keeping passwords safe and why this is important. When accessing our school online learning tool Purple Mash pupils are aware to always keep their passwords private and must not share with others.

**Appropriate Filtering and Monitoring**

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At this school, the internet connection is provided by LGfL TRUSTnet. This means we have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen, which is made specifically to protect children in schools.

**Managing the Internet**

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Internet is logged on the server and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

**How will Internet use enhance learning?**

**Pupils**

- Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Students will have supervised access to the Internet resources through the school's internet technology. (e.g Online Learning tool Purple Mash)
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.

**Staff**

- Staff will preview any recommended sites before use.
- Image searches are discouraged when working with pupils.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other resources.
- All users must observe copyright of materials from electronic resources.
- If staff or pupils discover an unsuitable site, the screen must be switched off, the computer isolated and the incident reported immediately to the teacher and then to the online safety co-ordinator/Head.
- A log sheet must also be completed by the member of staff.

**Mobile technologies**

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as iPads, iPod Touches, portable media players, PDA's, gaming device, mobile and smart phones are familiar to children outside of school. They often provide a collaborative, well known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

**Teaching and Learning**

Technologies provide a flexible solution and offer a range of exciting opportunities to extend children's learning

- School use of mobile devices, including laptops, mobile phones, cameras, iPads and iPod Touches are more common place and are essential elements of learning in our school.
- All staff share iPad rules with children, and they are displayed in all classrooms.
- Children will use a range of age appropriate apps (Interactive, reference and productivity) within lessons.

- iPads and iPod Touches have Internet access which include filtering. Staff are aware of in app purchases and monitoring will take place when technologies are in use.
- Children are taught to act safely and responsibly when using technology both within, and outside of the school environment.

**Personal Mobile Devices (including phones)**

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.
- Staff may use mobile phones only in designated areas away from children. Visitors can only use mobile phones in the staffroom or office. Visitors must read and sign acceptable use before entering the school.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices in to school must ensure there is no appropriate or illegal content on the device.
- Permission must be sought from the Head if a child requires a mobile phone in school. This must be taken to the office before registration and collected at hometime.

**School mobile devices**

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Where the school provides mobile technologies such as iPads laptops, cameras, video cameras etc for offsite visits and trips only these devices should be
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school. They are not to be used by children in school.

**iPad Acceptable use**

Staff should remember that, in school:

- iPads should be used for educational purposes only
- Follow the school's AUP for staff and the Child Protection Policy at all times
- Keep their iPad with them or in a secured (locked) area at all times
- Keep the four-digit security PIN on their iPads confidential
- Report loss, theft or damage to Headteacher or online safety lead immediately

**Managing E-mail**

The use of E-mail within most schools is an essential means of communication for staff and pupils. In the context of school, E-mail should not be considered private. Educationally, E-mail can offer significant be benefits including; direct written contact between schools on different projects, staff based, and pupil based (overseen by adults). Staff write E-mails with the children to model good 'nettiquette'.

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored
- The school gives all staff their own E-mail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious E-mails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the online safety and security of users and recipients, all mail is filtered and logged, if necessary, E-mail histories can be traced. This is the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal E-mail addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- All Email users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not
  revealing any personal details about themselves or others in Email communication or arrange to meet anyone without specific permission and virus checking attachments.
- Offensive Emails should be reported immediately. Staff inform online safety co-ord/Head.
- Pupils are introduced to email as whole class and are taught about appropriate use and what to do if they receive an offensive email.

**Safe use of Images**

**Publishing pupil images**

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose (For displays around the school, newsletter, online prospectus or websites and for social media). This consent form is considered valid for the entire year unless there is a change in the child's circumstances. Parents/Carers may withdraw permission, in writing, at any time. Pupil's names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published. Once photographs and class information/celebrations have been authorised by the Head/Senior Management Team, staff have authority to upload to the site (including Admin Officer).

**Digital images and video**

- Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose
- All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. No member of staff will ever use their personal phone to capture photos or videos of pupils.
- Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.
- We encourage young people to think about their online reputation and digital footprint, so we should be good adult role
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children
- Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

**Consent of the adults who work at the school**

Permission to use images of all staff who work at the school is sought on induction and, on the staff, acceptable use form.

**Storage of images**

- Images /videos of the children are stored on the school server.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the network.
- Images are regularly monitored and deleted when no longer needed.

