LEARNING OPPORTUNITIES

Online Safety Policy
incorporating 'Mobile and Smart Technology' and 'Social Media'

Learning Opportunities recognise online safety as a key safeguarding consideration and as such will ensure a whole school approach to meeting our statutory safeguarding responsibilities.

This policy, which should be read alongside Learning Opportunities Safeguarding Policy and Procedures Incorporating Child Protection, will be reviewed **at least** annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Key Details

Designated Safeguarding Lead (s): Simon Graydon (headteacher) / Kevin Dunk (Deputy Headteacher) / Catherine Graydon

Proprietor with lead responsibility: Lesley Buss

Date written/updated: 25 August 2024
Date agreed and ratified by the proprietor: 28 August 2024
Next review Date: August 2025

Contents

Page Number

INTRODUCTION - Policy aims and scope

This policy has been written by Learning Opportunities, involving staff, students and parents/carers, building on Kent County Councils LADO and Education Safeguarding Advisory Service mobile and smart technology policy template, with specialist advice and input as required.

It takes into account the Department for Education (DfE) statutory guidance 'Keeping Children Safe in Education' (KCSIE), Working Together to Safeguard Children' (WTSC), the DfE non-statutory guidance and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.

The purpose of this policy is to safeguard and promote the welfare of all members of our community when using mobile devices and smart technology.

- Learning Opportunities recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harm when using mobile and smart technology.
- As outlined in our Safeguarding / Child Protection Policy, the Designated Safeguarding Lead (DSL), Simon Graydon (Headteacher), is recognised as having overall responsibility for online safety.

Learning Opportunities will adopt a whole school approach to online safety which will empower, protect, and educate our students and staff in their use of technology, and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate. We will ensure online safety is considered as a running and interrelated theme when devising and implementing our policies and procedures, and when planning our curriculum, staff training, the role and responsibilities of the DSL and parental / carer engagement.

Learning Opportunities identifies that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful content. For example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact: being subjected to harmful online interaction with other users. For example, peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm. For example, making, sending and receiving explicit images (including consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Learning Opportunities recognises that technology, and the risks and harms related to it, evolve and change rapidly. We will carry out an annual review of our approaches to online safety, supported by an annual risk assessment, which considers and reflects the current risks our students face online.

This policy applies to all access to and use of all mobile and smart technology on site; this includes but is not limited to mobile/smart phones and personal devices such as tablets, e-readers, games consoles and wearable technology, such as smart watches and fitness trackers, which facilitate communication or have the capability to record sound and/or images.

This policy applies to students, parents/carers and all staff, including the proprietor, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as “staff” in this policy).

LINKS WITH OTHER KEY POLICIES

This policy links with several other policies, practices and action plans, including but not limited to:

- Anti-bullying policy
- Acceptable Use Policies (AUP)
- Positive Behaviour management policy
- Safeguarding / Child protection policy
- Staff code of conduct
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data security

SAFE USE OF ARTIFICIAL INTELLIGENCE (AI)

Learning Opportunities acknowledges that generative AI tools can be used to produce content that is dangerous, harmful, and inappropriate. The school will follow the procedures set out in the Child Protection and Safeguarding Policy and the online-Safety Policy to ensure that students are not able to access or be exposed to harmful content.

Students will be taught about the risks of using AI tools and how to use them safely. They will be made aware of how to report any concerns or incidents involving generative AI, and who to talk to about any issues regarding the use of AI tools.

Teaching about the safe and appropriate use of AI will ensure that students benefit from a knowledge-rich curriculum which enables them to become well-informed users of technology and understand its impact on society. Students, as appropriate, will gain strong foundational knowledge which ensures they are developing the right skills to make the best use of AI tools.

The school will ensure (where practical) that the appropriate filtering and monitoring systems are in place to protect students online, following the DfE’s filtering and monitoring standards.

All staff members will receive training on the safe use of AI as part of their online safety training, which is regularly updated.

FILTERING & MONITORING

Filtering and monitoring systems are an important part of safeguarding. They provide a safe environment to learn and work by protecting students and staff from harmful and inappropriate content online.

