ONLINE SAFETY POLICY

NEXT REVIEW: Spring 2026

Policy Approved: 1 April 2025
Review Period: 1Yr
Policy Responsibility: BM
Policy Approval: FGB

Introduction

Key people

Lakelands Academy	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	**Mark Hignett** - Headteacher/DSL /Online Safety Lead
	Deputy Designated Safeguarding Leads / DSL Team Members	**Kirstie Mansfield -** Senior Deputy DSL/Science teacher **Aimee Warren** - Deputy DSL/SENDCo/Geography teacher **Amanda Price** – Deputy DSL/Attendance and Welfare Manager **Karen Preece** - Deputy DSL/ Mental Health Lead/Assistant Headteacher **Rhiannon Jones** - Deputy DSL/ RSE Lead/Science teacher **Zoe Marks** - Deputy DSL/Art teacher **Jon Evans** - Deputy DSL/DT teacher **Chloe Kynaston -** Deputy DSL/Food Technology teacher **Kirsty Stephens** - Deputy DSL/Pastoral Support Officer **Hannah Davie** - Deputy DSL/ Pastoral Support Officer **Julie Metcalf** - Deputy DSL/Kettlemere Faculty Lead
	Link governor/Trustee for safeguarding and online safety	**Debbie Simmonds**
	Curriculum leads with relevance to online safeguarding and their role	**Tim Purslow –** Deputy DSL/Computing and Business Studies teacher **Rhiannon Jones** - Deputy DSL/PSHEE/RSE Leads
	Strategic Desktop Support Officer	**Gavin Shropshire**

What has changed in this policy for 2024?

The DSL now leads web filtering and monitoring, requiring schools to adhere to new DfE standards. All staff, especially DSLs and SLT, must understand, review, and drive decisions in this area. Close collaboration between tech and safeguarding teams is crucial, with technicians conducting regular checks and providing feedback to DSL teams. Staff awareness of changes is vital, and active participation in reporting over-blocking or filtering gaps is expected. Schools will review monitoring approaches to align with the standards.

What is this policy?

This policy aligns with *Keeping Children Safe in Education* 2024 (KCSIE), the Children Act 2004, and *Working Together to Safeguard Children,* which sets out how organisations and individuals should collaborate to safeguard and promote children's welfare. *Working Together* defines safeguarding as:

- providing help and support to meet the needs of children as soon as problems emerge
- protecting children from maltreatment, whether that is within or outside the home, including online
- preventing impairment of children's mental and physical health or development
- ensuring that children grow up in circumstances consistent with the provision of safe and effective care
- promoting the upbringing of children with their birth parents, or otherwise their family network through a kinship care arrangement, whenever possible and where this is in the best interests of the children
- taking action to enable all children to have the best outcomes in line with the outcomes set out in the Children's Social Care National Framework

The policy complements statutory guidance, including *Teaching Online Safety in Schools* and RSE guidance, integrating safeguarding principles across the curriculum. All online safety concerns must follow the school's safeguarding and child protection procedures.

When is it renewed?

This policy is a dynamic document, undergoing a comprehensive annual review and adjustments as needed throughout the year in response to school and local developments. Although many aspects will be informed by legislation and regulations, Lakelands Academy actively engages staff, governors, students, and parents in crafting and reviewing the policy to ensure clarity, feasibility, and alignment with day-to-day practices. Involving students in designing a version tailored to their understanding and aiding compliance audits enhances stakeholder comprehension. Acceptable Use Policies for various stakeholders contribute to this process (**Appendix B**).

Who leads online safety?

KCSIE makes clear that "the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety)." The DSL can delegate activities but not the responsibility for this area and whilst subject leads, e.g. for RSE will plan the curriculum for their area, it is important that this ties into a whole-school approach. Our DSL at Lakelands Academy is **Mark Hignett.**

What are the main online safety risks in 2024/2025?

Current Online Safeguarding Trends

In 2024/2025, the primary online safety risks identified align with findings from recent Ofcom reports and other leading online safety studies. Key risks include cyberbullying and harassment, phishing and social engineering attacks, misinformation and fake news, privacy invasions and data breaches, and exposure to inappropriate content. According to Ofcom's latest report, cyberbullying tactics have become more sophisticated, with increased instances of doxxing, swatting, and cyberstalking. Phishing attacks are now highly personalised, leveraging AI to create convincing fake communications. The spread of false information, often created using deepfake technology, makes it very hard to tell what is real and what is not. Privacy invasions and data breaches continue to rise, leading to identity theft and financial fraud, while harmful content remains easily accessible to children and young people.

Online predation and grooming are escalating concerns, as predators use social media, gaming platforms, and chat apps to exploit children. Ofcom's findings highlight the growing prevalence of digital addiction and its associated mental health issues, such as anxiety, depression, and sleep disturbances, due to excessive screen time and social media use. Malware and ransomware attacks are becoming more sophisticated, targeting individuals, businesses, and critical infrastructure. Financial scams, like investment fraud and cryptocurrency scams, are increasing and often use social media to reach more people. Also, security weaknesses in Internet of Things (IoT) devices create significant risks, possibly allowing unauthorised access to personal and sensitive information.

Current safeguarding trends, supported by Ofcom's latest research, focus on enhanced parental controls and monitoring tools, increased digital literacy and online safety education, and stricter regulatory and legislative measures. Improved tools help parents monitor and control their children's online activities, while educational initiatives in schools highlight the importance of digital literacy and safe online practices. Governments are implementing stricter regulations to protect personal data and hold platforms accountable for harmful content. Enhanced collaboration between tech companies and law enforcement is crucial for detecting and preventing cybercrimes, particularly those targeting children. Utilising AI and machine learning to detect and mitigate online threats in real-time is also a key strategy in maintaining online safety.

How will this policy be communicated?

For effective impact, this policy must be a regularly updated living document, accessible and understood by all stakeholders. It will be communicated through various channels:

- Posted on the school website.
- Included in the induction pack for all new staff (temporary, supply and non-classroom based staff and those starting mid-year).
- Integral to safeguarding updates and training for all staff, especially in September refreshers.
- Clearly reflected in Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors Parents and students (which must be in accessible language appropriate to these groups), which will be issued to whole school community, on entry to the school, annually and whenever changed and displayed in school (see **Appendix B**)

Overview

Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Lakelands Academy community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSE) and beyond.
- Helping 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, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching and 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.
- Helping 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.
- Establishing clear structures by which online misdemeanors will be treated, and procedures to follow where there are doubts or concerns (please see our Behaviour Policy)

Further help and support

Please follow internal school channels, as outlined in our policy documents, for reporting and support, especially in response to incidents, which should be reported in accordance with our Child Protection and Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH), and normally, referrals to the LA designated officer (LADO) will be managed by the DSL.

