LLOYD WILLIAMSON
FOUNDATION

The Lloyd Williamson Schools Foundation

ONLINE SAFETY POLICY

Introduction

This policy applies to Lloyd Williamson Schools Foundation. The term schools/school encompasses nursery and EYFS provision, Lower School and Upper School.

LWSF recognises that IT and the internet are excellent tools for learning and communication that can be used to enhance the curriculum, challenge pupils, and support creativity and independence. Using IT to interact socially and share ideas can benefit everyone at LWSF.

It is important that IT is used responsibly. Pupils, staff and parents should use it appropriately and maintain safety online. We recognise the importance of being aware of the dangers of using the internet and how members of LWSF should conduct themselves online.

Online safety covers the Internet, but it also covers mobile phones and other electronic communication technologies. We know that some adults and young people may attempt to use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

Education about the risks and responsibilities of online safety falls under the duty of care for safeguarding.

We encourage a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential.

This policy should be read alongside all relevant policies pertaining to safeguarding, including – though not limited to:

- Safeguarding and Child Protection Policy
- Children Missing from Education Policy
- Prevent Strategy
- Anti-bullying Policy
- Exclusion Policy
- Media Policy
- Cyber-security Policy
- E-Safety Policy: Bring Your Own Device (BYOD) Policy for Staff and Visitors
- Data Protection Policy
- Use of Computers and Internet Access Policy
- Whistleblowing Policy
- Allegations of Abuse Against Staff Policy
- Safer Recruitment Policy
- Staff Code of Conduct
- Behaviour Policy

This policy covers fixed and mobile internet devices provided by LWSF (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils and staff brought onto school premises (personal laptops, tablets, wearable technology e.g. smart phones and watches, etc.).

Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed. We include occasional information in the schools' weekly newsletter.

Using IT and the Internet

The Internet is used at LWSF to support learning and the professional work of staff. Technology is part of everyday life, education and business. We aim to equip our pupils with the IT skills they will need to enable them to progress confidently into a professional working environment when they leave school. We balance this with a need to prepare children for the risks inherent in using technology. Children are taught to use the internet and ICT safely.

Issues within online safety are categorised into four areas of risk (KCSiE 2024):

- **Content**: being exposed to illegal, inappropriate or harmful material, e.g., pornography, fake news, racist or radical and extremist views

- **Contact**: being subjected to harmful online interaction with other users; e.g., commercial advertising as well as adults posing as children or young adults

- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm: e.g., making, sending, and receiving explicit images, or online bullying

- **Commerce**: being exposed to risks such as online gambling, inappropriate advertising, phishing and or financial scams

Responsibilities

Board of Trustees

In line with KCSIE , the trustees are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy by reviewing online incidents and monitoring reports.

Online safety falls within the remit of the trustee responsible for Safeguarding.

The role of the safeguarding trustee will include:

- ensuring an online safety policy is in place, reviewed every year and/or in response to an incident

- ensuring that LWSF has an appointed DSL with responsibility for online safety who has been trained to a level of knowledge appropriate to the position

- ensuring that safeguarding training for staff, including online safety training, is integrated and considered as part of the whole school safeguarding approach

- ensuring that pupils are taught about safeguarding, including online safety

- ensuring that procedures for the safe use of IT and the Internet, including appropriate online filtering and monitoring systems, are in place and adhered to

- holding the Headteacher accountable for online safety

Headteacher and Senior Leadership Team

The Head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community.

The role of the Head will include:

- Ensuring access to induction and training in online safety practices for all users

- Ensuring all staff receive regular, up to date training (Educare)

- Ensuring appropriate action is taken in all cases of misuse

- Liaising with the ICT Lead to ensure that Internet filtering methods are appropriate and effective

- Ensuring that pupil or staff personal data, as recorded within school management system, sent over the Internet is secured

- Ensuring systems / policies to protect pupils are appropriate and managed correctly

- Working with the ICT Lead to make sure the IT system is reviewed regularly regarding security and that virus protection is installed and updated regularly

Designated Safeguarding Lead (DSL)

The DSL has overall responsibility for online safeguarding, including online filtering and monitoring.