**Misuse and Infringements**

**Complaints**

Complaints relating to online safety should be made to the online safety co-ordinator or Headteacher. Incidents should be logged and the flowchart for managing an online safety incident should be followed (see page 15)

**Unsuitable/ Inappropriate material**

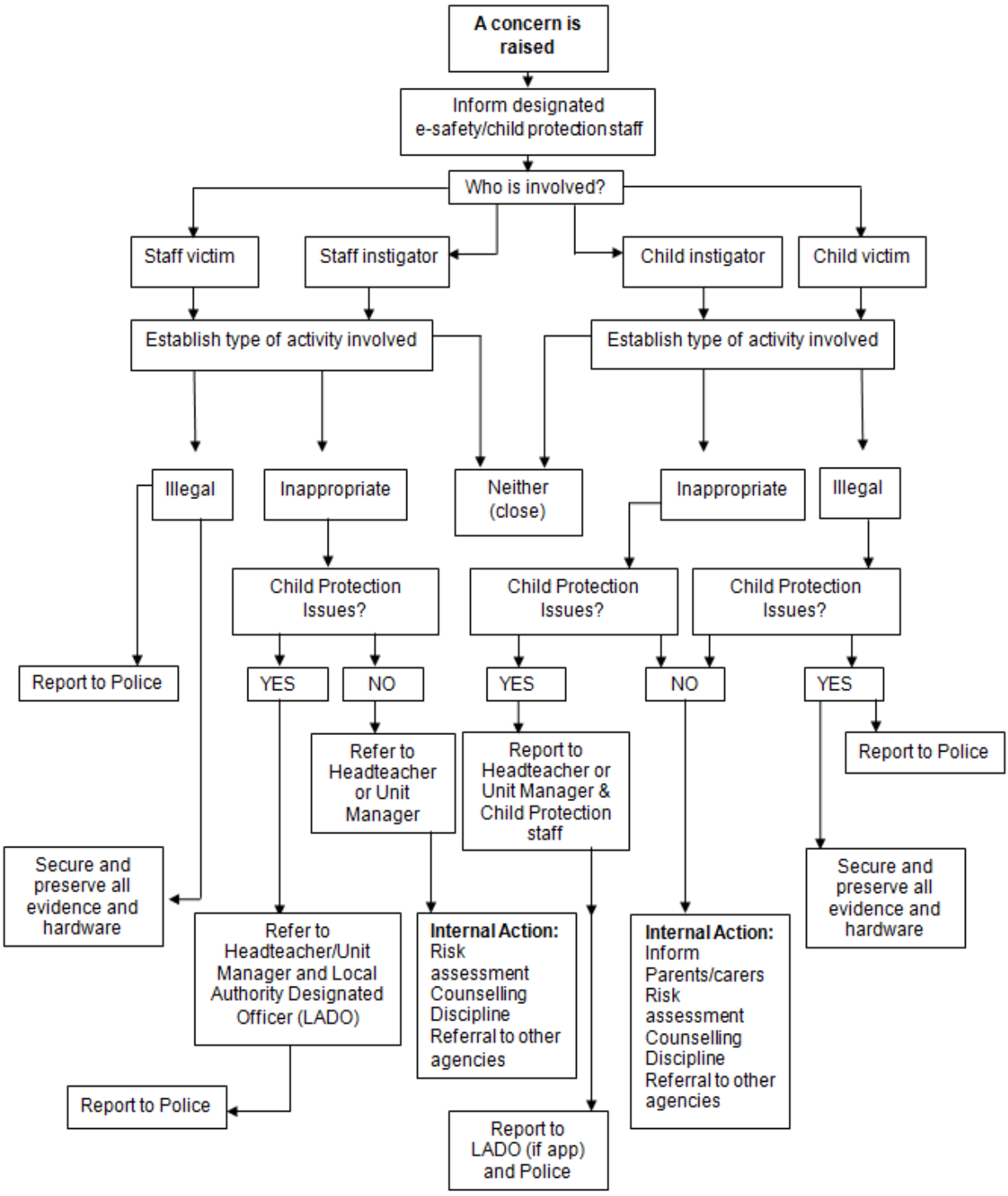
- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be reported to the online safety co-ordinator/Head.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the online safety co-ordinator, depending on the

seriousness of the offence: investigation by the Head/LEA, immediate suspensions, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)

- Users are made aware of sanctions relating to the misuse or misconduct on the Acceptable Use Agreement.