Scope

This policy applies to all members of the Lakelands Academy community (including teaching, supply and support staff, governors, volunteers, contractors, students, 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

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, students, families and the reputation of the academy. We learn, make mistakes, and support each other in the interconnected world of online and offline experiences.

All members of the school community must read the relevant section in ***Appendix A***, which outlines individual roles and responsibilities based on their specific role. It is crucial for everyone to comprehend their responsibilities, especially in filtering and monitoring, in 2024. All staff play a key role in providing feedback on potential issues.

Education and curriculum

It is important that schools establish a carefully sequenced curriculum for online safety that builds on what students have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help students navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of students, including vulnerable students. RSE guidance also recommends schools assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress."

The following subjects have the clearest online safety links:

- **Relationships education, relationships and sex education (RSE) and health (also known as RSE or PSHEE)**
- **Computing**

All staff should integrate online safety into various school activities, both inside and outside the curriculum. Support curriculum leads and utilise unexpected learning opportunities.

When overseeing technology use in school or for homework, staff must encourage sensible use, monitor student activities, and assess potential dangers and age-appropriateness of websites (consult the DSL). It is important for parents to understand the school's filtering and monitoring systems. Staff should closely supervise and guide students in online learning activities, providing support for search skills, critical thinking, age-appropriate materials, and legal issues. Lakelands Academy integrates online safety and digital resilience into the curriculum, regularly reviewing plans to align with key areas such as self-image, relationships, reputation, bullying, information management, health, privacy, and copyright.

Handling safeguarding concerns and incidents

All staff must recognise that online safety is integral to safeguarding and part of the Computing, PSHEE/RSE, and Citizenship curriculum strands.

Address general concerns like any other safeguarding issue. Safeguarding is likened to a jigsaw puzzle, and stakeholders should communicate with the online safety lead/designated safeguarding lead to contribute to the overall picture or highlight potential issues. Support staff can often gather insights about issues first in communal areas outside the classroom, providing a unique perspective on matters like bullying and sexual harassment and violence.

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

- **Safeguarding and Child Protection Policy**
- **Anti-Bullying Policy**
- **Behaviour for Learning and Relationships Policy (including school sanctions)**
- **Acceptable Use Policies**

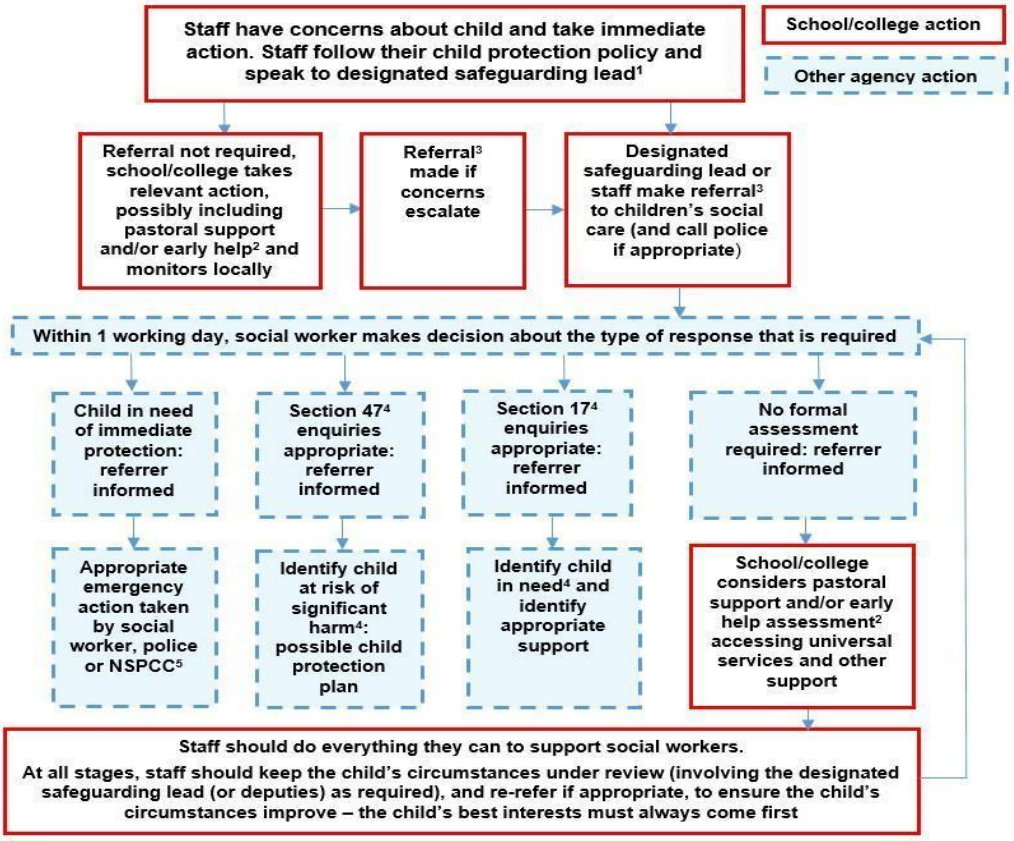
This academy is dedicated to taking reasonable precautions for online pupil safeguarding. Incidents may occur inside and outside school, impacting students during school hours or extended periods away. Prompt reporting of issues by all school members is encouraged for swift and sensitive resolution through 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**, or urgently by the end of the lesson. Concerns or allegations about staff misuse are referred directly to the Headteacher, or the Chair of Governors and the LADO in the case of concerns about the Headteacher. Staff can also use the NSPCC Whistleblowing Helpline.

The school will seek support from relevant agencies as required, including the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF, and Harmful Sexual Behaviour Support Service. The DfE guidance Behaviour in Schools, advice for headteachers and school staff February 2024, provides advice and legal duties, including support for students and staff powers in responding to incidents. Pages 31-33 offer guidance on child-on-child sexual violence and harassment, behaviour incidents online, and mobile phones.

Parents/carers will be informed of online safety incidents involving their children, and the Police will be notified if staff or students engage in behaviour deemed particularly concerning or unlawful (specific procedures apply for sexting and upskirting; refer to the section below).