The DSLs and leadership team (SLT) follow the guidance regarding online safety within ‘Keeping Children Safe in Education’; and the DfE guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.

Their role includes:

- Recognising the risks associated with online safety, including the additional risks faced by pupils with SEND
- Leading safeguarding, including online safety, meetings
- Liaising with staff on matters of safety and safeguarding, including online and digital safety
- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments
- Reporting to SLT / Headteacher about matters of online safety
- Liaising with the nominated member of the governing body and Headteacher to promote online safety
- Facilitating training / infomration for pupils, staff, Trustees / Governors and parents to improve understanding of all aspects of online safety
- Keeping up to date on current online safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International, NSPCC, and the LSCP for RBKC.

ICT Lead

ICT Lead is responsible for:

- Ensuring the technical infrastructure is secure and is not open to misuse or malicious attack
- Making sure the schools meet required online safety technical requirements
- Ensuring that staff may only access the networks and devices through a properly enforced password protection policy
- This Online Safety Policy, together with the school’s approach to filtering and monitoring (Famisafe) is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person

- Keeping up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant

- Monitoring the network / internet / email in order that any misuse/attempted misuse can be reported to the Headteacher or the DSL for investigation/action/sanction

- Monitoring software/systems and that they are implemented and updated

- Ensuring the system is reviewed regularly with regard to security and that virus protection is installed and updated regularly

Staff / Volunteers / Contractors

Staff / Volunteers / Contractors are expected to:

- Read and follow the provisions of this Policy

- Read and Agree to the Acceptable Use of IT Policy/Agreement (Staff and Trustees / Governors)

- Complete training (Educare) relating to online safety

- Address any online safety issues which may arise in classrooms on a daily basis

- Report to the DSL / Headteacher of their School if they become aware of misuse or attempted misuse of Digital

Technology within the schools

Pupils

Pupils are expected to:

- Follow the schools' Acceptable Use Guidance for pupils relating to the use of digital technology and accessing wi-fi

- Report to a DSL or Headteacher / trusted adult when they believe that the school's systems are being misused or abused in any way

Parents

Parents, guardians and carers should be fully involved with promoting online safety both in and outside of school.

It is important for parents and carers to be aware of what their children are being asked to do online, including the sites the school will ask them to access and who they will be asked to interact with online.

Parents should:

- Read policies relating to online safety, and guidance that is circulated from time to time e.g., in newsletters

Education and training

Staff: awareness and training

- Staff / Volunteers receive online safety and acceptable use information as part of their induction (online training via Educare).
- All teaching staff receive regular information and training on online safety issues in staff meetings and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. This includes updated information regarding online filtering and monitoring responsibilities and procedures in the school.
- Staff training in the schools is logged and monitored via Educare
- All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school online safety procedures.
- Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.
- All incidents relating to online safety should be reported to the DSL.

Pupils: Online safety in the curriculum

LWSF includes (appropriate to age, and stage of development) online education through PSHE, assemblies, discussion, talks and the academic curriculum.

These lessons are designed and delivered using appropriate guidance, tools, and resources. The goal is to equip all pupils with the essential knowledge and behaviours required to navigate the online world safely, in a manner suited to their age and ability.

In staff meetings/briefings we explore ideas for promoting online safety and regularly monitor the children’s understanding of it. In PSHE, pupils
are taught to consider and manage their personal online safety.

We strive to educate pupils on distinguishing between acceptable and unacceptable online behaviour, raising awareness of potential online risks, and empowering them to make informed decisions about how to act and respond. Additionally, we emphasise the importance of knowing when, where, and how to seek support if they feel concerned or upset by something they encounter online.

Where appropriate for their age, pupils are taught to recognise online dangers such as sexual exploitation, stalking, and grooming, as well as the associated risks and their responsibility to report any such incidents involving themselves or their peers. Pupils can raise concerns with the DSL or any trusted adult on the school staff.

