Lister Infant School and Nursery

Respect for All. Learners for Life.

Online Safety Policy

September 2021

Key People

	Designated Safeguarding Lead (DSL) team	Janet Davies, Kirsty Gordon, Natalie Clarke
	Online-safety lead	Rachel Manley
	Online-safety / safeguarding link governor	Steven Pritchard Gill Bell
	PSHE/RSHE lead	Eugina Kervin
	Network manager / other technical support	Peter Davies
	Date this policy was reviewed and by whom	September 2021
	Date of next review and by whom	September 2022

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2021 (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
- 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).
- Child friendly AUPs are displayed in classrooms

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

Aims

This policy aims to:

- 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)

Scope

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 Infants community (including teaching and support staff, supply teachers, governors, volunteers, 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, or who use technology in their school role.

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

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. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Head teacher

Key responsibilities:

- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards.
- 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 requirements.

Safeguarding and Online Safety Lead

Key responsibilities

(This assertion and all quotes below are from Keeping Children Safe in Education 2021):

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).
- Work with the HT and technical staff to review protections for pupils in the home and remote-learning procedures, rules and safeguards
- 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 to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs and Senior Mental Health Leads) on matters of

safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies."

- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply.
- 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 safeguarding and "undertake training.
- 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 in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life.
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, but also including hard-to-reach parents.
- Communicate with SLT and the designated safeguarding and online safety governor/committee to discuss current issues. Review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- 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 incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues.
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are also aware.
- Ensure that staff adopt a zero-tolerance, whole school approach to bullying.
- Facilitate training and advice for all staff, including supply teachers:
- All staff must read KCSIE Part 1 and all those working with children Annex B. Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.

It would also be advisable for all staff to be aware of Annex D (online safety). Cascade knowledge of risks and opportunities.

Governing Body, led by Online Safety / Safeguarding Link Governor
Key responsibilities (quotes are taken from Keeping Children Safe in Education 2021):

- Approve this policy and strategy and subsequently review its effectiveness.
- Ask about how the school has reviewed protections for pupils in the home and remote-learning procedures, rules and safeguards.
- "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 coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meeting.s
- 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 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.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B; check that Annex D 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.

All staff

Key Responsibilities:

- In 2021 pay particular attention to safeguarding provisions for home-learning and remote-teaching.
- Recognise that RSHE is now statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject.
- Understand that online safety is a core part of safeguarding and know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are.
- Read Part 1, Annex B and Annex D of Keeping Children Safe in Education. (Whilst Part 1 is statutory for all staff, Annex B for SLT and those working directly with children, it is good practice for all staff to read all three sections.)
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself.
- Sign and follow the staff acceptable use policy and code of conduct/handbook.
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites.
- When supporting pupils remotely, be mindful of additional safeguarding considerations.
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using.
- Encourage pupils to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Notify the DSL/OSL of new trends and issues before they become a problem.
- Take a zero-tolerance approach to bullying and sexual harassment.

- Be aware that you are often most likely to see or overhear online-safety issues (e.g. relating to bullying) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know.
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues.
- 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.

PSHE Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should now be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

Computing lead

Key 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 RSHE lead to avoid overlap but ensure a complementary whole-school approach.
- 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 Technician

Key Responsibilities:

- Support the HT and DSL team as they review protections for pupils in the home and remote-learning procedures, rules and safeguards.
- 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.
- Liaise with RSHE lead to see how the online-safety curriculum delivered through this new subject can complement the school IT system and vice versa, and ensure no conflicts between educational messages and practice.
- 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 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 and protect school network with LGfL solutions.

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

Key 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.

Volunteers

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP.)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP.
- Model safe, responsible and professional behaviours in their own use of technology at school.

Pupils

Key Responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually.
- Treat home learning during any isolation/quarantine or school lockdown in the same way as regular learning in school and behave as if a teacher or parent were watching the screen.
- 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.
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- 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.

Parent's/Carers role

Key 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 and others' 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.
- Support and encourage children to engage fully in home-learning during any period of isolation/quarantine or school closure and flag any concerns.

Education and Curriculum

The following subjects have the clearest online safety links

- Relationships education and health (also known as PSHE/RSHE)
- Computing

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the internet, new technology etc) in school or setting as homework tasks, all staff encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), 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.

At Lister Infants we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans / schemes of work are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling Online Safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying).

School procedures for dealing with online-safety will be mostly detailed in the following policies

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents may occur both inside school and outside 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.