The school will assess the adequacy of reporting procedures for future closures, lockdowns, isolations, etc., and make advance alternative provisions where necessary.

Actions where there are concerns about a child



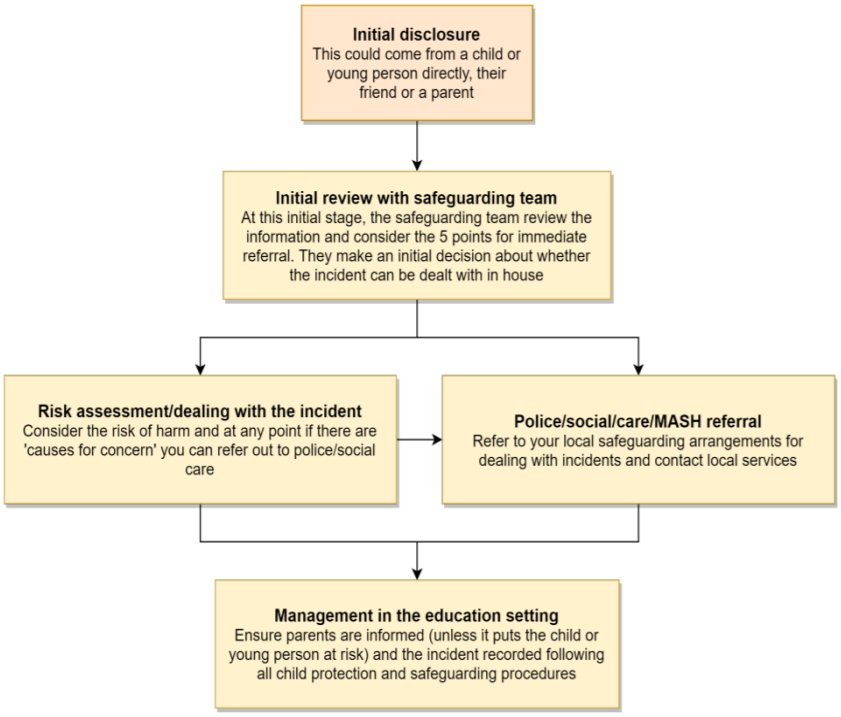
The flow chart is taken from **page 24** of **Keeping Children Safe in Education 2024** as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.

Sexting – sharing nudes and semi-nudes

All schools, regardless of phase, should follow the UK Council for Internet Safety (UKCIS) guidance on sexting, now referred to as Sharing nudes and semi-nudes: advice for education settings to prevent unnecessary criminalisation of children. Note that if one party is over 18, it is considered child sexual abuse rather than sexting.

A concise one-page overview titled Sharing nudes and semi-nudes: how to respond to an incident is provided for all staff (not limited to classroom-based staff). Recognising that incidents are often first noticed by someone other than the designated safeguarding lead (DSL) or online safety lead, it is crucial for them to take the correct initial steps. Staff, excluding the DSL, should refrain from attempting to view, share, or delete the image and should promptly report the incident to the DSL.

The school DSL will then refer to the comprehensive guidance document Sharing nudes and semi-nudes – advice for educational settings to determine the next steps and assess whether other agencies need to be involved.



***Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

It is important that everyone understands that whilst sexting is illegal, students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Upskirting

It's crucial for everyone to recognise that upskirting, which involves taking a photo of someone under their clothing (not exclusively a skirt), is now a criminal offense and constitutes a form of sexual harassment, as emphasised in Keeping Children Safe in Education 2024. Students, like in other cases of child-on-child abuse, are encouraged to approach staff if they've made a mistake or encountered issues in this regard.

Bullying

Online bullying, including incidents occurring outside of school or from home, should be addressed using the school's bullying policy, treating it like any other form of bullying. This includes issues related to ***banter*** and may be referred to as cyberbullying.

Child-on-child sexual violence and sexual harassment

Part 5 of Keeping Children Safe in Education addresses 'Child-on-child sexual violence and sexual harassment.' It is beneficial for all staff to familiarise themselves with the outlined aspects in order to support a whole-school response. Case studies will be used for training purposes.

Any incident of sexual harassment or violence, whether online or offline, should be reported to the DSL, who will follow the full guidance. Staff should cultivate a ***zero-tolerance culture*** and maintain an attitude of ***'it could happen here.'*** The guidance emphasises the need to take all forms of sexual violence and harassment seriously, highlighting that behaviours often perceived as 'low level' must be treated seriously and not allowed to persist. The document specifically mentions behaviours such as bra-strap flicking and the careless use of language.

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

Clear and well-communicated rules and procedures are crucial to govern the use of school networks, internet connectivity, devices, cloud platforms, and social media by both students and adults, both on and off school premises. These guidelines are outlined in the relevant Acceptable Use Policy and within this document, particularly in sections pertaining to the professional and personal use of school platforms, networks, clouds, devices, and other technology, as well as the BYOD (bring your own device) policy.

Any violation of these rules by students will be subject to the school's behaviour policy, and staff members found in contravention will face actions in line with the staff code of conduct. At Lakelands Academy we will reinforce these rules at the beginning of each school year and remind students of their applicability during home learning in any future periods of absence, closure, or quarantine.

In addition to these measures, ***the school retains the right to withdraw access temporarily or permanently to such technology or the right to bring devices onto school property***. With the DSL leading new responsibilities for filtering and monitoring in line with the latest DfE standards, there may be an increase in the discovery of such incidents in the coming year. The school will make efforts to remind students and staff of this heightened scrutiny at the start of each academic year.

Social media incidents

Refer to the social media section later in this document for rules and behaviour expectations for both students and adults in the Lakelands Academy community. These guidelines are also governed by school Acceptable Use Policies and the school social media policy.

Breaches will be addressed in accordance with the school behaviour policy for students or the code of conduct for staff. Additionally, in the case of an inappropriate, upsetting, violent, or abusive social media post by a member of the school community, Lakelands Academy will request the prompt deletion of the post.

If the offending post is made by a third party, the school may report it to the hosting platform and may seek assistance from the Professionals' Online Safety Helpline (POSH), run by the UK Safer Internet Centre, to expedite the resolution process.

Data protection and cybersecurity

All members of the school community, including students, staff, governors, volunteers, contractors, and parents, must adhere to the school's data protection and cybersecurity policy. It's crucial to recognise the interconnection between data protection, cybersecurity, and a school's ability to safeguard children effectively. KCSIE highlights this relationship and references the DfE Standards of Cybersecurity for the first time in 2023.

