LIMPSFIELD GRANGE SCHOOL

'together we make a difference'

Online Safety & Digital Resilience Policy

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment

Governor's Committee Responsibility: Curriculum, Community and Student Welfare

Date Approved: Autumn Term 2023

Review Period: Annually

Next Review Date: Autumn Term 2024

The Limpsfield Grange Values:

At Limpsfield Grange we believe in working together to make a difference.

We are a tolerant community; we accept, value and understand others.

We care for all members of our community without judgement.

We are responsible for our own learning, behaviour and actions.

We accept that sometimes things go wrong. We work together to take responsibility for our mistakes and for putting things right.

We are a respectful community and we treat others as we would like to be treated, even if they have different views and opinions to our own.

We understand that good behaviour helps us to prepare for life beyond Limpsfield Grange.

We are positive and resilient. We celebrate difference in everything that we do.

We are all proud to be part of the Limpsfield Grange community.

July 2023

Limpsfield Grange School

Online Safety & Digital Resilience Policy

Background and rationale

"*It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.*" KCSiE 2023 pg. 35

Limpsfield Grange School believes that online safety and digital resilience are essential elements of safeguarding students and adults in the digital world, when using technology such as computers; mobile phones; tablets; smart watches and games consoles.

Limpsfield Grange has identified that the Internet and information communication technologies are an integral part of everyday life, so students must be supported to be able to learn how to develop strategies to manage and respond to risk so that they can be empowered to build resilience online. Limpsfield Grange has a duty to provide the school community with quality Internet access to raise education standards; promote students achievement; meet students' needs; support the professional work of the staff and enhance the school's leadership and management functions.

Limpsfield Grange also identifies that there is a clear duty to ensure that students are protected from potential risks and harm online.

Keeping Children Safe in Education (2023) catergorised the following 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**: online behaviour that increases the likelihood of, or causes, harm, for example making, sending or receiving explicit images e.g.: 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 or financial scams. If you feel that a student or member of staff is at risk from phishing activity, please report it to the Anti-Phishing Working Group (https://apwg.org)

Aims of this policy

- To clearly identify the key principles expected of the school community with regards to safe and responsible use of technology to ensure that Limpsfield Grange is a safe and secure environment.
- To safeguard and protect members of the Limpsfield Grange community online.
- To raise awareness with all members of the Limpsfield Grange community regarding the potential risks as well as benefits of technology.
- Enable staff to work safely and responsibly, to role model positive behaviour online and to be aware of the need to manage their own standards and practice when using technology.
- To identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

- To promote a real world, responsible and positive outlook towards digital literacy and resilience and online safety aimed at preparing students for expected standards of behaviour in adult life and the workplace.
- To ensure that this policy is closely integrated with other relevant policies and procedures including:
    - Child Protection & Safeguarding policy
    - Behaviour policy (including Anti Bullying)
    - Staff Behaviour policy including the acceptable use of technology
    - Procedures for accessing school email on handheld devices
    - Online safety rules (students)
- To enable Governors, school leaders and staff to understand the importance of online safety and digital resilience, and recognise the potential impact of online activity on children's mental health, both positive and negative.

Scope

The policy applies to staff including Teachers; Teaching Assistants (including Bank Staff); members of the Residential and Support teams; the Governing Body, volunteers, visitors, contractors and other individuals who work for or provide services on behalf of Limpsfield Grange School, as well as students; parents; carers and family members of students at the school.

This policy applies to all access to the Internet and use of information communication devices including personal devices or where students, staff or other individuals have been provided with Limpsfield Grange issued devices for use off-site, such as a work laptop or mobile phone.

Limpsfield Grange is also *in loco parentis* (Children Act 1989) which allows the school to report and act on instances of cyberbullying, abuse, harassment (including sexual harassment) malicious communication and grossly offensive material; including reporting to the police, social media websites and hosting providers on behalf of students.

The Limpsfield Grange School Online Safety & Digital Resilience policy has been written by Limpsfield Grange School, building on Surrey County Council advice with specialist advice and input as required. It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2023, 'Working Together to Safeguard Children' 2018 and the Surrey Safeguarding Children Board procedures.