Pupils learn to respect others' personal information and images, understand the impact of cyberbullying, and know how to seek help if affected. For further details, please refer to the school's Anti-Bullying Policy, which outlines preventative measures and the procedures followed when incidents of bullying occur.

Vulnerable Pupils

Some pupils are potentially more vulnerable online. These may include, though not limited to: children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss. It may also include those children who have received multiple suspensions or are at risk of being permanently excluded.

LWSF teachers will differentiate for ability in online safety education, access and the DSL will ensure support is provided to vulnerable pupils as needed.

LWSF will seek input from specialist staff as appropriate, including the SENCo.

Cyberbullying

LWSF takes Cyber bullying very seriously and will be dealt with by following the Behaviour Policy and Anti-Bullying Policy.

The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person.

LWSF is clear in its commitment to respecting peers, pupils, members of the public and staff. Intentional breach of this will result in disciplinary action.

If an allegation of bullying is reported, LWSF will:

- Take it seriously

- Act as quickly as possible to establish the facts – it may be necessary to check logs or contact the service provider to identify the bully

- Record and report the incident

- Provide support and reassurance to the victim and support the perpetrator via the Schools’ Behaviour Policy

The Risk of Online Radicalisation

In accordance with Prevent guidance, LWSF is committed to safeguarding children from the risk of radicalisation. Measures are in place to ensure that pupils are protected from terrorist and extremist content when accessing the internet at school and to prevent the misuse of social media for such purposes.

To support this, website filtering and monitoring systems (such as Famisafe) are used to restrict access to extremist and terrorist material, as well as social networking platforms like Facebook, Instagram, and Twitter.

For further information on how social media can be exploited to promote extremism and radicalisation, please visit the *Educate Against Hate* website: www.educateagainsthate.com.

Responding to Online Safety Incidents and Concerns

Staff are made aware of the reporting procedures for online safety and safeguarding concerns regarding pupil welfare, including: breaches of filtering, youth produced sexual imagery (sexting), upskirting, cyberbullying, online sexual harassment (including cyberflashing - sending images of one’s genitals to strangers online, which became a criminal offence on 31st January 2024), sextortion (individuals being forced into paying money or meeting another financial demand, after a person has threatened to release nude or semi-nude photos of them (this could be a real photo, or a fake image created of the victim by the person threatening its release) and illegal content. The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.

LWSF staff, volunteers and contractors must respect confidentiality and the need to follow the official school procedures for reporting concerns.

For further detailed information, the Safeguarding and Child Protection policy, Complaints Policy and Whistleblowing Policy are on the school website.

After any investigations are completed, the school will identify lessons learnt and implement any policy or curriculum changes as required.

If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the LADO. Where there is suspicion that illegal activity has taken place, the school will contact the Local Authority Safeguarding Team or the Police using 101, or 999 if there is immediate danger or risk of harm.

Any allegations regarding a member of staff’s online conduct will be referred to the Headteacher and discussed with the DSL and the LADO (Local Authority Designated

Officer) if necessary. Appropriate action will be taken in accordance with the Staff Code of Conduct / Allegations Against Staff Policy.

When made aware of concerns involving consensual and non-consensual sharing of, or the threat to the sharing of, nudes and semi-nude images and/or videos by children, staff are advised to:

- Report any concerns to the DSL immediately.
- Never view, copy, print, share, store or save the imagery, or ask a child to share or download it. If staff have already viewed the imagery by accident, this must be immediately reported to the DSL.
- Not delete the imagery or ask the child to delete it.
- Not say or do anything to blame or shame any children involved.
- Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.
- Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.

The DSL will respond to the concerns as set out in the non-statutory UKCIS guidance: Sharing nudes and semi- nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)

Monitoring and Filtering

LWSF will implement appropriate filtering and monitoring systems to safeguard pupils and staff when accessing school systems and the internet, ensuring risks are reasonably limited.