It's essential for schools to understand that data protection does not impede the sharing of information for the purpose of ensuring children's safety. As stated in the 2024 guidance on Data Protection in Schools, *"It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child."* Additionally, KCSIE 2024 emphasises, *"The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."*

Appropriate filtering and monitoring

Keeping Children Safe in Education has consistently emphasized the need for schools to implement "appropriate" web filtering and monitoring systems, ensuring the safety of children online without unnecessary restrictions.

In KCSIE 2024, acknowledging the critical role of these systems in child safety, the designated safeguarding lead now holds primary responsibility for filtering and monitoring (refer to page 2 – 'Key people'). Schools are also asked to follow the new DfE filtering and monitoring standards, which require them to:

- **identify and assign roles and responsibilities to manage (locally) filtering and monitoring systems.**
- **review filtering and monitoring provision at least annually.**
- **block harmful and inappropriate content without unreasonably impacting teaching and learning.**
- **have effective monitoring strategies in place that meet their safeguarding needs.**

As schools adapt to these new standards, DSLs and SLT face the challenge of comprehending, evaluating, and steering decisions in this area. Closer collaboration between our IT Network staff and safeguarding team is essential, with IT Network staff tasked to conduct routine checks and provide feedback to our safeguarding team. IT Network staff:

- Monitor individual devices through software or third-party services.
- Montor network using SENSO alerts.
- Review of log files of internet traffic and web access.

THE DSL will take lead responsibility for any safeguarding and child protection matters picked up through monitoring. The monitoring of devices is managed by our IT Network staff and/or third-party providers through:

- Making sure monitoring systems are working as expected.
- On request, provide reports on pupil device activity.
- Participating in safeguarding training, including online safety.
- Recording and reporting safeguarding concerns to the DSL.
- Making sure data is received in a format that is easily understood.

- Making sure users are identifiable, so we can trace concerns to an individual, including guest accounts.

ALL STAFF will be informed about the changes, heightened emphasis, and contribute by reporting concerns, potential for students to bypass systems and any potential over blocking. Concerns can be submitted at any time through CPOMS, and feedback will be solicited during regular checks.

Staff will receive reminders about systems and responsibilities during induction, start-of-year safeguarding, through AUPs, and periodic training updates aligned with the annual review and routine checks. It's crucial for schools to grasp the distinctions between filtering and monitoring, comprehend terms like overblocking, and optimise system utilisation.

Since monitoring can't stop unsafe activity, our staff should make every reasonable effort to:

- Provide effective supervision.
- Take steps to maintain awareness of how devices are being used by pupils.
- Report any safeguarding concerns to the DSL.

At Lakelands Academy:

- web filtering is provided by Telford & Wrekin LA, via Lightspeed, on the school site and for school devices used in the home.
- changes can be made by the Headteacher, Business Manager and/or IT Network Technician.
- overall responsibility is held by the DSL with further SLT support from the Deputy Headteacher.
- technical support and advice, setup and configuration are available from the IT Network Technician.
- Regular checks (scheduled evaluations of our filtering and monitoring systems to ensure they are configured correctly, active, and effective at safeguarding pupils and staff. These checks aim to identify any technical issues or vulnerabilities in the system)

Why regular checks are crucial:
These checks ensure our school's systems remain robust against emerging threats and help maintain compliance with safeguarding standards. They also provide reassurance to staff, pupils, and parents/carers that online safety measures are prioritised.

Key details about regular checks:

- **Purpose of checks:**
  - Ensure systems are operational and have not been deactivated or altered.
  - Identify any gaps in filtering that could expose pupils or staff to harmful content.
  - Verify that new devices and services are properly integrated into the system.

- **Frequency:**
  - Half-termly (unless context or risk assessments suggest a higher level of threat).

- **Responsibilities:**
  - The **Strategic Desktop Support Officer** typically conducts the technical checks.

        - The **Online Safety Coordinator** oversees the process, ensures issues are addressed, and reviews evidence, such as filtering logs.
        - Collaboration with the IT service provider (Telford & Wrekin) is essential to maintain system reliability.

    - **Scope of checks:**
        - **Devices and services:** Review school-owned devices (both on-site and off-site) and services for consistent filtering.
        - **Site areas:** Check functionality in various geographical areas across the school, including classrooms and communal spaces.
        - **User groups:** Verify systems are operational for different user categories, such as staff, students, and guests.

    - **Additional actions:**
        - Ensure all staff know how to report and record concerns related to filtering or inappropriate content.
        - Review and update the list of blocked sites to reflect current safeguarding risks.
        - Test the filtering system using appropriate testing tools.
        - A filtering and monitoring review and checks template is attached as appendix C.

    - **Documentation:**
        - Maintain a filtering log to document checks, findings, and any updates made. This log should be regularly reviewed by the Online Safety Coordinator.

We undertake an annual review in order to:

- Ensure compliance with safeguarding standards.
- Adapt systems to emerging threats and changes in school practices.
- Protect pupils and staff while building a proactive safeguarding culture.

Purpose of the review:

- Confirm that the system protects against known and emerging risks.
- Determine whether it supports the school's current and future needs, such as remote access or the use of new technologies.

When to conduct a review:

- At least once a year (e.e: during the summer term to prepare for September).
- Additionally, after identifying new risks, introducing new technologies, or implementing changes in working practices.

Who should be involved:

- Online Safety Group:
    - Online Safety Lead or Coordinator.
    - Designated Safeguarding Lead (DSL).
    - Strategic Desktop Support Officer.
    - IT Subject Specialist.
- IT service provider.
- Link-Governor responsible for online safety.

Messaging systems (including email, learning platforms etc.)

Authorised systems

- Students at this school are able to communicate with each other and with staff using:
    - School email (this is monitored by SENSO and has to pass through email filters)
    - Satchel:One notes (including discussion notes).
    - MS Teams (this is monitored by SENSO and has to pass through email filters).
    - Mathswatch (feedback on homework)
    - Exampro (feedback on work/answers)
    - Unifrog (work experience communications)

- Staff at this school use the email system provided by Telford & Wrekin LA for all school emails. They should never use a personal/private email account (or other messaging platform other than the school ParentMail account) to communicate with students or parents/carers, or to colleagues when relating to school/student data, using a non-school-administered system.

Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, students and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.
Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed. Approval, depending upon context may be given by the following: Headteacher, Data-Protection Officer (Deputy Headteacher), and/or the Business Manager.

Any unauthorised use of an alternative system may raise safeguarding or disciplinary concerns, requiring notification to the DSL (if by a student) or the Headteacher (if by a staff member). In cases where devices have multiple accounts for the same app, errors can occur, leading to actions like sending emails or uploading data to the wrong account. If a private account is mistakenly used for communication or data storage, the DSL/Headteacher/DPO (determined by the incident's specifics) should be informed immediately.

Behaviour/usage principles

- Refer to the ***Social media*** section, acceptable use agreements, behaviour policy, and staff code of conduct for detailed information on the following points.
- Maintain appropriate behaviour, refraining from sending materials or language that could be deemed bullying, aggressive, rude, insulting, illegal, or otherwise inappropriate. For staff, avoid actions that may bring the school into disrepute or compromise professionalism.
- Adhere to data protection principles in all school communications, following the school's Data Protection Policy and using authorised systems.
- Students and staff can use the email system for reasonable personal use (not excessive or during lessons), with awareness of monitoring. All communications must comply with rules of appropriate behaviour. Emails containing inappropriate content may be blocked and subject to the relevant policy and procedure.

Online storage or learning platforms

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc.

For all these, it is important to consider data protection and cybersecurity before adopting such a platform or service and at all times when using it. Lakelands Academy has a clear cybersecurity and data protection policy which staff, governors and volunteers must follow at all times.

School website

The school website serves as a vital public information platform for both current and potential stakeholders, carrying significant reputational value. The day-to-day responsibility for updating the website and ensuring compliance with DfE requirements has been delegated to (Jacky Warren) by the Headteacher and Governors. The site is managed in school by the Headteacher.

When staff contribute information to the website, it is crucial to uphold copyright laws, as schools can face substantial fines for copyright breaches. Proper crediting of sources and obtaining permission for material usage are mandatory. Numerous open-access libraries offer public-domain images/sounds that can be utilised. Simply finding content on Google or YouTube does not guarantee compliance with copyright laws. In case of uncertainty, consult with Mr Mark Hignett Headteacher/DSL/Online Safety Lead.

Digital images and video

When a student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For social media
- For a specific high-profile image for display or publication

Whenever a photo or video is captured, the staff member will verify the most recent database before utilising it for any purpose. In public-facing materials, students are never identified with more than their first name, and photo file names/tags exclude full names to prevent inadvertent sharing. All staff are bound by their employment contract and the school's Acceptable Use Policy, which addresses the use of mobile phones/personal equipment for photographing students and specifies storage protocols.

At Lakelands Academy no member of staff will ever use their personal phone to capture photos or videos of students unless with prior consent from the Headteacher. This will only be for appropriate use, where an appropriate alternative is not available, linked to school activities, taken without secrecy and not in a one-to-one situation. Photos are always moved to school storage as soon as possible, after which they must be deleted from personal devices or cloud services (NB - many phones automatically back up photos).

Photos are stored with Microsoft One Drive which is cloud based in accordance with the school's Data Protection Policy retention schedule. Staff and parents are reminded, as appropriate, about the importance of not sharing without permission, considering child protection, data protection, religious or cultural reasons, and personal privacy. We encourage responsible online behaviour, emphasising the significance of maintaining a positive digital footprint. Students learn about image manipulation and are guided on publishing content suitable for various audiences, including governors, parents, or younger children.

Students are cautioned about the potential risks of sharing personal photos on social media and are educated on maintaining privacy settings. They are instructed not to post images or videos of others without consent, understanding the risks associated with revealing identities and locations. Students are educated on keeping their data secure and how to respond to bullying or abuse and about promoting a safe online environment.

Social Media

Lakelands Academy follows the principle that effective management of our social media reputation is crucial, recognising that if we don't handle it, someone else will. Online Reputation Management (ORM) involves understanding and overseeing our digital footprint, considering everything visible or accessible about the school online. Many parents research schools online before applying, and Ofsted pre-inspection checks include online monitoring.

Negative online coverage often leads to disruptions, with up to half of cases handled by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involving schools' and staff members' online reputation. Consequently, we carefully manage and monitor our social media presence to stay informed about discussions regarding the school and respond to criticism and praise responsibly.

Mr Mark Hignett Headteacher/DSL/Online Safety Lead oversees the management of our X (Twitter), Facebook and Instagram (plus any additional accounts added following the ratification of this policy), checking Wikipedia, Google reviews, and other online mentions.

Staff, students' and parents' SM presence

Social media, encompassing various apps, sites, and interactive games, is an integral part of modern life, acknowledged and accepted by our school community, including parents, staff, and students. Complying with our acceptable use policies, signed by all members of the school community, we anticipate respectful and positive behaviour in online interactions, mirroring face-to-face conduct.

This positive behaviour entails refraining from making posts that may be perceived as bullying, aggressive, rude, insulting, illegal, or otherwise inappropriate. This expectation applies to both public pages and private posts, such as those within parent chats, pages, or groups.

Parents with concerns about the school are encouraged to contact us directly and privately for resolution. If unresolved, follow the school complaints procedure (available via our website or on request). Publicly sharing complaints on social media is unlikely to help and may cause distress, impacting staff, students, and parents, as well as the school's reputation.

While many social media platforms have a minimum age of 13 (note WhatsApp is 16+), the school encounters issues involving students under 13 on these platforms. Parents are urged to respect age ratings and discourage underage use, as stricter age verification measures are expected with Online Harms regulation.

The school aims to strike a balance between discouraging underage use and addressing the reality of students' online engagement. Online safety lessons cover social media behaviour, being a good online friend, and reporting issues. Parents can support by discussing their child's online activities, referring to the Digital Family Agreement, Top Tips for Parents ,resources from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

Official communication with the school should be through email, not social media or chat apps like WhatsApp. 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. Students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. Staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher 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 (if by a child) or to the Headteacher (if by a staff member).

Staff must uphold professionalism by maintaining strict privacy settings and avoiding inappropriate sharing on social media to prevent bringing the school or the profession into disrepute. Discussing the school or stakeholders on social media is prohibited, as personal opinions could be wrongly attributed to the school, trust, or local authority, causing reputational harm.