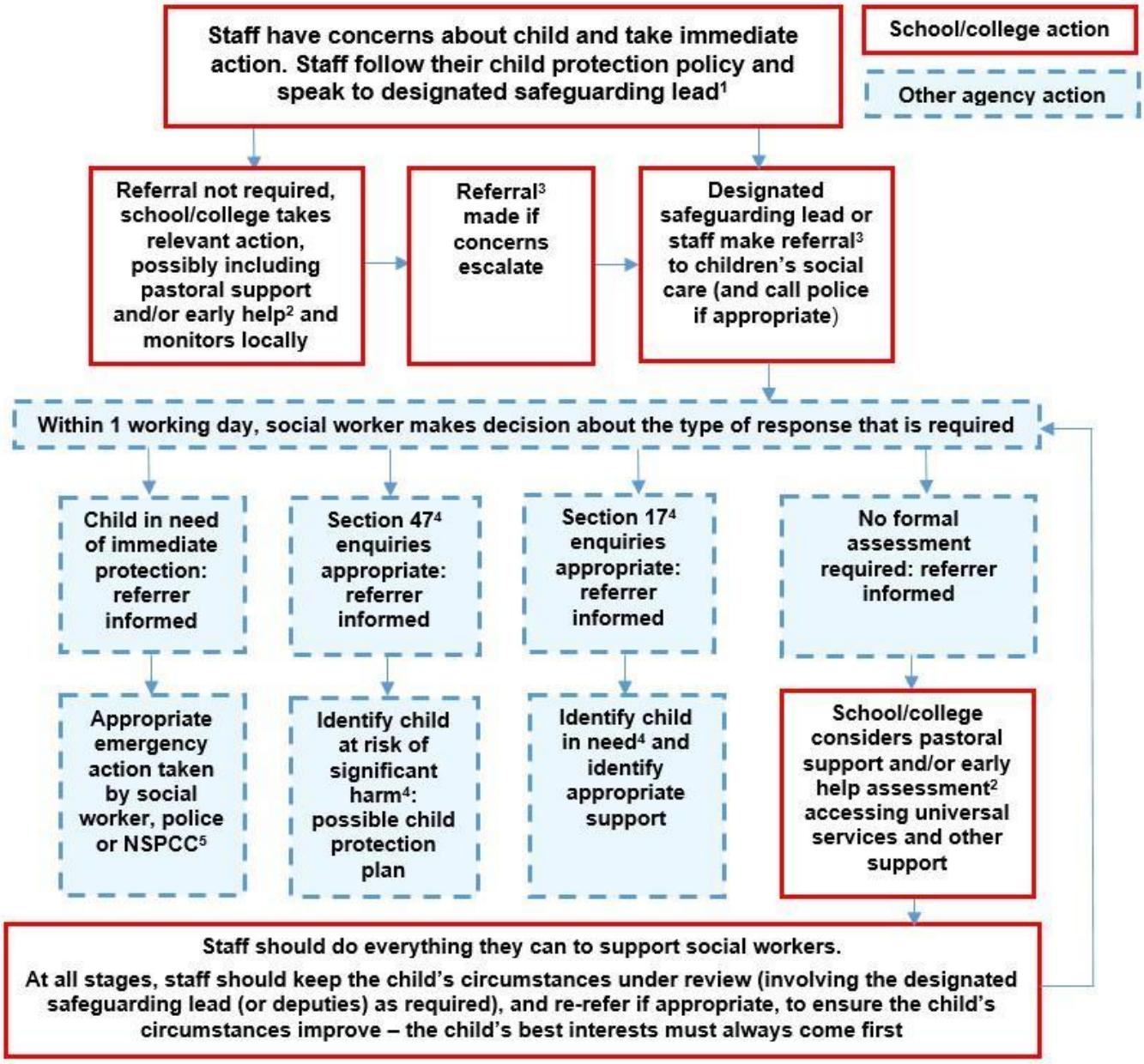
Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

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 (POSH), NCA CEOP, Prevent Officer, Police). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

The school should evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

Actions where there are concerns about a child.

The following flow chart (it cannot be edited) is taken from Keeping Children Safe in Education 2021 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



Bullying

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. Also refer to the school Anti-bullying policy.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology,

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, further action will be taken.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that the same applies for any home learning that may take place in future periods of absence/ closure/quarantine etc.

Social Media

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Lister Infants community.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the school will request that the post be deleted and will expect this to be actioned promptly.

Data protection and data security

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018).This quote from the latter document is useful – note the highlights:

"*GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe*. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) *it is considered best practice for them to record who they are sharing that information with and for* what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children."

Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection e.g. USO sign on for LGfL services.

The Headteacher data protection officer and governor's 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.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use to encrypt all non-internal emails is compulsory for sharing pupil data.

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. 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 3, which is made specifically to protect children in schools.

Email

General principles for email use are as follows:

- The official school run email service Office 365 is regarded safe and secure and is monitored. All staff communicate via this.
- 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 -mails and avoids the risk of personal profile information being revealed.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- If data or personal information needs to be shared with staff or external agencies, all emails must be password encrypted.

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. All staff are delegated to the responsibility of updating content of the website.

Digital images and video

- 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.
- Whenever a photo or video is taken/made, the member of staff taking it will check the latest consent database before using it for any purpose.
- Any pupils shown in public facing materials are never identified with first name.
- 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.
- Staff and parents are reminded about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.
- We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing.

Social Media

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online).

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

All staff are responsible for managing class social media accounts on Twitter.

Staff, pupils' and parents social media presence

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 should be followed.

The school and year groups have an official Twitter account and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

Many social media platforms have a minimum age of 13. Pupils are not allowed to be 'friends' with or make a friend request to any staff, governors or otherwise communicate via social media. 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 social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, we are aware children will often learn most from the models of behaviour they see and experience, which will often be from adults. We advise parents to support this by talking to their children about the apps, sites and games they use. Parents/carers are continually sign posted to guidance and support.

Staff exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Head teacher and should be declared upon entry of the pupil or staff member to the school.

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.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video and permission is sought before uploading photographs, videos or any other information.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity,

Device usage
Personal Devices

- All staff should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- Volunteers, governors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos.
- Parents should not capture other children in particular when at school events.

Network/Internet access on school devices

- Pupils are not allowed networked file access. However, they are allowed to access the school wireless internet network for school-related internet use. All use is monitored.

- Home devices are issued to some pupils. These are restricted to the apps/software installed by the school and may be used for learning but not for personal use at home, but all usage may be tracked.
- All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone.
- Volunteers and governors have no access to the school network or wireless internet on personal devices.

Trips/events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with school. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden.

Date this policy was reviewed and by whom: September 2021
Date of next review and by whom: September 2022