Online safety and digital resilience at Limpsfield Grange: key responsibilities

Safeguarding; Online Safety & Filtering and Monitoring Governor – key responsibilities

- Hold regular meetings with the Designated Safeguarding Lead.
- Receive (collated and anonymised) reports of online safety incidents on a termly basis.
- Check that online safety provision and staff training is taking place as intended.
- Ensure that the filtering and monitoring provision is reviewed and recorded at least annually (the review will be conducted by the Business Manager, DSL and IT service provider and involve the responsible Governor) in line with the DfE Filtering and Monitoring Standards.
- Report termly to the Governors Resources committee.
- Undertake basic cyber-security training.

The Senior Leadership Team - key responsibilities

- Ensure that there are appropriate and up-to-date policies regarding online safety and digital resilience; including an acceptable use of technology policy, which covers acceptable use of technology for staff.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical providers to monitor the safety and security of systems and networks.
- Ensure that online safety and digital resilience is embedded within the IT and WACI curriculum (including RSE), which enables all students to develop an age-appropriate strategies to manage and respond to risk so that they can be empowered to build digital resilience.
- Support the DSL and the deputy DSLs by ensuring they have sufficient time and resources to fulfil their online safety and digital resilience responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety and digital resilience practice to identify strengths and areas for improvement
- Review and evaluate each week, student and staff Internet use and suspicious Internet search data, and take appropriate action.
- Provide training opportunities for staff and wider stakeholders and parents and carers relating to online safety and digital resilience.
- Liaise with the Local Authority and other local and national bodies as appropriate.
- Report online safety concerns, as appropriate, to the Governing Body.

The School Business Manager - key responsibilities (oversight of providers managing the technical environment)

- Ensure that technical providers (SoftEgg) provide technical support and perspective to the DSL and deputy DSLs and Senior Leadership Team, especially in the development and implementation of appropriate online safety and digital resilience strategies.
- Implement appropriate security measures as directed by the Senior Leadership Team, to ensure that the IT systems are secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that appropriate access and technical support is given to the DSL and deputy DSLs to our filtering and monitoring systems, to enable them to take appropriate safeguarding action as required.
- With the DSL alerting the Leadership Team of day-to-day online safety issues, including suspicious searches and record any issues.
- Liaise with LA contacts and SoftEgg ICT support and service providers to ensure that our filtering and IT systems are fit for purpose, updated regularly and effective
- Identify sites which should be blocked and share this information with SoftEgg and the Senior Leadership Team, the Online Safety & Digital Resilience Coordinator and with staff across the education and residential teams.
- Ensure that Limpsfield Grange practice is in line with GDPR legislation.

The Online Safety & Digital Resilience Coordinator - key responsibilities

The Limpsfield Grange's designated Online Safety & Digital Resilience Coordinator is Sam Janaway - Student Support Lead, who reports to the Headteacher and coordinates online safety and digital resilience provision across the school and wider school community.

The Online Safety & Digital Resilience Coordinator will:

- Act as a named point of contact for online safety and digital resilience issues and liaise with other members of staff as appropriate.
- Report online safety concerns, as appropriate, to the Senior Leadership Group.
- Deliver online safety and digital resilience training for staff and Governors.
- Raise and maintain staff awareness regarding their responsibilities relating to online safety and digital resilience procedures.
- Ensure all students have agreed to our online safety rules.
- Keep up-to-date with current research, legislation and trends.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and digital resilience and have the relevant knowledge required to keep students safe online.
- Ensure that the School Business Manager is aware of any filtering or network issues which contribute to poor online safety.
- Work with the Headteacher to review and update online safety and digital resilience policies.
- Coordinate participation in local and national events to promote positive online behaviour.
- Ensure that online safety and digital resilience is integrated with our WACI curriculum; and other relevant policies and procedures.
- Ensure that online safety and digital resilience is promoted to parents and carers and the wider community, and that training for this group is offered.

