Lanesfield Primary School

On-Line Safety Policy 2020

Review: September 2021

Key people

Lanesfield Primary School	Designated Safeguarding Lead (DSL)	Mrs Z Rollinson
	Online-safety lead (if different)	Mrs Z Rollinson
	Online-safety / safeguarding link governor	Mrs K Budding
	PSHE/RSE lead	Mrs E Whitehouse
	Network manager / other technical support	Concero Uk, Cloud W
	IT/Computing lead	Mrs S Davidson

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2020 (KCSIE), 'Teaching Online Safety in Schools' 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside Lanesfield's Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures. This policy should be reviewed annually.

Aims

This policy aims to:

- Set out expectations for all Lanesfield Primary School's 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, and
    - 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.

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the Head Teacher will handle referrals to the LA designated officer (LADO). The local authority may also have advisors to offer general support.
Beyond this, reporting.lgfl.net has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline, the UK Safer Internet Centre and the NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud.

Scope

This policy applies to all members of the Lanesfield Primary 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, or who use technology in their school role.

Roles and responsibilities

At Lanesfield Primary School we are a community and all members have a duty to behave respectfully online and offline and to use technology for teaching and learning in order to best prepare pupils for life after school. Everyone has a responsibility to report any concerns or inappropriate behaviour immediately, 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/DSL

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- To ensure that DSL responsibilities 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 and relevant Local Safeguarding Partnerships
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the 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
- 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
- Ensure the school website meets statutory requirements
- Ensure that all staff have read and are aware of KCSIE 2020 Annex C (online safety)

Online Safety Lead

Key responsibilities:

- 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 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
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated safeguarding and compliance governors to discuss current issues and review incident logs
- 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
- Facilitate training and advice for all staff.

Governing Body, led by Safeguarding Link Governor

Key responsibilities:

- Approve this policy and strategy and subsequently review its effectiveness
- 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
- Work with the DPO, DSL/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
- Be clear that all staff have read the relevant safeguarding documents including KCSIE 2020
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction.
- Ensure that children are taught about safeguarding, including online safety, as part of providing a broad and balanced curriculum

All staff

Key responsibilities:

- Understand that online safety is an essential part of safeguarding; as such it is part of everyone's job - never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are

- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education 2020 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.
- 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, both outside the classroom and within the curriculum
- Whenever overseeing the use of technology in school or setting as homework tasks, encourage sensible use, monitor what pupils/students 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, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and data law
- Prepare and check all online source and resources before using within the classroom
- Encourage pupils/students 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
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety 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 / RSHE Lead/s

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. 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 / RSE.

IT/Computing Subject 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 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

Network Manager - CloudW IT Technician - Concero UK

Key responsibilities:

- As listed in the 'all staff' section, plus:
- 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 DSL / online safety lead / DPO
- 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)
- 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, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- Work closely with the IT/Computing Lead to develop systems and procedures as well as monitor existing ones.

Data Protection Officer (DPO)

Key responsibilities:

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education 2020' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document: "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."

- Work with the DSL, Head Teacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and Students

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the DSL
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Pupils

Key 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

Parents/carers

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.

Education and Curriculum

At Lanesfield Primary School, we aim to give our pupils the life-skills that will enable them to embrace and utilise new technology in a socially responsible and safe way. We want our children to become confident, creative and independent users of computing technologies, gaining confidence and enjoyment from their learning experiences. We want the use of technology to support learning across the entire curriculum and to ensure that our curriculum is accessible to every child. It is our mission that all our pupils have a breadth of experience to develop their understanding of themselves as individuals within their community but also as members of a wider global community and as responsible digital citizens.

The following subjects have the clearest online safety links and the medium term planning reflects this:

- PSHE
- Relationships education, relationships and sex education (RSE)
- 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. As a 1:1 IPad school, pupils use devices across a range of subjects and their use is fully in-built within day-to-day learning.
We recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why it does not stand alone as a linear subject. Teachers plan opportunities to work on key areas: Self-image/Identity, Online relationships and reputation, Online bullying, Managing online information, Health, Wellbeing and Lifestyle, Privacy, Security, Copyright and Ownership.