The ICT Lead and DSL/SLT regularly review these systems to assess their effectiveness, considering the specific safeguarding needs of pupils, including age-related risks and vulnerabilities such as SEND or EAL, as well as staff.

Trustees hold overall strategic responsibility for ensuring staff are trained in safeguarding, recognising that maintaining a safe online environment is a shared responsibility. They ensure adherence to the Staff Code of Conduct, policies, and procedures, and that concerns are appropriately reported and recorded.

The DSL leads safeguarding and online safety, overseeing filtering and monitoring reports, addressing concerns, and ensuring system checks are conducted.

The ICT Lead manages the technical aspects of filtering and monitoring, generating reports, and taking necessary actions when issues arise.

Identifying individuals attempting to access unsuitable or illegal material is crucial, allowing appropriate staff, such as the SLT or DSL, to provide necessary support.

LWSF reserves the right to monitor and filter employees' and pupils' internet, social media, and email usage on LWSF-provided equipment. This includes reviewing emails and photographic content to ensure compliance with policy.

All staff need to be aware of reporting procedures for safeguarding and technical concerns.

They must report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system

Incidents could be of a malicious, technical, or safeguarding nature. Staff know that in the first instance, they report their concerns to the DSL.

If it is discovered that any of the systems are being abused and/or that the terms of this Policy are being infringed, disciplinary action may be taken in accordance with LWSF's disciplinary policies and procedures.

Online Safety Review

The DSLs will review online safety as part of the annual Safeguarding Audit.

Security and Management of Information Systems

LWSF will review and manage the security of the computers and Internet networks to ensure compliance with this policy.

In line with GDPR, LWSF takes its responsibility for the protection of data very seriously. This means protecting the network, as far as is practicably possible, against viruses, hackers and other external security threats.

The ICT Lead will review the security of the Group information systems and users regularly and virus protection software will be updated regularly.

The ICT Lead will act in line with the Cyber Safety Policy. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT will be **immediately** reported to the IT team.

Emails

LWSF uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of the schools' communication.

Staff and pupils should be aware that LWSF email accounts should only be used for LWSF related matters – strictly for staff to contact parents, pupils, other members of staff and other professionals for work purposes. This is important for confidentiality. LWSF retains the right to monitor emails and their contents but will only do so if it feels there is reason to.

Staff Use of Email and the Internet

Staff should be aware of the following when using emails at LWSF:

- Staff must only use official LWSF provided email accounts to communicate with pupils, parents or carers. Personal email accounts must never be used to contact any of these people.

- LWSF permits the incidental personal use of email, the internet, social media and related types of electronic communication and information, and electronic equipment by an employee as long as it is kept to a minimum and takes place substantially out of normal working hours and only in designated areas.

- Staff should be aware that all their personal interactions (email and internet) on an LWSF provided device are logged and may be monitored.

- Use must not interfere with an employee's work commitments, or those of others. If it is discovered that excessive periods of time have been spent on the internet or other electronic media provided by LWSF, either in, or outside, working hours, disciplinary action may be taken, and internet access or use of electronic equipment may be withdrawn without notice at the discretion of the Headteacher.

- Emails sent from LWSF accounts should be professionally and carefully written. Staff are always representing the school and should take this into account when entering into any email communications.

- Where possible, staff should avoid 'replying to all' or blindly forwarding emails they have received.

- Staff must tell the Senior Leadership Team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

- The forwarding of chain messages is not permitted.

- Using photographic material of any kind to bully, harass or intimidate others is strictly forbidden and may lead to dismissal.

Pupil Use of Email
Pupils should be aware of the following when using email:

- Pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

- Pupils must be careful not to reveal any personal information over email or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

Pupils will be educated through the PSHE curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the LWSF network or their personal account or wellbeing.

Safe Use of Digital and Video Images of Pupils

Digital imaging technologies offer valuable learning opportunities, enabling staff and pupils to capture and use images instantly. However, sharing digital images online poses risks such as cyberbullying, stalking, or grooming. Once published, images can remain on the internet indefinitely, potentially leading to harm or embarrassment.