The Designated Safeguarding Lead and Deputy Designated Safeguarding Leads - key responsibilities

- Consult with the Senior Leadership Team and Online Safety Coordinator to decide which incidents are reported to CEOP, Local Police, LADO, Social Services and parents/carers.
- With the School Business Manager maintain a log of submitted online safety reports and incidents, and address issues with students and staff, recording actions taken as required, feeding back to the Leadership Team weekly.
- Ensure staff and Governors have signed the Staff Behaviour policy.
- Monitor the number of online safety incidents to identify gaps / trends.
- Ensure that online safety incidents and subsequent actions are recorded as part of Limpsfield Grange's safeguarding recording structures and mechanisms.

The Designated Safeguarding Lead specific responsibilities:

- Hold the lead responsibility for online safety within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up-to-date capability required to keep children safe whilst they are online
- Meet regularly with the Online Safety Governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual filtering and monitoring checks are carried out.
- Attend relevant Governing Body meetings.
- Receive reports of online safety incidents, investigate them and liaise with the relevant agencies if necessary, ensuring that all incidents are recorded.
- Liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety).

- Half termly monitoring of staff and student log ins to review efficacy of the school's filtering systems.

Staff - key responsibilities

- Take part in our online safety and digital resilience awareness as part of the staff induction program.
- Read, understand, sign and comply with the Staff Behaviour policy including the acceptable use of technology agreement.
- Be aware of the current Limpsfield Grange Online Safety & Digital Resilience policy, practices and associated procedures for reporting online safety incidents.
- Understand the policies relevant to the Internet, social media and computer use in school.
- Understand that online safety is a core part of safeguarding.
- Follow the school procedures, as set out in the staff handbook in regard to external off-site use, personal use of social media and the Internet ensuring that they do not bring the school into disrepute.
- Monitor students' Internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones and other gadgets on the school site and off site when they are engaged in school activities such as SOLD.
- Report any issues with online safety and digital resilience to the DSL or Deputy DSLs.
- Promote best practice regarding avoiding copyright infringement and plagiarism.
- Ensure that Internet usage and suggested websites and videos are pre-vetted and documented in curriculum planning.
- Ensure that any online bullying is dealt with appropriately and in line with the Limpsfield Grange Behaviour policy (including Anti Bullying).
- Undertake regular cyber security training.

Students – key responsibilities

- Read, understand and comply with the Limpsfield Grange online safety rules.
- Respect the feelings and rights of others both on and offline.
- Seek help from a trusted adult if things go wrong in school, and support others who might be experiencing online safety issues.
- Seek help from their parents or carers if things go wrong whilst they are at home.
- At a level appropriate to their age, ability and vulnerability, be responsible for keeping themselves and others safe online.
- At a level appropriate to their age, ability and vulnerability be responsible for their own learning and awareness in relation to the opportunities and risks posed by new and emerging technologies.
- At a level appropriate to their age, ability and vulnerability assess the personal risks of using any particular technology and behave safely and responsibly to limit those risks, to the best of their ability.
- Be aware of how to report online safety incidents in school using external reporting facilities, such as the CEOP report abuse button.
- Be aware that the online safety rules cover all computer, Internet and device usage in school (including on the playground each morning before the start of the school day) and the residential provision.
- Be aware that their Internet use out of school on social networking or gaming sites such as Instagram, WhatsApp or Roblox is covered under the online safety rules if it impacts on the school and/or staff and students in terms of online bullying, reputation or illegal activities.

Parents and carers – key responsibilities

- Support the Limpsfield Grange Online Safety & Digital Resilience policy through promoting safe, responsible and appropriate Internet behaviour and use of ICT equipment both at school and at home.
- Discuss online safety issues with their children and reinforce appropriate safe online behaviour at home.
- Monitor their child's social media and Internet at least weekly, and discuss this monitoring with their child.
- Ensure that their child's social media accounts are not public and privacy settings are limited to friends and family only. Where possible location and Bluetooth should also be switched off.
- Consider and abide by the age limits set by different social media platforms.
- Address friendships issues or peer disagreements on social media which involve their child that take place outside of school hours direct with other parents.
- Model safe and appropriate uses of emerging technology and social media.
- Identify changes in behaviour that could indicate that a child is at risk of harm online, and seek help and support from the school or other appropriate agencies, if their child encounters difficulties online.
- Be aware of the Limpsfield Grange online safety rules for students and support their child to uphold these rules when using websites and social media outside of school.
- Report any issues to the school as soon as possible

IT provider (SoftEgg) – key responsibilities

- Ensure that the school technical infrastructure is secure and not open to misuse or malicious attack.
- Ensure that the school meets the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges
- Ensure that there is clear, safe and managed control of user access to networks and devices.
- Keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Regularly and effectively monitor the use of technology in order than any misuse/attempted misuse can be reported to the Business Manager for investigation and action
- Apply and update the filtering policy on a regular basis

How will the school provide online safety education?

