Online Safety Policy

Contents

1. Introduction and Aims

It is the duty of Leighton Park to ensure that every pupil in its care is safe, and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse, and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction, and leisure activities. Current and emerging technologies used in and outside of school include Websites; Email and instant messaging; Blogs; Social networking sites; Chat rooms; Music / video downloads; Gaming sites; Text messaging and picture messaging; Video calls; Podcasting; Online communities via games consoles; and Mobile internet devices such as smart phones and tablets.

This policy, supported by the separate Staff IT and Communications Acceptable User Policy for all staff and pupils, is implemented to protect the interests and safety of the whole school community. It aims to:

- provide clear guidance on how to minimise risks, and
- establish clear mechanisms on how to deal with any infringements.

It is linked to other school policies outlined in section 6.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Leighton Park, we understand the responsibility to educate our pupils on Online Safety issues, teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about Online Safety and listening to their fears and anxieties as well as their thoughts and ideas.

1.1 The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism

- Contact – being subjected to harmful online interaction with other users, such as 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, such as making, sending and 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; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents, and visitors who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and legal or educational guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the separate IT Acceptable Use Policy for all staff and pupils cover both fixed and mobile internet devices provided by the school (such as chromebooks, PCs, laptops, webcams, tablets, Clevertouch boards, digital video equipment, etc.) as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smartphones, etc.).

This policy has been prepared following consultation and discussion with school stakeholders and refers to guidance from outside specialist agencies. Behaviour and safeguarding issues related to online safety for students must be recorded on MyConcern.

This policy will be reviewed every year by the DSL and DDSL in charge of online safety. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks students face online.

3. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:
Teaching online safety in schools;
Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff;
Relationships and sex education;
Searching, screening and confiscation; and it also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996

(as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

4. Roles and responsibilities

4.1 The Governing Body

The governing body of the school is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at the dates specified. The nominated member of the Governing Body for Safeguarding and Online Safety will liaise with the Designated Safeguarding Lead on a regular basis. The governing body members are regularly trained in safeguarding and promotion of welfare.

4.2 The Head and Senior Leadership Team

The Head has overall responsibility for the safety of the members of the school communities and this includes responsibility for Online Safety. The role of the Headmaster and the Senior Leadership team is to ensure that: staff, in particular the Designated Safeguarding Lead, are adequately trained about Online Safety and staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of Online Safety in connection to the school.

4.3 Designated Safeguarding Lead & Online Safety Lead

The Designated Safeguarding Lead and Online Safety DDSL have responsibility for ensuring this policy is upheld by all members of the school community and working with IT staff to achieve this. They will keep up to date on current Online Safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), and the Berkshire West Multi-Agency Safeguarding Hub.

4.4 IT Staff

The school's technical staff have a key role in maintaining an ethical and safe technical infrastructure at the school and in keeping abreast of the rapid succession of technical developments. They are responsible for the security of the school's hardware systems, its data and for induction/training the school's teaching and administrative staff in the use of IT. They have oversight of internet use and email although emails are not routinely monitored. IT staff maintain content filters and will report inappropriate usage, a daily digest of which goes to the DSL and the Designated Safeguarding Team.

4.5 All staff and volunteers

All staff are required to sign the Staff Acceptable Use Policy before accessing the school's systems after induction. Staff may also be asked to update their understanding and sign subsequent issues of the IT Acceptable Use Policy.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture to address any Online Safety issues which may arise in classrooms or around the school on a daily basis.

Staff should not encourage nor facilitate any online activity that is intrinsically unsafe or exposes pupils or other members of staff to danger or significant risk. It is the responsibility of those responsible in the classroom to monitor the online activities of the pupils through the use of: the school's safeguarding software, SENSO, normal good classroom practice such as, for example, circulating around the classroom and talking to the pupils, or positioning themselves such that the teacher can see all the screens, and to assess the risk of any online learning activity set by them.

The school Google Classroom and email facilities provide secure, closed social media and instant messaging platforms for educational purposes within the classroom, boarding or school trips, and it is expected that these are the default platforms for use when communicating with pupils or about pupils. Purely educational resource curation platforms are acceptable, but teachers must be mindful of their responsibility to check the suitability of any resource curated on the site. These should follow the expectations outlined in the staff code of conduct, Online Safety Policy and IT AUP, be for school related matters only, conducted in a professional manner, and should be closed or deleted as soon as the activity or trip is completed. The default is that a school account or school device should be used for such communications but, in the unlikely event that a personal mobile device was needed to be used due to an emergency, as soon as possible the communication should be transferred to a school device. If there is a need for a longer use of a personal device, then advice should be sought from the Designated Safeguarding Lead or the Trips Coordinator.