To mitigate these risks, staff will educate pupils on the responsible use of digital images, including taking, sharing, and publishing them. Pupils will also be encouraged to understand the dangers of posting their own images online, particularly on social media.

School Website and Newsletter

LWSF uses its website and newsletters to share school news, celebrate achievements, and promote projects while keeping parents, pupils, and staff informed.

All published content follows best practices for safety, copyright, and privacy. No personal information about staff or pupils will be shared and contact details will be limited to the school office.

Safe Use of a Pupil’s Digital Images and Data

Consent and Data Protection

In accordance with the Data Protection Act 2018, LWSF will not publicly display images of pupils or staff, in print or online, without consent. Upon admission, parents/carers sign a photography consent form, and pupils aged 13+ must provide their explicit consent. This prevents repeated requests for permission, as the terms of use remain unchanged.

Published images will not identify pupils without consent, and they may only be identified by their first name. Images on the school website cannot be reused or manipulated. Only school-approved images will be used publicly, and no external photography of pupils is permitted without the school's authorisation.

Guidelines for Use of Images

By Parents

- Parents may take photos or videos of their children at school events for personal use, ensuring courtesy to others. Flash photography is not permitted at indoor events.
- Parents should not take or share images of other pupils without prior consent.
- Care should be taken to ensure pupils are appropriately dressed and not depicted in ways that could bring disrepute to the school.
- LWSF does not permit the use of such images for any purpose beyond personal use.
- The school reserves the right to refuse or withdraw permission to take photographs if guidelines are not followed.
- Copyright restrictions may prevent filming or recording certain school events.

By Pupils

- Pupils are not allowed to have personal recording devices, including mobile phones, while at school or school events.
- If permitted under teacher supervision, cameras or filming devices must not be used in toilets, changing areas, or in a way that could cause harm or offense.
- Pupils must not capture, share, or publish images of others without consent.
- Sharing or threatening to share nude/semi-nude images of minors (including consensually) is illegal and will be treated as a safeguarding issue, reported to the DSL.
- Any misuse of images or recording equipment will be dealt with under the relevant school policy.

By the School

- LWSF celebrates pupil achievements and may use images/videos in promotional materials or media coverage. Consent from pupils and parents (where applicable) will be obtained before publication.
- Images/videos will not be used without appropriate consent.
- Staff and volunteers may take images for educational purposes but must follow this policy on sharing and distribution.
- Only LWSF-issued equipment may be used for capturing pupil images.

- In Early Years Foundation Stage (EYFS) settings, teachers use the EYFS Tapestry platform, which parents can access. However, parents must not share images from Tapestry.

Complaints About Misuse of Digital Images or Videos

Parents with concerns about the misuse of images or videos published by the school should follow the standard complaints procedure, outlined in the **Complaints Procedure** available on the school website. Issues will be addressed in line with **Safeguarding** policies.

Misuse of images or videos by pupils or others will be managed under the **Behaviour Policy** and **Anti-Bullying Policy**, depending on the nature of the incident. Any incidents involving the sharing of nude or semi-nude images of under-18s, which is illegal regardless of consent, will be immediately reported to the **DSL and Headteacher**.

Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are potentially more vulnerable to content, contact and conduct behavioural issues. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. There are various restrictions on the use of these sites in school that apply to both pupils and staff.

Expectations

- The expectations regarding positive, safe and responsible use of social media applies to all members of the school community. The school will control pupil and staff access to social media whilst using school provided devices and systems on site.
- All members of the school community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- Concerns regarding the online conduct of any member of the Group community on social media, should be reported to the Head and will be managed in accordance with our Anti- Bullying, Behaviour, and Safeguarding Policies, and Staff Code of Conduct.

Use of Social Media at LWSF

Staff Personal Use of Social Media

All staff will receive guidance on the safe and responsible use of social media, networking, and personal publishing sites during induction, with regular updates through ongoing training. Additional guidelines are outlined in the **Staff Code of Conduct**.