What counts as harmful or upsetting content will depend on the student – for example, their age. Harmful content could be legal or illegal, and includes pornography, promotion of self-harm or suicide, misogyny, racism, fake news and extremist views.

The Headteacher (DSL) has overarching responsibility for the different areas of filtering and monitoring. They are supported in this role by our IT Consultants Primary Technologies.

Staff have a responsibility to report to the Headteacher (DSL), or in their absence directly to Primary Technologies when:

- They witness or suspect unsuitable material has been accessed
- They can access unsuitable material
- They are teaching topics that could create unusual activity on the filtering logs
- There is failure in the software or an abuse of the system
- They think there are some unreasonable restrictions that affect teaching and learning or administrative tasks
- They notice abbreviations or misspellings that allow access to restricted material

Learning Opportunities will do all we reasonably can to limit student's exposure to online harms through school provided devices and networks and in line with the requirements of the Prevent Duty and KCSIE, we will ensure that appropriate filtering and monitoring systems are in place e.g.

- Education broadband connectivity is provided through BT.
- We use Watchguard, which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with Primary Technologies to ensure that our filtering policy is continually reviewed.

If students or staff discover unsuitable sites or material, they are required to:

- turn off monitor/screen,
- report the concern immediately to a member of staff
- The member of staff will report the concern (including the URL of the site if possible) to the DSL and/or Primary Technologies
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Kent Police or CEOP.

Our leadership team and relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.

All staff will receive training to understand their own role, which includes following policies, processes and procedures, process for acting on reports and concerns, and monitoring what students are looking at when using internet-enabled devices in lessons.

All users will be informed that use of our systems can be monitored, and that monitoring will be in line with data protection, human rights, and privacy legislation.

We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:

- Monitoring / supervision of students
- Monitoring internet and web access using securus

Filtering breaches or concerns identified through our monitoring approaches will be recorded and reported to the DSL who will respond as appropriate.

When implementing appropriate filtering and monitoring, Learning Opportunities will ensure that "over blocking" does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

Whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of Learning Opportunities approach to online safety. We recognise that we cannot rely on filtering and monitoring alone to safeguard our students; effective safeguarding practice, robust policies, appropriate classroom / behaviour management and regular education/training about safe and responsible use is essential and expected.

- Students will use appropriate search tools, apps and online resources as identified by staff, following an informed assessment of suitability.
- Internet use will be supervised by staff as appropriate to students age and ability.
- Students will be directed to use age/ability appropriate online resources and tools by staff.

Responsibilities

- The proprietor of Learning Opportunities has overall strategic responsibility for filtering and monitoring approaches, including ensuring that our filtering and monitoring systems are regularly reviewed, and that the leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.
- Simon Graydon (Headteacher) and the proprietor are responsible for ensuring that our school has met the DfE filtering and monitoring standards
- The leadership team, in conjunction with our IT consultants (Primary Technologies) are responsible for:
    - documenting decisions on what is blocked or allowed and why
    - reviewing the effectiveness of our provision
    - overseeing reports
    - ensuring that staff understand their role, and are appropriately trained, follow policies, processes and procedures and act on reports and concerns.
- The DSL has lead responsibility for overseeing and acting on:
    - Any filtering and monitoring reports
    - Any child protection or safeguarding concerns identified
    - Checks to our filtering and monitoring system
- Our IT Consultants have technical responsibility for:
    - Maintaining filtering and monitoring systems
    - Providing filtering and monitoring reports
    - Completing technical actions identified following and concerns or checks to the system
    - Working with the leadership team / DSL to procure systems, identify risks, carry out reviews and checks.
- All members of staff are provided with an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of our induction process, and in our child protection staff training.
- All staff, students, parents/carers have a responsibility to follow this policy to report and record any filtering or monitoring concerns.

Decision making

When making filtering and monitoring decisions, Learning Opportunities will consider those students who are 'potentially at greater risk of harm' and how often they access the IT system along with the potential safeguarding risks.

- Learning Opportunities leadership team have ensured that our school has age and ability appropriate filtering and monitoring in place to limit student's exposure to online risks.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with safeguarding, educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring systems to ensure that we understand the changing needs and potential risks posed to our community.
- Learning Opportunities are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

INFORMATION SECURITY & ACCESS MANAGEMENT

Learning Opportunities is responsible for ensuring an appropriate level of security protection procedures are in place, in order to safeguard our systems as well as staff and students. Further information can be found in our acceptable use (AUP) policies.