Staff are allowed to operate social media sites wholly administered for public facing marketing and publicity purposes under the direction of and with full knowledge of the Senior Management Team of Leighton Park but must be used with caution and moderated regularly. Personal information regarding children must be limited to their first names only, and staff should be mindful of any restrictions on individual children being photographed or named at all.

Any instance of misuse, including cyber-bullying, are to be reported immediately and dealt with according to policy.

4.6 Pupils

Pupils are responsible for using the school IT systems in accordance with the IT Acceptable Use Policy and for letting staff know if they see IT systems being misused.

4.7 Parents

Leighton Park believes that it is essential for parents to be fully involved with promoting Online Safety both in and outside of school. We regularly consult and discuss Online Safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school hopes that parents will feel able to share any concerns with the school regarding Online Safety or its misuse.

Parents and carers are responsible for endorsing the school's Pupil Acceptable Use Policy.

5. Education and training

5.1 Staff: awareness and training

New staff receive information on Leighton Park's Online Safety and IT Acceptable Use policies as part of their induction.

All staff receive periodic information updates and, at least annually, training on Online Safety and Safeguarding issues in the form of INSET training and/or internal meeting time and are made aware of their individual responsibilities relating to the safeguarding of children.

Agencies for supply teaching staff provide details of training and checks and supply teaching staff receive a briefing sheet on their first day of work that includes guidance about Online Safety. Long term agency staff receive full safeguarding training including online safety.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages;
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups; and
    - Sharing of abusive images and pornography, to those who don't want to receive such content

Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff to:

- develop better awareness to assist in spotting the signs and symptoms of online abuse;
- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks; and to
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures. These behaviours are summarised in the IT Acceptable Use Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT policies and applicable legislation.

Teaching staff are encouraged to incorporate Online Safety activities and awareness within their subject areas and adopt a culture of talking about issues as they arise.

Staff should know what to do in the event of misuse of technology by any member of the school community. If Staff have any concerns or if any incident relating to Online Safety occurs, they should report them as soon as possible directly to the school's Designated Safeguarding Lead.

5.2 Pupils: Online Safety and Safeguarding in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for Online Safety and safeguarding guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote Online Safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about Online Safety and safeguarding within a range of curriculum areas and specifically in IT and AtL lessons. Educating pupils on the dangers of technologies that may be encountered outside school may also be carried out via PSHE and by, for example, presentations in collect, as well as informally when opportunities arise, such as discussions in tutor groups.

At age-appropriate levels, and usually via PSHE, pupils are taught about their Online Safety responsibilities and how to look after their own Online Safety and safeguarding. Pupils are also taught about the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the Designated Safeguarding Lead, their tutor, as well

as parents, house parents, peers, the IT helpdesk and other school staff for advice or help if they experience problems when using the internet and related technologies.

Pupils are also encouraged to make use of the Student Pastoral and Safeguarding Info folder on their Google bookmarks bar which provides valuable resources such as: a student wellbeing guide, Whisper for anonymous disclosures, external pastoral support, NSPCC links, Kooth, Teen Tips Wellbeing Hub and YouHQ.

By the end of secondary school, students will know:

- Their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- 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 material or 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
- How information and data is generated, collected, shared, and used online
- How to identify harmful behaviours online (including bullying, abuse, or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

5.3 Parents

The school seeks to work closely with parents and guardians in promoting a culture of Online Safety. The school will always contact parents if it has any

concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their children when they use electronic equipment at home. The school therefore arranges annual discussion evenings for parents and advises about Online Safety and on the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity. All parents receive electronic links to Teen Tips – Wellbeing Hub. Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Online media literary resources

6. Policy Statements

6.1 Cyber-bullying

6.1.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.1.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors, and volunteers (where appropriate) receive training on cyber-bullying, its impact, and ways to support students, as part of safeguarding training (see section 5 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate, or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.2 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads, Chromebooks, and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete the material, or
- Retain it as evidence (of a possible criminal offence or a breach of school discipline), and/or
- Report it to the police

If a staff member believes a device may contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people and any searching will be carried out in line with this guidance.

Staff will also confiscate the device to give to the police if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

6.3 Use of school and personal devices

6.3.1 Staff

School devices assigned to a member of staff as part of their role must have a unique password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Some staff may have devices which have encryption to protect data stored on them.

Staff are permitted to bring in personal devices such for their own use only and are expected to use them within professional bounds and keeping to the IT Acceptable Use Policy.

Personal telephone numbers, email addresses, or other contact details should not normally be shared with pupils or parents; if it is necessary to do so, any pupil or parental contact details should be removed from personal phone or email directories as soon as possible.