**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 accidently, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of an online safety incident it is important that there is a considered, coordinated and consistent approach. Incidents will be managed using the incident flowchart below


A concern is raised
Inform designated e-safety/child protection staff
Who is involved?
Staff victim
Staff instigator
Child instigator
Child victim
Establish type of activity involved
Establish type of activity involved
Illegal
Inappropriate
Neither (close)
Inappropriate
Illegal
Child Protection Issues?
Child Protection Issues?
Child Protection Issues?
Report to Police
YES
NO
YES
NO
YES
Refer to Headteacher or Unit Manager
Report to Headteacher or Unit Manager & Child Protection staff
Report to Police
Secure and preserve all evidence and hardware
Refer to Headteacher/Unit Manager and Local Authority Designated Officer (LADO)
Internal Action: Risk assessment Counselling Discipline Referral to other agencies
Internal Action: Inform Parents/carers Risk assessment Counselling Discipline Referral to other agencies
Secure and preserve all evidence and hardware
Report to Police
Report to LADO (if app) and Police

**Equal Opportunities**

**Pupils with additional needs**

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's online safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

Where a pupil social understanding needs, careful consideration is given to group interactions when raising awareness of online safety. Internet activities are planned and well managed for these children and young people.

**Social media (staff, parents and pupils)**

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve). Many social media platforms have a minimum age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults. Parents can best support this by talking to their children about the apps, sites and games they use.

The school has an official Twitter account to showcase achievements, success and celebrations. Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school. School will not respond to general enquiries and asks parents/carers not to use these channels to communicate about their children.

Pupils/students are not allowed to be ‘friends’ with or make a friend request to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from ‘following’ staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts. Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

## Appendix

Acceptable Internet Use agreements for staff/governors and supply staff

Acceptable Use agreements/code of conducts for visitors

Curriculum

## Acceptable Use Agreement/Code of conduct: Staff and Governors

ICT and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Rachel Manley, the school's Online Safety co-ordinator.

**Deliberate access to inappropriate materials by any user will lead to the incident being logged by the online safety co-ordinator, depending on the seriousness of the offence; investigation by the Head Teacher/LEA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.**

- I will support and promote the school's online safety policy and help pupils to be safe and
  responsible in their use of ICT and related technologies.
- I will report and incidents of concern regarding children's safety to the designated Child Protection Co-ordinator. (Janet Davies)
- I will only use the approved, secure email system(s) for any school business.
- I understand that it is a criminal offence to use the school ICT system for purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, digital cameras; email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that the school information systems may not be used for private purposes without specific permission from the Head Teacher.
- I understand that my use of school information systems, laptops, iPads, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any hardware or software without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head Teacher
- I will respect copyright and intellectual property.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

*The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.*

Signature: ..... Date: .....
Full name (printed)..... Job title: .....

## Acceptable Use Agreement/Code of conduct: Visitors

ICT and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all visitors are aware of their professional responsibilities when using any form of ICT within school. All visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Rachel Manley, the school's online safety co-ordinator.

**Deliberate access to inappropriate materials by any user will lead to the incident being logged by the online safety co-ordinator, depending on the seriousness of the offence; investigation by the Head teacher/LEA, immediate suspension, possibly leading to the involvement of police for very serious offences.**

- I will not give out my personal details, such as mobile phone numbers and personal e-mail address to pupils.
- I will only use my mobile phone in the designated areas (staffroom/office).

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature: ..... Date: .....
Full name (printed)..... Job title: .....

**Curriculum**

At Lister Infant School we teach the children about online safety through our Computing curriculum. This is reinforced at various points throughout the school year within assemblies and PSHE sessions. As part of our curriculum we teach our children the importance of online safety and how to stay safe online through the following-

Developing online safety guidelines- Online rules that help us stay safe

Social and emotional wellbeing and developing resilience. Digital citizenship- Online behaviours and respect

Responsible Internet use- Using child friendly search engines safely

Keeping information safe- Understanding what is personal information and why we keep it safe

**Curriculum Overview**

It is important that we educate children to be safe and responsible whilst using the internet and technology. As part of their education, we need to teach them how to remain safe whilst online and how to use technology both appropriately and effectively. Children need to know how to protect themselves online whilst promoting the use of technology. Children are learning that appropriate, respectful ways to communicate are important and this should include digital communications, whether online or offline.

**Teaching aims EYFS**

In EYFS we introduce children to safe use of equipment and discuss the Online Safety tips shown on the posters that are displayed in classrooms.

Online Safety Awareness- Discuss internet and websites they like to use
Understand the importance to use the internet with grown-ups and why they stay on programs they are using
Talk about the range of technology they access at school and at home
Encourage nice behaviour and kind words when communicating,
Stranger Danger in the online world- keeping their name private.

**Teaching aims KS1:**

We teach the children in KS1 about SMART rules and display them in classrooms

Online safety Awareness- Online life and what it is?
Know the functionality of the internet and staying safe
Learn about the risks, who to turn to if they see anything inappropriate
Learn about email and gaming
Why it is important to keep all personal information private.
What is Cyber Bullying and why it is wrong, who to trust.
Communicating safely and with respect.