All members of staff are made aware through induction, ongoing training, policies and AUPs that all school related communications / messages must be kept confidential. It is imperative that these are not accessed by students, staff's own family members or members of the public. To minimise the likelihood of this happening email notifications should be turned off on all personal mobile and/or smart technology devices.

The above is also applicable to the introduction within the school of instant messaging on Microsoft Teams. Staff are aware that messages shared must be professional at all times. To avoid disruptions during teaching / class-based activities and / or the possibility of students / visitors viewing confidential information, staff will set their teams status to 'do not disturb'. When the 'do not disturb' mode is enabled, any notifications that would normally appear when they come in will not be visible to the user. Instead they will be muted – by turning on this setting, staff will avoid having their workflow interrupted by unimportant notifications, allowing them to stay focussed on the task in hand.

Learning Opportunities will review the effectiveness of our procedures periodically to keep up with evolving cyber-crime technologies.

Security and management of information systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Password encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.

- Not using portable media without specific permission; portable media will be checked by an anti-virus/malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
- Checking files held on our network, as required and when deemed necessary by leadership staff.
- The appropriate use of user logins and passwords to access our network.
- Specific user logins and passwords will be enforced for all users.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Password policy

All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private. We require all staff to:

- use strong passwords for access into our system.
- change their passwords regularly, every 30 days is recommended.
- not share passwords or login information with others or leave passwords/login details where others can find them.
- not to login as another user at any time.
- lock access to devices/systems when not in use.

Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the DfE.
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or student's personal information will not be published on our website; the contact details on the website will be our setting address, email addresses and telephone numbers.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

STAFF TRAINING

Learning Opportunities will ensure that all staff, including the proprietor receive online safety training as part of induction, which will include an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring.

Ongoing online safety training and updates for all staff will be integrated, aligned and considered as part of our overarching safeguarding approach.

Through support / training, DSLs will understand the unique risks associated with online safety, will be able to recognise the additional risks students with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep students safe online.

Through induction and ongoing training, all staff will be made aware that technology is a significant component in many safeguarding and wellbeing issues and that abuse can take place wholly online, or technology may be used to facilitate offline abuse.

Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

Staff will be made aware that students may not feel ready or know how to tell someone that they are being abused, exploited, or neglected, and/or they may not recognise their experiences as harmful. This could be due to their vulnerability, disability and/or sexual orientation or language barriers. This should not prevent staff from having a professional curiosity and speaking to the DSL if they have concerns about a student.

SAFE USE OF MOBILE & SMART TECHNOLOGY EXPECTATIONS

Learning Opportunities recognises that use of mobile and smart technologies is part of everyday life for many students, staff and parents/carers.

Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of our community are advised to:

- take steps to protect their personal mobile phones or other smart devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on personal phones or devices.

Mobile devices and other forms of smart technology are **only** permitted to be used in designated areas on site.

The sending of abusive or inappropriate messages or content, including via personal mobile devices and/or smart technology is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, behaviour and safeguarding / child protection policies and staff code of conduct.

All members of the Learning Opportunities are advised to ensure that their personal mobile and smart technology devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour or child protection policies.

SCHOOL PROVIDED MOBILE PHONES & DEVICES

Members of the leadership team will be issued with a work phone number in addition to their work email address, where contact with students or parents/carers is required.

Staff providing formal remote/online learning will do so using school provided equipment in accordance with our Acceptable Use Policy (AUP).

School mobile phones and/or devices e.g. laptops / chrome books will be suitably protected via a password and must only be accessed or used by members of staff and/or students**.**

School mobile phones and/or devices will always be used in accordance with our staff code of conduct/behaviour policy, acceptable use of technology policy and other relevant policies.

Where staff and/or students are using school provided mobile phones and/or devices, they will be informed prior to use via our Acceptable Use Policy (AUP) that activity may be monitored for safeguarding reasons and to ensure policy compliance.