We will establish and embed a progressive online safety curriculum which will raise awareness and promote safe and responsible Internet use amongst students by:

- Ensuring education regarding safe and responsible use supports Internet access.
- Including online safety and digital resilience in our WACI (Wellbeing Achievement Communication and Independence) curriculum including in our Relationships and Sex Education (RSE) and IT lessons. Online safety and digital resilience in WACI lessons covers all information regarding content, contact, conduct and commerce as detailed in *Keeping Children Safe in Education (2023)*
- Regularly reinforcing online safety messages through Wellbeing Wednesday activities.
- Educating students in the effective use of the Internet to research; including the skills of knowledge location, retrieval, reliability and critical evaluation.
- Teaching students how to judge the validity of online information, where to go for advice and how to respond to and report concerns.

Engagement with students

By the end of Year 11 students will know:

- Their rights, responsibilities and opportunities online.
- About online risks, including that any material someone provides to another which has the potential to be shared online and the difficulty of removing potentially compromising material placed online (for example nudes.)
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report inappropriate material or conduct and manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children* (including those created by children) is a criminal offence which carries severe penalties including jail. *In this case a child is anyone under the age of 18.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse, harassment, coercion, exploitation and trolling) and how to report, or find support, if they have been affected by those behaviours.
- How to assess the quality of information retrieved from the Internet, including recognising how reliable, accurate and relevant information is – particularly information obtained from search engines.
- About copyright and plagiarism infringement laws and potential consequences with regard to copying material for homework and coursework, copying photographs and images on social networking sites, copying material for using in teaching materials, downloading music, video, applications or other software files illegally.
- The importance of digital literacy skills in the workplace.
- Why harmful or abusive images on the Internet might be inappropriate or illegal or harmful or unsafe.
- How accessing or sharing people's personal information or photographs might be inappropriate or illegal.
- About Youth Produced Sexual Imagery and online radicalisation.
- Why some online behaviour carries an unacceptable level of risk, including talking to strangers on social networking sites and how grooming (CSE and County Lines) and radicalisation can take place, and how to stop it, report it and deal with the consequences of it.
- How spending a lot of time online or gaming can impact on an individual in terms of their mental wellbeing and social interaction.
- How spyware can allow unauthorised users to access a webcam or built-in camera on a device.
- How to create strong passwords and the importance of not using the same password for every account and regularly updating them.
- About online identities, fake profiles and online relationships.
- How online advertising and influencers can influence Internet users and how they can impact on body image and self-esteem.

Engagement and education of staff

- The Limpsfield Grange Online Safety and Digital Resilience policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of Limpsfield Grange's safeguarding practice.
- Staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and will have clear procedures for reporting issues or concerns.
- Staff will be made aware that their online conduct outside of Limpsfield Grange could have an impact on their role and reputation within Limpsfield Grange. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Engagement and education of parents and carers

- Limpsfield Grange recognises that parents and carers have an essential role to play in enabling students to become safe and responsible users of the Internet and digital technology.
- We will build a partnership approach to online safety and digital resilience with parents/carers by:
  - Providing information and guidance on online safety and digital resilience in a variety of formats;
  - Requesting that parents and carers support the school's online safety rules and discuss these with their child.

Information system security

Managing personal data online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. Full information can be found in Limpsfield Grange's Data Protection policy.