Inappropriate social media behaviour has led to numerous Prohibition Orders from the Teacher Regulation Agency. The school community is reminded to adhere to the Digital Images and Video policy, seeking permission before sharing photographs, videos, or information about others. The Acceptable Use Policies and the Data Protection Policy signed by all members are applicable to social media activity (available on our website or via request).

Device usage

AUPs provide guidelines on the proper use of school technology, emphasising that devices used at home should adhere to the same standards as if they were in the presence of a teacher or colleague. Please refer to the relevant sections of this document, such as copyright, data protection, social media, misuse of technology, and digital images and video, in conjunction with the AUPs.

Personal devices (including wearable technology and BYOD)

- **Students** are allowed to bring mobile phones in to school for emergency use only, but not when moving around the school buildings. During lessons, phones must remain turned off at all times and placed out of site inside the student's bag or securely in their pocket. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to and the withdrawal of mobile phone privileges. Important messages and phone calls to or from parents can be made at the school office, who will also pass on messages from parents to students in emergencies.
- Under no circumstances **should staff who work directly with students** have their mobile phone or personal device on their desk or on display in the classroom. They should remain on silent and only used in private staff areas during school hours. See also the 'Digital images and video' section of this document and the school data protection cybersecurity policies. 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, contractors, 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. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the Headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. 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, please refer to the Digital images and video section of this document on page 16. Parents are asked not to call students on their mobile phones during the school day; urgent messages can be sent via the school office.
- **All visitors** to the school site receive a 'visitor information booklet' which contains specific requirements relating to mobile device use.

Use of school devices

- Staff and students must adhere to the school's acceptable use policies (AUPs) for appropriate behaviour on school devices, whether on-site or at home.
- The use of school devices should comply with AUPs, the behaviour policy, and staff code of conduct.
- Wi-Fi access is available to all groups listed under Appendix A for school-related internet use, with restrictions outlined in the acceptable use policy. All such use is monitored.
- School devices, whether used at home or school, are limited to the apps/software installed by the school and may only be used for the student's learning and not for personal use.
- All device and system usage, including platforms, may be tracked.

Trips

During school trips or events away from the school, teachers will be provided with a school duty phone for authorised or emergency communications with students and parents. Any deviation from this policy will be promptly reported to the Headteacher. In the event of an emergency, if a teacher uses their personal phone, they will ensure that their number is hidden to maintain privacy.

Searching and confiscation

In line with the DfE guidance Searching, screening and confiscation: advice for schools, the Headteacher and staff authorised by them have a statutory power to search students/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. Full details of the school's search procedures are available in the school Behaviour for Learning and Relationships Policy.

Appendix A - Roles

All school staff **must** read the **"All staff"** section as well as any other relevant to specialist roles.

Roles:

- **All staff**
- **Headteacher** - Mr Mark Hignett
- **Designated Safeguarding Lead/Online Safety Lead** - Mr Mark Hignett
- **Governing body - Link governor/ Trustee for safeguarding and online safety** - Mrs Debbie Simmonds
- **RSE/PSHEE Lead** - Mrs Rhiannon Jones and **Computing Teacher –** Mr Tim Purslow
- **Online Safety Coordinator** – Mr Mark Hignett
- **Faculty leaders (inc. Subject Leader)** - Claire Clewlow, Josh Smallbone, Emily McGill, Karen Williams, Vicky Heath, Deb Campbell
- **Network Manager** - Gavin Shropshire
- **Data Protection Officer (DPO) -** Gerard Pyburn
- **Volunteers and contractors (including tutors)**
- **Students**
- **Parents/carers**
- **External groups**

All staff

All staff are required to sign and adhere to the staff acceptable use policy, aligning it with the school's main safeguarding policy, code of conduct, and relevant sections of Keeping Children Safe in Education for a comprehensive school-wide safeguarding approach.

This entails promptly reporting any concerns to the designated safety lead specified in the AUP, staying informed about current online safety issues (refer to the beginning of this document for 2024/25 issues), following guidance such as KCSIE, exhibiting safe and responsible behaviour in their technology use both in and outside of school, and refraining from using alarming or victim-blaming language.

Staff should also be mindful of the new DfE standards, stay informed about changes to filtering and monitoring, and contribute feedback regarding issues like overblocking, gaps in provision, or students circumventing protections.

Headteacher – Mr Mark Hignett

Key responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding.
- Oversee and support the activities of the designated safeguarding lead team and ensure they work technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school).
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance.
- Ensure **ALL** staff undergo safeguarding training (including online-safety) at induction and with regular updates and that they agree and adhere to policies and procedures.

- Ensure **ALL** governors and trustees undergo safeguarding and child protection training and updates (including online-safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements.
- 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 remote systems are implemented according to child-safety first principles.
- Understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards—through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
- Regular checks and annual reviews, upskilling the DSL and appointing a filtering and monitoring governor.
- Liaise with the designated safeguarding lead (where they are not the same person) on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Support safeguarding leads and technical staff as they review protections for students in the home and remote-learning procedures, rules and safeguards.
- 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 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.
- 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 students, including risk of children being radicalised.
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead/Online Safety Lead – Mr Mark Hignett

Key responsibilities:

- The DSL should "take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).
- Ensure "An effective whole school approach to online safety" as per KCSIE.
- Collaborating with technical colleagues, SLT, and the new filtering governor to take responsibility for filtering and monitoring. This involves gaining a deeper understanding, reviewing, and driving the rationale behind existing systems, initiating regular checks and annual reviews, and providing support for home devices.
- Where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible, but which cover areas of online safety (e.g. RSE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to students confused.
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated. This must include filtering and monitoring and help them to understand their roles.
- all staff must read KCSIE Part 1 and all those working with children also Annex B – translations are available in 13 community languages at kcsietranslate.lgfl.net (B the condensed Annex A can be provided instead to staff who do not directly work with children if this is better)
- Cascade knowledge of risks and opportunities throughout the organisation.

- Ensure that ALL governors and trustees undergo safeguarding and child protection training (including online-safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated.
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.
- 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 closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school).
- Work with the Headteacher (where not the same person), DPO and governors to ensure a 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 Prevent awareness 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 – see weekly newsletters, monthly spotlights and pre-recorded webinars from S4S.
- Ensure that online-safety education is embedded across the curriculum in line with the statutory RSE guidance 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, including hard-to-reach parents – see newsletters to parents and our website.
- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), 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 students to disclose issues when off site, especially when in isolation/quarantine, e.g. a survey to facilitate disclosures and an online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox
- Ensure staff adopt a **zero-tolerance**, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).
- Pay particular attention to online tutors, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP.
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the RSE 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.