STAFF USE OF MOBILE & SMART TECHNOLOGY

Members of staff will ensure that use of any mobile and smart technology, including personal phones, wearable technology and other mobile/smart devices, will take place in accordance with the law, as well as relevant school policy and procedures, including confidentiality, child protection, data security staff behaviour/code of conduct and Acceptable Use Policies.

Staff will be advised to:

- Keep personal mobile and smart technology devices in a safe and secure place during lesson time.
- Keep personal mobile phones and devices switched off or set to ‘silent’ or ‘do not disturb’ modes during lesson times.
- Ensure that Bluetooth or other forms of communication, such as ‘airdrop’, are hidden or disabled during lesson times.
- Not use personal mobile or smart technology devices during teaching periods, unless **written** permission has been given by the headteacher, such as in emergency circumstances.
- Ensure that any content bought onto site via personal mobile and smart technology devices is compatible with their professional role and our behaviour expectations.

Members of staff are not permitted to use their own personal mobile and smart technology devices for contacting students or parents and carers.

- Any pre-existing relationships or circumstance, which could compromise staff’s ability to comply with this, will be discussed with the DSL and/or headteacher. Staff will only use school provided equipment (not personal devices):
- to work directly with students during lessons/educational activities.
- to communicate with parents/carers.

Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices with prior approval from the headteacher, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy.

If a member of staff breaches our policy, action will be taken in line with our staff employee handbook, code of conduct, child protection policy and/or allegations policy.

If a member of staff is thought to have illegal content saved or stored on a personal mobile or other device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted, and the LADO (Local Authority Designated Officer) will be informed.

<u>STUDENTS USE OF MOBILE & SMART TECHNOLOGY</u>

'<u>Behaviour in School: Advice for headteachers and school staff</u>' states "Headteachers should decide if mobile phones can be used during the school day. Many pupils, especially as they get older, will have one of their own. Allowing access to mobiles in school introduces complexity and risks, including distraction, disruption, bullying and abuse, and can be a detriment to learning…

If headteachers decide not to impose any restrictions on mobile phones, they should have a clear plan to mitigate the risks of allowing access to phones. This plan, as part of the school's behaviour policy, should outline the approach to mobile phones and be reiterated to all students, staff and parents / carers throughout the school year. Headteachers should ensure it is consistently and fairly applied."

Students will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.

Safe and appropriate use of mobile and smart technology will be taught to students as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies e.g. Computing.

Personal mobile or smart technology devices is permitted on site for students.

- Personal mobile or smart devices will not be used by students during lessons or formal educational time.
- Personal mobile or smart devices can be used by students during break or free time in designated areas, but any use must be in accordance with our anti-bullying and behaviour policy. If students breach our policies, this may be revoked.

Learning Opportunities expects students' personal mobile or smart technology devices to be kept safe and secure when on site. This means:

- kept in a secure place
- switched off and kept out of sight during lessons and while moving between lessons.

If a student needs to contact their parents or carers whilst on site, they will be allowed to use a school phone.

- Parents / carers are advised to contact their child via the school phone; exceptions may be permitted on a case-by-case basis, as approved by the headteacher.

If a student requires access to personal mobile or smart technology devices in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the headteacher prior to use being permitted.

- Any arrangements regarding access to personal mobile or smart technology devices in exceptional circumstances will be documented and recorded by the school.
- Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the student and/or their parents carers before use is permitted.

Where students' personal mobile or smart technology devices are used when learning at home, this will be in accordance with our Acceptable Use Policy.

Personal mobile or smart technology devices must not be taken into examinations. Students found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

SEARCHING, SCREENING & CONFISCATION OF ELECTRONIC DEVICES

Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.

Where there are any concerns regarding students' use of mobile or smart technology or policy breaches, they will be dealt with in accordance with our existing policies, including anti-bullying, child protection, online safety and behaviour.

The Headteacher / Deputy may confiscate a students' personal mobile or smart technology device if they believe it is being used to contravene our child protection or behaviour policy.

Personal mobile or smart technology devices that have been confiscated will be held in a secure place and released to parents/carers at the earliest opportunity.