Virtual Meetings and Home Learning

- All staff and governors will use Microsoft Teams to facilitate virtual meetings
- A member of school staff will set up the meeting and send invitations
- All staff and governors are expected to attend virtual meetings in a private space where conversations can remain confidential.
- Staff and governors should follow the dress code in the school's Code of Conduct and ensure that the background of the video call is appropriate
- There should be no recording of meetings without prior consent.
- All staff and governors will adhere to the Wolverhampton City Council Video Conferencing Data Protection Advice.

Trips / events away from school

For school trips/events away from school, the group leader will use their personal mobile phone as a contact for schools and in the event of an emergency, to contact any services needed and notify school to inform parents. Staff using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Handling online-safety concerns and incidents, including bullying

It is vital that all staff recognise that online-safety is a part of safeguarding.
General concerns must be handled in the same way as any other safeguarding concern. The Safeguarding and Child Protection Policy should be adhered to.
Lanesfield Primary School commits to take all reasonable precautions to ensure online safety, but 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 them to be dealt with quickly and sensitively through the school's escalation processes.

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.
Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.
Further to these steps, the school reserves the right to withdraw - temporarily or permanently - any or all access to such technology, or the right to bring devices onto school property.

Appropriate filtering and monitoring

At Lanesfield Primary School the internet connection is provided by British Telecommunications (BT) in connection with Concero UK. We have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of security, including a web filtering system.

Email

Staff and children at Lanesfield Primary School have Microsoft email accounts. These accounts are fully trackable and managed by Concero on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the HeadTeacher should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.
    - If data needs to be shared with external agencies, passport protection and encryption should be applied
    - Internally, staff should use the school network,
- Appropriate behaviour is expected at all times.

School website

Our school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The site is managed by Eservices at the Local Authority. There are dedicated links for parents and pupils relating to online safety.

Cloud platforms / TEAMs / Showbie Tapestry

This school adheres to the principles of the DfE document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'. Concero Uk monitor and review their use.
The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom.
- Regular training ensures all staff understand sharing functionality
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- Parent consent is requested before pupils are given access to Microsoft TEAMs and Showbie. Parents are directed to the relevant privacy notices
- Pupils are reminded about the importance of keeping passwords protected and this is referred to in the relevant Acceptable Use Policies.
- A letter is sent out to new EYFS parents to gain permission for the use of Tapestry.

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos. This information is stored electronically and deleted once the child leaves the school
Whenever a photo or video is taken, the member of staff taking it will check the latest database before using it for any purpose.
Any pupils shown in public facing materials are never identified with more than 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. At Lanesfield Primary School 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 regularly about the importance of not sharing without permission, due to reasons of child 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.
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 / or a friend are subject to bullying or abuse.

Social media

Lanesfield Primary School has a Facebook account and multiple Twitter accounts.
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.
The Eservices team at the Local Authority is responsible for managing our social media accounts.
Staff, governors, parents and children should ensure that they follow the guidance set out about the responsible use of social media accounts in the relevant Acceptable Use Policies. Staff should also refer to the staff code of conduct.
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 however the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.
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, children will often learn most from the models of behaviour they see and experience, which will often be from adults.
Parents can best support by talking to their children about the apps, sites and games they use.

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.
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.
Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL.

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.

Personal devices including wearable technology and mobile phones

- Pupils are not allowed mobile phones in school. If they bring them to school they must be locked away in the school office until the end of the day.
- Mobile phones should not be accessed during the school working day, with the exception of dinnertime away from the children. They should not be openly visible but locked away in a class cupboard or locker. For all members of staff, none class based mobile phones should be stored along with other personal belongings in school lockers.
- Under no circumstances are school photographs to be taken on mobile phone. A school IPad should be used.
- Volunteers, contractors, governors should be turned off and out of site. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Head Teacher should be sought and this should be done in the presence of a member staff.
- Parents are asked to keep their phones out of site and turned off when they are in school. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, parents are asked to take photos for personal use only and are to refrain from posting on social media accounts. They are reminded that there are some children at Lanesfield Primary School who do not have permission to have their photo taken or shared.

Network / Internet access on school devices

- Volunteers, contractors and governors can request access to the wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.
- Parents have no access to the school network or wireless internet on personal devices.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Head Teacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Signed _____ (Chair of Governors)

Date _____