Filtering & Monitoring

- SoftEgg will be the first port of call for advice regarding filtering, our filtering provider is Securly.
- The Securly system alerts the School Business Manager to any suspicious or blocked searches to enable further investigation to be carried out.
- Filtering and monitoring need to reflect real life rather than being a 'locked down' system.
- Students need to be taught positive responsible behaviour to carry forward into the workplace.
- If staff become aware of unsuitable online materials, the site must be reported to the School Business Manager who will share this information with the Designated Safeguarding Lead.
- If students become aware of unsuitable online materials, the site must be reported to the supervising member of staff.
- The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. These checks are carried out by the Designated Safeguarding Lead.
- 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.
- Games machines that have Internet access may not include filtering. Close supervision will be given to ensure appropriate use of both machine and software within the school.
- However, if a student is using a device through 4G or 5G and they are not connected to the schools WIFI then our filtering system is bypassed.

Security

Passwords:

- The school network profiles require users to input a username and password, this enables activity to be monitored in order to fulfil online safety requirements. The Online Safety Coordinator keeps a record of student passwords.
- The school will use 'strong' passwords.
- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and students must always keep their password private and must not share it with others or leave it where others can find it.

Disposal of computers and IT equipment:

- All school computer equipment is disposed of using a reputable company that wipes the data and provides the appropriate documentation to prove this has taken place.

Use of IT facilities for curriculum

- Use of the Internet and IT facilities should be clearly planned prior to the activity. Websites should be suggested and provided by bookmarks.

Managing the Limpsfield Grange website

- Limpsfield Grange will ensure that information posted on the Limpsfield Grange website meets the requirements as identified by the Department for Education (DfE).
- Limpsfield Grange 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 students' personal information will not be published on Limpsfield Grange's website without explicit student parent carer or staff permission.
- The administrator account for the Limpsfield Grange website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety and digital resilience, on our website for members of the community.

Publishing images and videos online

- In terms of online safety and digital resilience, Limpsfield Grange will ensure images and videos of students, staff, student's work and any other personally identifying material will be used, stored, archived and published in line with GDPR, the Data Protection Act, ICO guidance for schools, DFE guidance for schools and the schools' online safety rules and Staff Behaviour policy.
- Written consent from parents and carers will always be obtained before images or videos of students are electronically published.
- Photographs that include students will be carefully selected and will not enable individual students to be clearly identified.
- Staff may take photos of students for school purposes on their personal phones, for example if they are supervising offsite activities at SOLD. Any images taken must be uploaded to the school system immediately and then deleted from the members of staff's personal phone.
- Students are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.

- Any photographers that are commissioned by the school will be fully briefed on the appropriateness in terms of content and behaviour; will wear identification at all times and will not have unsupervised access to the students.
- Students are not permitted to take photos of each other, staff or the school buildings on their personal devices. They do not have permission to post any photos of students, staff or the school buildings online.

Managing emails

- Students and staff may only use approved email accounts on the school system.
- Students must immediately tell a supervising adult if they receive an offensive email.
- Staff must notify a member of the Senior Leadership Team immediately if they receive an offensive communication.
- Students must not reveal personal details or the personal details of others in email communications, or arrange to meet anyone without specific permission.
- All Limpsfield Grange staff are provided with a specific Limpsfield Grange email address to use for any official communication.
- The use of personal email addresses by staff for official Limpsfield Grange business is not permitted.
- Staff to student and / or parent email communication must only take place via the school email address.
- Emails sent to external organisations should be written carefully before sending, in the same way that an official letter from the school would be.
- Incoming emails should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how emails from students to external bodies are presented and controlled.
- The forwarding of chain letters is not permitted.

Social media

General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of the Limpsfield Grange community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of the Limpsfield Grange community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- All members of the Limpsfield Grange 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.
- Limpsfield Grange will control students and staff access to social media and social networking sites whilst on site and using Limpsfield Grange provided devices and systems.
- The use of social networking applications during working hours for personal use is not permitted.
- Inappropriate or excessive use of social media during Limpsfield Grange whilst using Limpsfield Grange devices in school or remotely may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of the Limpsfield Grange community on social media sites should be reported to the Headteacher and will be managed in accordance with existing Limpsfield Grange policies.

- Any breaches of Limpsfield Grange policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed.

Official use of social media

- Official use of social media sites by Limpsfield Grange will only take place with clear educational or community engagement objectives with specific intended outcomes e.g., increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and managed by the Headteacher. The Headteacher, Deputy Headteacher, and the Fundraising and Marketing Lead are the only members of staff with access to post on our social media accounts.
- Official Limpsfield Grange social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- All communication on official Limpsfield Grange social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official Limpsfield Grange social media sites will comply with legal requirements will not breach any common law duty of confidentiality, copyright etc.