Pupils’ Personal Use of Social Media

Pupils will be taught safe and appropriate social media use as part of a structured and age-appropriate educational programme. They are expected to refrain from engaging in **threatening, hurtful, or defamatory behaviour** on social media, online games, or within the metaverse.

Official LWSF Use of Social Media

The school’s official social media accounts are used solely for **educational, community engagement and marketing purposes**,with clear objectives and intended outcomes. These accounts are securely managed and, where possible, linked to the school website.

All official social media activity must comply with **Anti-Bullying, Data Protection, Safeguarding, and Staff Code of Conduct** policies.

Use of LWSF and Personal Mobile Phones and Devices

Personal mobile devices are not permitted during the school day. Pupils must hand them in upon arrival and collect them at the end of the day.

Staff are required to store their devices in designated lockers and may only use them during breaks and in specified areas. Any misuse must be reported to the **DSL** and will be addressed in accordance with the **Staff Code of Conduct** or, for pupils, the **Behaviour Policy**.

Concerns Regarding Mobile Devices

The presence of personal mobile devices in school can lead to several issues, including:

- Increased vulnerability to **cyberbullying** for both pupils and staff.
- Access to **inappropriate online content**.
- **Disruptions** to learning and classroom focus.
- Risk of **theft, loss, or damage** of valuable items.
- Potential **safeguarding and data protection breaches** due to built-in cameras.

To maintain a safe and focused learning environment, these rules are strictly enforced.

Personal Use of Devices by Staff

- Staff must always act in the **best interests of pupils** when engaging with or contributing to social media.
- **School-issued devices** must be protected with a password or device lock to prevent unauthorised access. These devices should only be used for school-related tasks, and when not in use, must be securely locked.
- **Official photographs** may only be taken using school devices under the Headteacher's direction. These images must be downloaded exclusively onto school computers and not personal devices.
- Staff **must not** contact pupils, parents, guardians, or carers via **personal phone numbers, emails, social media, or messaging apps**.
- Wherever possible, staff must use **LWSF-owned devices** for capturing images, videos, or live streaming. All images must be saved onto the **school's shared drive** in accordance with LWSF's **information security policies**.
- Personal cameras and mobile phone cameras **must not** be used on school premises or grounds. No images of the school or pupils may be taken using personal devices.
- Personal mobile phones may only be used in **designated staff areas** or in classrooms when pupils are not present.
- Any **computing devices or wearables** connected to the school network must have up-to-date software to protect against security vulnerabilities.
- Staff must **not accept phone calls** during lessons or while supervising children, except in emergencies. Staff must use school issue mobiles for trips and outdoor lessons. Calls from the **Head, DSL, or School Office** may be answered only during events like **Sports Day, school trips, or safeguarding situations**.
- Bluetooth and other communication features such as **AirDrop** should be disabled during lesson times.
- If a staff member is suspected of storing **illegal content** on a personal device or committing an **offence**, the police will be contacted.
- LWSF **does not take responsibility** for the theft, loss, or damage of personal property, including electronic devices, which are brought to school at the owner's risk.

Use by Pupils

General Rules

- Pupils **must not** carry mobile phones or personal devices while on school premises. Devices must be handed in upon arrival and collected at the end of the day.
- The use of **mobile and smart technology** is regulated due to the potential risks, including cyberbullying, harassment, and access to inappropriate content.
- **Parents are responsible** for ensuring age-appropriate content filtering on their child's smartphone.

Restrictions and Safeguarding Measures

- These rules apply to **all internet-connected devices**, including smartwatches and wearables.
- Pupils **are not allowed** to bring mobile phones or connected devices on **residential trips or visits**.
- Mobile phones and personal devices **must not be taken into exams**. Any pupil found in possession of one during an exam will be reported to the exam board, which may result in the board not accepting their script.
- Pupils are responsible for their devices **before handing them in and after collection** at the end of the school day.