Where a concern involves a potentially indecent image or video of a child, staff will respond in line with our child protection policy and will confiscate devices, avoid looking at any content, and refer the incident to the DSL (or deputy) urgently as they will be most appropriate person to respond.

If there is suspicion that data or files on a student's personal mobile or smart technology device may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Staff will respond in line with our child protection policy and follow the most appropriate safeguarding response if they find images, data or files on a student's electronic device that they reasonably suspect are likely to put a person at risk.

The DSL (or deputy) will be involved without delay if staff believe a search of a student's personal mobile or smart technology device is required due to a safeguarding risk.

In exceptional circumstances and in accordance with the DfE 'Searching, Screening and Confiscation' guidance, the headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so.

- In determining whether there is a 'good reason' to examine images, data or files, the headteacher or an authorised member of staff will need to reasonably suspect that the images, data or files on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
- In determining whether there is a 'good reason' to erase any images, data or files from the device, the headteacher should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable.
- If the data or files are not suspected to be evidence in relation to an offence, the headteacher or an authorised member of staff may delete the images, data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the student and/or the parent refuses to delete the data or files themselves.

If the headteacher or a member of staff finds any data or files that they suspect might constitute a specified offence, they will be delivered to the police as soon as is reasonably practicable.

VISITORS' USE OF MOBILE & SMART TECHNOLOGY

Parents/carers and visitors, including volunteers and contractors, are made aware that:

- mobile phones and personal devices are only permitted within specific areas and / or are only permitted for specific purpose, for example, as part of multi-agency working arrangements.

Appropriate signage and information are in place to inform visitors of our expectations for safe and appropriate use of personal mobile or smart technology.

Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our acceptable use of technology policy and other associated policies, including child protection.

If visitors require access to mobile and smart technology, for example when working with students as part of multi-agency activity, this will be discussed with the headteacher prior to use being permitted.

- Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the school. This may include undertaking appropriate risk assessments if necessary.

Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or headteacher of any breaches of our policy.

POLICY MONITORNING & REVIEW

Technology evolves and changes rapidly. Learning Opportunities will review this policy at least annually. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.

We monitor internet and technology use taking place via all school provided devices and systems and regularly evaluate online safety mechanisms to ensure this policy is consistently applied. Any issues identified as a result of our monitoring approaches will be incorporated into our action planning.

All members of the community will be made aware of how the school will monitor policy compliance e.g. AUPs, staff training, classroom management.

RESPONDING TO POLICY BREACHES

All members of the community are informed of the need to report policy breaches or concerns in line with existing school policies and procedures. This includes safeguarding / child protection and positive behaviour management policy, staff code of conduct, employee handbook.

Where students breach this policy:

- appropriate consequences and/or pastoral / welfare support will be implemented in line with our behaviour policy.
- concerns will be shared with parents/carers as appropriate.
- we will respond in line with our child protection policy, if there is a concern that a child is at risk of harm.

After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

We require staff, parents/carers and students to work in partnership with us to resolve issues.

All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.

Students' parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or headteacher will seek advice from Kent County Council or other agencies, as appropriate, in accordance with our child protection policy.

LEARNING OPPORTUNITIES

SOCIAL MEDIA

Policy aims and scope

This policy has been written by Learning Opportunities, involving staff, students and parents/carers, building on Kent County Councils LADO and Education Safeguarding Advisory Service Social Media policy template, with specialist advice and input as required.

It takes into account the Department for Education (DfE) statutory guidance 'Keeping Children Safe in Education' (KCSIE, 'Working Together to Safeguard Children'(WTSC), and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.

The purpose of this policy is to safeguard and promote the welfare of all members of Learning Opportunities community when using social media.

- Learning Opportunities recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harm when using social media.
- As outlined in our child protection policy, the Designated Safeguarding Lead (DSL), Simon Graydon (Headteacher) is recognised as having overall responsibility for online safety.

The policy applies to all use of social media; the term social media includes, but is not limited to, blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger apps or other online communication services.

This policy applies to students, parents/carers and all staff, including the proprietor, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy).