Staff personal use of social media

- Personal use of social networking, social media and personal publishing sites will be discussed by a member of the Senor Leadership Team with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all staff (including volunteers) as part of Limpsfield Grange's Staff Behaviour policy.
- Information that staff have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role.
- Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role at Limpsfield Grange.
- Members of staff are encouraged not to identify themselves as employees of Limpsfield Grange on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff and the wider Limpsfield Grange community.
- Members of staff will ensure that they do not represent their personal views as that of Limpsfield Grange School on social media.

Students use of social media

- Safe and responsible use of social media sites will be outlined for students and their parents as part of Limpsfield Grange Online Safety rules.
- Students will be advised to consider the risks of sharing personal details of any kind on social media sites or gaming platforms which may identify them and / or their location. Examples would include real/full

name, address, mobile or landline phone numbers, the school they attend, Instant messenger contact details, information through photographs, email addresses, full names of friends/family, specific interests and clubs etc.

- Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Students will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Any concerns regarding students' use of social media and personal publishing sites, both at home, will be dealt with in accordance with existing Limpsfield Grange policies. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

Official videoconferencing and webcam use

- Students should ask permission from the supervising adult before making or answering a video conference or Zoom call.
- Video-conferencing and Zoom will be appropriately supervised according to the students' age.
- Students are not permitted to share the details of staff meeting IDs and passwords with anyone who is not a member of the staff or student communities at Limpsfield Grange.

Mobile phones

- Students are only permitted to use their phones before school on the playground to listen to music and to play games. Students are not permitted to take photos of other students or of staff.
- Day students must hand in their phones to their tutor team during morning registration. The tutor team will then store the phone securely for the school day and will reissue phones to students at the end of the school day during pm registration so that students can use them in taxis on the way home.
- Residential students hand their phones in at the beginning of their boarding week, and their phones remain securely stored upstairs by the Residential team for the duration of their stay. Residential students have access to their mobile phones for limited periods before the start of the school day; during the evenings, in communal areas which are supervised by staff. Residential students collect their phones from the Residential team on Friday mornings, and then hand them into their tutor team to securely store for the school day, until pm tutor when the phone is returned to the student.
- The sending of abusive or inappropriate text messages will be dealt with using the Limpsfield Grange Behaviour policy, where messages were sent during the school day whilst the student was at school.
- Staff personal mobile phones should be 'silent' during lessons. Staff are not permitted to use or check their phones for personal use during lessons or times when they are supervising students.
- Staff will use a school phone where contact with students and parents is required. If using a personal mobile phone or home telephone we would advise that, wherever possible, staff withhold their number. If circumstances arise that staff need to use their own phones and they cannot withhold their number, a member of the Senior Leadership Team must be informed.
- There will be occasions when students will be asked to bring their own device to a Functional ICT or WACI lesson, where they will be taught how to use the different features on a mobile phone, take and download photos, and change privacy settings, location, etc. Students will be supervised by staff at all times during these lessons.

Data Protection and online safety

- The General Data Protection Regulations (GDPR) are relevant to online safety and digital resilience since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.
- Staff or students' personal information will not be published on the school website.
- Staff will ensure that care is taken to ensure the safety and security of personal data regarding all of the school population.
- Personal data will only be stored on secure devices – computers, servers, file-servers, cloud space, or devices which require a user name and password to access the information.
- Secure accounts will be logged off after use to prevent unauthorised access.
- Screen lock to be used (Ctrl/Alt/Delete) when members of staff are away from their desk.
- Any memory stick or pen drive can be converted for encrypted use with free software – http://www.esecurityplanet.com/views/article.php/3880616/How-to-Encrypt-a-USB-Flash-Drive.htm
- However, by far the most effective way to safeguard personal data when off the school site is not to transfer personal information outside school systems if possible.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the Online Safety Coordinator or a member of the Senior Leadership Team before use in school is granted.