Governing body - Link governor/Trustee for safeguarding and online safety - Mrs Debbie Simmonds

Key responsibilities:

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Undergo safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated.
- Ensure that all staff also receive appropriate safeguarding and child protection, including online training at induction and that this is updated.
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards.
- Support the academy 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 meetings.
- Work with the DPO, DSL and headteacher to ensure a 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 academy staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B.
- Ensure that all staff undergo safeguarding and child protection training, including online safety and now also reminders about filtering and monitoring.
- "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" KCSIE 2025.

RSE/PSHEE Lead – Mrs Rhiannon Jones and
Computing Teacher – Mr Tim Purslow

Key responsibilities, as listed in the 'all staff' section, together with:

- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHEE/RSE and Computing curriculums. "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."
- Focus on the underpinning knowledge and behaviors outlined in Teaching Online Safety in Schools in an age appropriate way to help students to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress" to complement the computing curriculum,.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHEE/RSE and Computing.

- 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.

Online Safety Coordinator - Mr Mark Hignett

Key responsibilities, as listed in the 'all staff' section, together with:

- 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.
- Oversee and lead on our approach to cyber-security and being robust in our approach.
- Collaboration with the IT Network Manager regarding effective filtering and monitoring software and processes.

Faculty leaders (inc. Subject Leader)

Key responsibilities, as listed in the 'all staff' section, together with:

- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSE and Computing curriculums, and model positive attitudes and approaches to staff and students alike.
- Consider how teaching Online Safety in Schools can be applied in your context.
- Work closely with the DSL/OSCo/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Ensure subject specific action plans also have an online-safety element.

Strategic Desktop Support Officer - Mr Gavin Shropshire

Key responsibilities, as listed in the 'all staff' section, together with:

- Collaborate regularly with the DSL and leadership team (including OSCo) to help them make key strategic decisions around the safeguarding elements of technology.
- Note that KCSIE changes expect a great understanding of technology and its role in safeguarding when it comes to filtering and monitoring and you will be required to support safeguarding teams to understand and manage these systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems - what is allowed, blocked and why and how 'overblocking' is avoided as per KCSIE, to support their role as per the new DfE standards, protections for students in the home and remote-learning.
- 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, Online Safety Coordinator, Data Protection Officer, Relationships and Sex Education Lead and Computing Teacher to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- 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.
- 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.
- Liaise with the data protection officer and the online safety group to ensure the data protection and cybersecurity policies are up to date, easy to follow and practicable.
- 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.

Data Protection Officer (DPO) - Mr Gerard Pyburn

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and Cybersecurity Policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2024, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2024, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."
- Note that retention schedules for safeguarding records may be required to be set as 'Very long-term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records.
- Ensure that all access to safeguarding data is limited as appropriate and monitored and audited.

Volunteers and contractors (including tutors)

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.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviors in their own use of technology at school and as part of remote teaching or any online communications.
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the academy, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Students

Key responsibilities:

- Accept and adhere to the Student Acceptable Use Policy**.**

Parents/carers

Key responsibilities:

- Read, sign and adhere to the school's Parental Acceptable Use Policy (AUP), read the pupil AUP and encourage their children to follow it.

External groups:

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within the academy.
- Support the academy in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviour 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, students or other parents/carers.

Appendix B – Acceptable Use Policies

Lakelands Academy Acceptable Use Policy - Students

The computer system is owned by the school. This Acceptable Use statement helps to protect students, staff and the school by clearly stating what use of the ICT resources is acceptable and what is not

- I will only use the school internet and network for my schoolwork or when a teacher has given permission. When temporarily leaving a workstation, it should be locked. (Win + L) to prevent unauthorised access.
- I will not look at or delete or amend other people's work or files.
- I will treat all IT equipment at school with respect and ensure the computer or mobile device is left in the state that I found it
- I will not install software on school IT facilities due to the risk of damage being caused by malware or viruses.
- I will not share my network, internet or any other school-related passwords. I will exorcise caution before giving out any personal details, or information about the school, over the network.
- I will only use my school-supplied email address for school-related activities.
- I will respect copyright when making use of images, videos or other media in my schoolwork
- I will be responsible and polite when I talk online to pupils, teachers and other people related to the school, both in school-time and outside school-time.
- I will not upload or download any pictures, writing or films which might upset people online or within the school.
- I will not share inappropriate images or videos of other pupils on the school network or personal devices.
- I will not look for, view, upload or download offensive, illegal, extremist, copyright-infringing or pornographic material. If I find such material on school IT equipment I will inform a teacher immediately.

The school may exercise its right to monitor the use of all the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is taking place, or the system is used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. Monitoring is triggered when a violation of this policy is registered on the system.

Acceptable Use Policy for Staff, Governors & Volunteers

I understand that I have personal and legal responsibilities, including treating others with dignity and respect, acting honestly, using public funds and school equipment appropriately, adhering to health and safety guidelines and safeguarding pupils at all times.

I understand that I must use school devices and systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of systems and other users.

I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to benefit from the use and application of appropriate digital technology.

I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with children and young people.

Professional and personal safety:

- I understand that the school has in place a filtering system and will monitor my access to digital technology and communications systems whilst using school devices, and/or access to the school network via personal devices, where such access has been granted.
- I understand that the rules set out in this agreement also apply to use of school devices and digital technologies out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use in line with the general principles of this agreement and the expectations of professional behaviour set out in the Staff Code of Conduct.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should keep passwords safe and not share them with anyone.
- I will immediately report any incidence of access to illegal, inappropriate or harmful material, deliberate or accidental, by myself or others, to the appropriate person.
- I will not install or attempt to install programmes of any type on a device, nor will I try to alter computer settings, unless this is permitted by the Network Manager.
- I will not deliberately disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Lakelands Academy Privacy Notice for Students & Parents/Carers
- I understand that Data Protection Policy requires that any staff or student data to which I have access, will be kept private and confidential, except when required by law, or by school policy, to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving devices or software, however this may have happened.
- I have permission to access pupil areas to mark work
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will log out of a device when I have finished using it.