Policy Enforcement

- Concerns regarding mobile phone use will be addressed in line with **safeguarding, behaviour, and anti-bullying policies**.
- **Staff may confiscate** devices if they are used in violation of school policies. Confiscated devices will be stored securely and returned to parents/carers.
- **School leadership may search** a pupil's device with the Headteacher's authorisation. If policy violations are found, content may be deleted or requested to be deleted.
- Searches will follow the **DfE's 'Searching, Screening and Confiscation' guidance (July 2023)** as detailed in the school's **Searches – Guidance and Protocol** document.

Serious Concerns and Legal Matters

- Breaches of this policy will be managed according to the **Behaviour Policy**, with appropriate **sanctions and pastoral support**.
- Parents/carers will be informed of any serious concerns regarding their child's use of mobile technology.
- If a child is suspected to be **at risk of harm**, the school will respond in line with its **Safeguarding Policy**.
- If a device contains **potentially illegal material** or evidence of a criminal offence, it will be handed over to the **police** for further investigation.

Management of Applications which Record Children's Progress (Data and Images)

The Schools use applications such as Tapestry (EYFS) and AIMS to track pupils progress and share appropriate information with parents and carers. The Headteacher is responsible for the security of any data or images held of children. As such, they will ensure that tracking systems are appropriately risk assessed and are used in accordance with GDPR and data protection legislation.

To safeguard data:

- Only LWSF approved apps will be used to access any pupil details, data and images, and these require secure sign ins, passwords and often two-factor authentication.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

Managing Emerging Technologies

LWSF staff and pupils may use AI, proactively monitoring and keeping abreast of emerging technologies and inherent risks. This allows LWSF to promptly devise and implement suitable strategies to navigate the ever-changing technological landscape in line with the AI Policy.

Protecting Personal Data

LWSF takes its compliance with the Data Protection Act 2018 seriously. Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation. Full information can be found in the Data Protection Policy, available on the school websites.

Breaches of Policy by Employees

Staff must adhere to the **Staff Code of Conduct** and all relevant policies governing **Online Safety, Internet Use, and the Acceptable Use of IT**.

Misconduct and Disciplinary Action

- Any breach of this policy may be considered **misconduct** and will be addressed in line with the school's **disciplinary procedures**.
- The **Headteacher** reserves the right to escalate serious matters to the **Police** or other external agencies if necessary.

Employee Complaints

- Staff who have concerns about a colleague's use of **email, internet, social media, electronic images, or related communications** should report the matter to the **Headteacher or DSL**.
- Complaints from staff will be handled promptly in accordance with the **Whistleblowing Policy**.

Complaints Against Employees

- Complaints made by **pupils or parents** regarding staff breaches of this policy will be handled under the **Allegations Against Staff Policy**.
- If a breach raises **safeguarding concerns**, it will be addressed in line with the **Safeguarding Policy**.

Visitors’ Use of Mobile and Smart Technology

Visitors, including **volunteers and contractors**, who are on-site for regular or extended periods must adhere to the school's **acceptable use guidance** and all related policies, including **safeguarding policies**.

Staff are responsible for addressing any concerns regarding a visitor’s use of mobile or smart technology. Any breaches must be reported to the **DSL or ICT Lead** for further action.

Reporting Concerns

Any concerns or complaints regarding **online safety** from **staff, pupils, parents, guardians, or carers** will be addressed promptly.

- Complaints should be reported to the **DSL**, who will **immediately investigate** and coordinate with the **SLT** and any relevant staff or pupils.
- For further guidance, please refer to the **Complaints Procedure**.

Monitoring and review

- This policy is reviewed at least annually by the DSL and the Headteacher. This policy will be updated as needed to ensure it is up-to-date with online safety and safeguarding issues as they emerge and evolve, including any lessons learnt.
- Any changes made to this policy will be communicated to all members of staff. All members of staff are required to familiarise themselves with all processes and procedures outlined in this policy as part of their induction programme.

The next scheduled review date for this policy is **August 2025**.

January 2025

Lucy Meyer
Co-principal