Responding to Online Incidents and Concerns

- All members of the Limpsfield Grange community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.)
- Emma Phillips Deputy Headteacher and deputy DSL will be informed of any online safety incidents involving child protection concerns, immediately via email (as outlined in the Limpsfield Grange Child Protection and Safeguarding policy.)
- The DSL / deputy DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Surrey Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under Limpsfield Grange's complaints procedure, which is available on the school's website.
- Any complaint about staff misuse will be referred to the Headteacher. Allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Any complaint about the Headteacher's online conduct must be referred to the Chair of Governors.
- All members of the Limpsfield Grange community will need to be aware of the importance of confidentiality and the need to follow the official Limpsfield Grange procedures for reporting concerns.
- All members of the Limpsfield Grange community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the Limpsfield Grange community.
- Limpsfield Grange will inform parents and carers of any incidents of concerns as and when required.
- Parents and students will need to work in partnership with Limpsfield Grange to resolve issues.

Illegal incidents

- If there is any suspicion that a website concerned may contain child abuse images, or if there is any other suspected illegal activity, this must be reported to the DSL or a deputy DSL immediately who will report the matter to the police and the Headteacher. If the incident involves a member of staff the Headteacher will contact the LADO.

Other incidents

It is hoped that all members of the school community will be responsible users of the digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- More than one member of the Senior Leadership Team should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by students and if necessary can be taken off site by the Police should the need arise. Use the same computer for the duration of the procedure.
- Relevant staff should have appropriate Internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to a form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement of the LADO
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- **Isolate the computer in question. Any change to its state may hinder a later Police investigation.**

Copyright Infringement and DMCA

If a website is hosted in the USA, or operates under US law, then the Digital Millennium Copyright Act will apply for copyright infringement. This is very useful when seeking to remove photographs and other material which has been copied onto sites such as Facebook and Twitter.

Monitoring the Online Safety and Digital Resilience policy

The online safety policy will be actively monitored and evaluated by the following people:

- Online Safety Coordinator (Student Support Lead)
- Designated Safeguarding Lead (Head of Residential Provision)
- Senior Leadership Team
- Headteacher
- Safeguarding and Online Safety & Filtering and Monitorinng Governor

The Online Safety policy will be monitored through:

- Lesson drop ins
- Weekly monitoring of suspicious Internet searches and reporting to the Leadership Team at weekly Leadership Team meetings
- Regular and ongoing monitoring of Internet use through Lightspeed reporting
- Regular monitoring by the Online Safety Coordinator
- Headteacher reports to Governors
- Online Safety & Filtering and Monitoring Governor visits
- Standard 3 visits and reports in the Residential Provision
- Ofsted inspections (Education and Residential)

Online Safety & Digital Resilience Policy review and evaluation schedule

The Online Safety & Digital Resilience policy is reviewed annually, and additionally in the case of the following:

- Serious and/or frequent breaches of the Online Safety Rules, Staff Behaviour policy or other in the light of online safety incidents.
- New guidance by Government/ LA /Surrey Safeguarding Children Board / Ofsted / the Police.
- Significant changes in technology used by the school or students in the wider community.
- Online safety incidents in the community or local schools which might impact on the school community.
- Advice from the Police.
- The Online Safety & Digital Resilience policy will be monitored through updates to the Curriculum Community and Student Welfare Committee
- The Governing Body will receive a report on the progress, evaluation, impact and effectiveness of the Online Safety & Digital Resilience policy regularly in the Headteacher's Report to Governors. This report will include a synopsis of any online safety incidents and how they have been resolved, listing counter measures implemented.

Related policies and documents

- Behaviour Policy including Anti Bullying
- Child Protection and Safeguarding Policy
- Complaints Policy & Procedures
- Data Protection Policy
- Dignity at Work Policy
- Disciplinary Policy & Procedure
- Equality & Diversity Policy
- Online Safety Rules (students)
- Staff Behaviour Policy (including the acceptable use of technology agreement)
- Staff Handbook
- Student Privacy Notice
- Whistleblowing Policy

National Links

- CEOP: www.thinkuknow.co.uk www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.Internetmatters.org
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk

- Internet Watch Foundation (IWF): www.iwf.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferInternet.org.uk

Review

The Governing Body of Limpsfield Grange School adopted this policy on:
It will be reviewed on:
Signed
Dated