Electronic communications and use of social media:

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will use social networking sites responsibly, taking care to ensure that appropriate privacy settings are in place, and ensure that neither my personal nor professional reputation, nor the school's reputation, is compromised by inappropriate postings, to include past postings.
- I will never send or accept a 'friend request' made through social media from a student at school. I understand that such requests should be raised formally as an incident.
- I will not, under any circumstances, make reference to any staff member, student, parent or school activity/event via personal social media or other communication technologies.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner. At no time will I use or share a personal email address, phone number or social networking site for such communication purposes.
- I will notify the Headteacher of any current or future, direct or incidental contact with students, parents or carers, for example where parents or carers are part of the same social group
- I will not engage in any online activity, at, or outside school, that may compromise my professional responsibilities. This includes making offensive, aggressive or defamatory comments, disclosing confidential or business-sensitive information, or information or images that could compromise the security of the school.
- I will not use the school's name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material, online or in print.
- I will not post any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school.

Use of school and personal mobile devices and technologies

- When I use my own mobile device (e.g. laptop / tablet / mobile phone / USB device) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will keep my personal phone numbers private and not use my own mobile phone, or other device, to contact students or parents in a professional capacity.
- I will keep my mobile phone secure whilst on school premises. If I need to use my mobile phone whilst in school or on school duties I will ensure that use is discreet and appropriate, e.g. not in the presence of students.
- I will keep mobile devices switched off and left in a safe place during lesson times. I understand that the school cannot take responsibility for personal items that are lost or stolen.

- I will report any text or images sent to me by colleagues or students which could be viewed as inappropriate. I will not use a personal device to photograph a student(s), except with the written permission of the Headteacher.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails if I have any concerns about the validity of the email or its source is neither known nor trusted.
- I will, when I take and/or publish images of others, do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use any personal devices to record these images, unless I have written permission from the Headteacher. Where these images are approved by the school to be published (e.g. on the school website) it will not be possible to identify by name, or any other personal information, those who are featured.
- I will not attempt to upload, download or access any material which is illegal (for example; images of child sexual abuse, criminally racist material, adult pornography), inappropriate or may cause harm or distress to others. I will not attempt to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

Conduct and actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school devices and digital technology in school, but also applies to my use of school systems and equipment off the premises. This Acceptable Use Policy also applies to my use of personal devices on the premises or in situations related to my employment by the school.
- I understand that should I fail to comply with this Acceptable Use Policy Agreement, I may be subject to disciplinary action in line with the school's agreed Disciplinary Procedure. In the event of any indication of illegal activity, I understand the matter may be referred to the appropriate agencies.

I have read and understood the above and agree to use school devices and access digital technology systems (both in and out of school), as well as my own devices (in school and when carrying out communications related to the school), within this agreement.

I understand that in the event of any query or concern about this Agreement, I should contact Mr M Hignett E-Safety Co-ordinator.

Staff / Volunteer Name:	
Signed:	
Date:	

Appendix C

Filtering and monitoring review and checks template

This includes:

- A filtering and monitoring review template
- A filtering and monitoring checks template

Filtering and monitoring: review template

Review your filtering and monitoring provision **annually**, or where:

- You identify a safeguarding risk
- There's a change in your working practice (e.g. you allow remote access or staff to bring their own device)
- You introduce new technology

Use your filtering and monitoring review to inform:

- Your school's related safeguarding or technology policies and procedures
- Roles and responsibilities
- Staff training
- Curriculum and learning opportunities
- Procurement decisions
- What is checked, and how often
- Monitoring strategies

Policy Approved: 1 April 2025
Review Period: 1Yr
Policy Responsibility: BM
Policy Approval: FGB

REVIEW	COMMENTS	NEXT STEPS/ACTIONS
If you're part of a multi-academy trust (MAT): is the level of online protection the same across all schools in the MAT?	*For example: Yes, but not all schools are using the same filtering and monitoring software*	• *Work with schools to roll out a consistent system across all schools*
What is the risk profile of your pupils? ○ Their age range ○ Pupils with special educational needs and disabilities (SEND) ○ Pupils with English as an additional language (EAL)	*For example: We have a high proportion of pupils with SEND who access individual tablets as part of their learning*	• *Termly checks on pupil tablets to make sure filtering systems are still in place and effective* • *Procure a monitoring system that allows teachers to view tablet screens for all pupils during a lesson*
Does your filtering and monitoring system adhere to the technical requirements?		
What does your filtering system currently block or allow, and why?		

REVIEW	COMMENTS	NEXT STEPS/ACTIONS
What limitations are there to your filtering system? How will you mitigate them?		
How do you know your filtering and monitoring system meets the needs of your school? Use your prevent risk assessment help you decide what's appropriate for your school		
What outside safeguarding influences impact your school? At Lakelands Academy: County lines, Domestic abuse….		
Are there any relevant safeguarding reports that impact your filtering and monitoring?		

REVIEW	COMMENTS	NEXT STEPS/ACTIONS
What is the digital resilience of your pupils? • This means whether your pupils have the knowledge and skills to make decisions online that keep themselves safe, and whether they know what to do if they come across something that's wrong		
Are you clear on your teaching requirements, for example, your RHSE and PSHE curriculum?		
Does your school outline any specific uses of technologies? For example: do you allow staff and/or pupils to 'Bring Your Own Device' (BYOD)?		
What related safeguarding or technology policies do you have in place?		

REVIEW	COMMENTS	NEXT STEPS/ACTIONS
What checks are currently taking place? (use our template below to help you) How do you handle any resulting actions?		

Filtering and monitoring: checks template

You need to carry out physical checks on your systems to make sure they're properly configured and that they haven't been changed or deactivated.

It's likely your IT service provider will carry out these checks in practice, but you still need to work with them and oversee the checks they're doing.

Do these checks termly, but you may decide to do them more often based on:

- Your context
- The risks highlighted in your review (above)
- Any other risk assessments

Your checks should cover a range of:

- School-owned devices and services, including those used off site
- Geographical areas across the site
- User groups, e.g. teachers, pupils and visitors

CHECKS	DATE OF CHECK	WHO DID THE CHECK	RESULTING ACTIONS
Have we checked that our filtering and monitoring system is still fit for purpose? You can signpost your IT service provider to South West Grid for Learning's (SWGfL) testing tool.			
Is the system running and working?			
Have we checked that our filtering and monitoring system works on: › All devices › New devices and services before they're given to staff or pupils			
Have we reviewed the list of blocked sites on our network? Is this list still accurate/does it reflect any changes to safeguarding risks?			
Does our filtering system adhere to the requirements?			
Does our monitoring system adhere to the requirements?			