LINKS WITH OTHER KEY POLICIES

This policy links with several other policies, practices and action plans, including but not limited to:

- Anti-bullying policy
- Acceptable Use Policies (AUP)
- Behaviour management policy
- Safeguarding / Child protection policy
- Staff code of conduct
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), and Relationships and Sex Education (RSE)
- Data security

GENERAL SOCIAL MEDIA EXPECTATIONS

Learning Opportunities believes everyone should be treated with kindness, respect and dignity. Even though online spaces may differ in many ways, the same standards of behaviour are expected online as offline, and all members of our community are expected to engage in social media in a positive and responsible manner.

All members of our community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

We will monitor student and staff access to social media via our filtering and monitoring systems which are applied to all school provided devices and systems.

The use of social media during school hours is not permitted.

Concerns regarding the online conduct of any member of Learning Opportunities community on social media will be taken seriously. Concerns will be managed in accordance with the appropriate policies, including anti-bullying, allegations against staff, behaviour, staff code of conduct, Acceptable Use Policies, and child protection.

STAFF USE OF SOCIAL MEDIA

The use of social media during school hours for personal use is not permitted for staff.

Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our code of conduct and/or acceptable use of technology policy.

The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.

Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and code of conduct, and allegations against staff policy.

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media. This may include, but is not limited to:

- Setting appropriate privacy levels on their personal accounts/sites.
- Being aware of the implications of using location sharing services.
- Opting out of public listings on social networking sites.

- Logging out of accounts after use.
- Using strong passwords.
- Ensuring staff do not represent their personal views as being that of the school.

Members of staff are encouraged not to identify themselves as employees of Learning Opportunities on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.

All staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.

Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues, will not be shared or discussed on social media sites.

Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with students and their families

Staff will not use any personal social media accounts to contact students or their family members.

All members of staff are advised not to communicate with or add any current or past students or their family members, as 'friends' on any personal social media accounts.

Any communication from students and parents/carers received on personal social media accounts will be reported to the DSL (or deputy) and/or the headteacher.

Any pre-existing relationships or situations, which mean staff cannot comply with this requirement, will be discussed with the DSL and the headteacher. Decisions made and advice provided in these situations will be formally recorded to safeguard students, members of staff and the setting.

If ongoing contact with students is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.

STUDENTS USE OF SOCIAL MEDIA

The use of social media during school hours for personal use is not permitted for students.

Many online behaviour incidents amongst children and young people occur on social media outside the school day and off the school premises. Parents/carers are responsible for this behaviour; however, some online incidents may affect our culture and/or pose a risk to children and young people's health and wellbeing. Where online behaviour online poses a threat or causes harm to another student, could have repercussions for the orderly running of the school when the student is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school, action will be taken in line with our behaviour and child protection/online safety policies.

Learning Opportunities will empower our students to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to students as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies for example, RSE and Computing.

Students will be advised:

- to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
- to only approve and invite known friends on social media sites and to deny access to others, for example by making profiles private.
- not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
- to use safe passwords.
- to use social media sites which are appropriate for their age and abilities.
- how to block and report unwanted communications.
- how to report concerns on social media, both within the setting and externally.

Any concerns regarding students' use of social media will be dealt with in accordance with appropriate existing policies, including anti-bullying, child protection and behaviour.

The DSL (or deputy) will respond to social media concerns involving safeguarding or child protection risks in line with our child protection policy.

Consequences and/or pastoral/welfare support will be implemented and offered to students as appropriate, in line with our child protection and behaviour policy. Civil or legal action may be taken if necessary.

Concerns regarding students' use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

POLICY MONITORING & REVIEW

Technology evolves and changes rapidly. Learning Opportunities will review this policy at least annually. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.

An annual risk assessment will be undertaken by the Leadership Team and the outcome shared with staff. This will consider and reflect the specific risks faced by our students.

We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied. Any issues identified will be incorporated into our action planning.

All members of the community will be made aware of how the school will monitor policy compliance for example, AUPs, staff training, classroom management.

RESPONDING TO POLICY BREACHES

All members of the community are informed of the need to report policy breaches or concerns in line with existing school policies and procedures. This includes child protection and/or behaviour policies.

After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

We require staff, parents/carers and students to work in partnership with us to resolve issues.

All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.

Students, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or headteacher will seek advice from Kent County Council or other agencies, as appropriate, in accordance with our child protection policy.