Appendix 1

Responding to concerns regarding Youth Produced Sexual Imagery ("Sexting" or consensual and non-consensual sharing of nude and semi-nude images and/or videos)

- Limpsfield Grange recognises youth produced sexual imagery (known as "sexting" or consensual and non-consensual sharing of nude and semi-nude images and/or videos) as a safeguarding issue; all concerns will be reported to and dealt with by the DSL or one of the deputy DSLs.
- We will follow the advice as set out in the non-statutory UKCIS guidance: "Sharing nudes and semi-nudes advice for education settings" and SSCB guidance.
- Limpsfield Grange will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not view any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
- We will not send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request students to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
  o Act in accordance with our child protection policies and the relevant Surrey Safeguarding Child Board's procedures;
  o Ensure the DSL (or deputy) responds in line with the UKCIS guidance
  o Store the device securely;
- If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image. We will carry out a risk assessment which considers any vulnerability of students involved; including carrying out relevant checks with other agencies. We will inform parents/carers, if appropriate, about the incident and how it is being managed. We will make a referral to Social Care and/or the Police, as deemed appropriate in line with the UKCIS guidance.
- We will provide the necessary safeguards and support for students.
- We will implement appropriate sanctions in accordance with the Limpsfield Grange Behaviour policy but taking care not to further traumatise victims where possible.
- We will consider the deletion of images in accordance with the UKCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance;
- Images will only be deleted once the DSL or deputy DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- We will review the handling of any incidents to ensure that best practice was implemented; the Senior Leadership Team will also review and update any management procedures, where necessary.

Appendix 2

Responding to concerns regarding Online Child Sexual Abuse and Exploitation (including Child Criminal Exploitation)

- Limpsfield Grange will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Limpsfield Grange recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy DSL).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for students, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to students and other members of our community on the Limpsfield Grange website.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our child protection policies and the relevant Surrey Safeguarding Child Board's procedures;
    - If appropriate, store any devices involved securely;
    - Make a referral to Social Care (if required/appropriate) and immediately inform the Police via 101, or 999 if a child is at immediate risk;
    - Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies);
    - Inform parents/carers about the incident and how it is being managed;
    - Provide the necessary safeguards and support for students
    - Review the handling of any incidents to ensure that best practice is implemented; the Senior Leadership Team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
- Where possible, students will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Surrey Education Safeguarding Team and/or the Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL (or deputy DSL).
- If students at other setting are believed to have been targeted, the DSL (or deputy DSL) will seek support from the Police and/or the Surrey Education Safeguarding Team first to ensure that potential investigations are not compromised.

Appendix 3

Responding to concerns regarding Indecent Images of Children (IIOC)

- Limpsfield Grange will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy DSL) will obtain advice immediately through the Police and/or the Surrey Education Safeguarding Team.
- If made aware of IIOC, we will:
  - Act in accordance with our Child Protection & Safeguarding policy and the relevant Surrey Safeguarding Children Boards procedures;
  - Store any devices involved securely;
  - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), the Police.
- If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children, we will:
  - Ensure that the DSL (or deputy DSL) is informed;
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk ;
  - Ensure that any copies that exist of the image, for example in emails, are deleted;
  - Report concerns, as appropriate to parents/carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
  - Ensure that the DSL (or deputy DSL) is informed;
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk ;
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the Police via 101 (999 if there is an immediate risk of harm) and Social Care
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the Police only;
  - Report concerns, as appropriate to parents/carers.
  - Review the school's monitoring and filtering processes and systems.
- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
  - Ensure that the Headteacher is informed;
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations
  - Quarantine any devices until Police advice has been sought.

Appendix 4

Responding to concerns regarding radicalisation or extremism online

- Limpsfield Grange will take all reasonable precautions to ensure that students are safe from terrorist and extremist material when accessing the Internet in school and that suitable filtering is in place which takes into account the needs of students.
- When concerns are noted by staff that a student may be at risk of radicalisation online then the DSL or deputy DSL will be informed immediately and action will be taken in line with Limpsfield Grange's Child Protection & Safeguarding policy.
- If we are concerned that staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and the LADO will be contacted immediately.