6.3.2 Pupils

Pupils are allowed to bring mobile phones to school. According to the rules within the Gold Book, years 7-11 should store their phones appropriately during the day and these should not be visible and may only be taken out under the direction of a member of staff during school hours. This applies to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The school provides technologies for pupil use. Chromebooks are provided to all pupils in the school in years 7-11 and an IT facilities including iPad, desktops, tablet, Chromebooks etc. are available for use in learning areas.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with The SENDCO to agree how the school can appropriately support such use. The SENDCO will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1 and 2). Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

6.4 Use of Internet and email

6.4.1 Staff

Staff are expected to maintain professional conduct at all times when accessing personal email or any personal website, be this on a school provided computer or their own device. Staff should use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school, as outlined in the Staff Code of Conduct.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff who need one are issued with their own school email address for work purposes for use on our network and by remote access. Teaching staff are also issued with a @leightonpark.com email address for communicating directly with pupils about curriculum matters and for use on google classroom. Access is via a personal login, which is password protected and all work email communications should be conducted using this email address. Staff should be aware that email communication sent from the school email systems is bound to a school owned domain name and, as such, all communications represent the school. Staff should represent only the most positive views when communicating with parents, suppliers, and other agencies outside of the school domain. Staff should note that email, some elements of social network traffic and instant messaging may be virus scanned, subject to an acceptable word list and should only be used for bona fide school business. A pre-formed disclaimer may be added to each email without explicit permission of the staff member.

Personal email should therefore be sent through one of the many web-mail services such as Gmail or Hotmail mail servers rather than the school email account. It is recommended that this kind of activity is kept on personally owned devices such as smartphones and tablets etc.

6.4.2 Social Networks

Staff are expected to use social networks responsibly and to consider the ramifications of posting messages from school premises and computers or to online groups with memberships of current students or parents. As a default, a separate social network from the member of staff's school account and identity should be used for school purposes. Pupils should not

be exposed to contact with other non-Leighton Park authorised adults across school related social networks nor with staff using their personal email or social network accounts. Pictures of staff and pupils published on the internet should be in line with the school's policy on use of pupil images and staff should be mindful of misinterpretation or manipulation of such images when placed online.

Staff must immediately report to the Designated Safeguarding Lead the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and they must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the IT technical team.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- breach confidentiality, copyright, data protection legislation; or
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion, or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive or bring Leighton Park into disrepute.

Any digital communication between staff and pupils or parents/carers must be professional in tone and content. Under no circumstances should staff contact, on school business, a pupil or parent/carer using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

6.4.3 Governors

Additionally, governors are specifically provided with their own personal school-based email address separate to the main school system but bound to a school owned domain and have their own separate area where documents are stored and available to access online. This enables them to conduct all official governor business associated with the school securely via the school email system and not on a personal email address.

6.4.4 Pupils

All school pupils are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure and must be used for all school-assigned working

assignments / research / projects. Pupils should be aware that email communications go through the school network and, although school email addresses are not routinely monitored, they may be subject to viewing and are therefore not necessarily private.

There is strong antivirus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for schoolwork / research purposes, pupils should contact the IT technical team for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to the DSL Team/IT technical team/or another member of pastoral staff.

The school expects pupils to think carefully before they post any information online, or re-post or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of an inappropriate or distressing nature directly to the DSL Team/or another member of pastoral staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being dealt with under the school's IT Acceptable Use Policy and the Behaviour and Discipline Policy. Pupils should be aware that all internet usage via the school's systems and its wifi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for schoolwork / research purposes, pupils should contact the IT technical team for assistance.

6.5 Data storage and processing

The school takes its compliance with the Data Protection Act 1998 and UK GDPR seriously. Please refer to the Data Protection Policy and privacy notices, and the IT Acceptable Use Policies for further details.

Staff and pupils are expected normally to save all data relating to their work to their Google Drive Account, or one of the other safe storage options including the network shared drives, and Microsoft 365. Any portable storage media should be encrypted, or password protected. The IT technical team can be consulted for advice in this respect.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the DSL Team and the IT technical team.

6.6 Password security

Pupils and staff have individual school network logins and email addresses and storage on the cloud. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should: use strong passwords, which should be changed regularly; not write passwords down and not share passwords with other pupils or staff.

6.7 Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying, stalking, or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet (e.g., on social networking sites).

Parents are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published or tagged on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.
Staff and volunteers are allowed to take digital / video images to support educational aims but must follow this policy and the IT Acceptable Use Policy. School equipment for taking images is available and personal devices should not be used as far as is possible with any images being deleted from their personal devices once finished with.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils are encouraged not to share, publish, or distribute images of others without permission and should act responsibly if they do so.

Photographs published for school promotion purposes that include pupils will be selected carefully, will be used according to our Terms and Conditions, and will comply with good practice guidance and school policies on the use of such

images. Pupils' full names should not be used anywhere on a website or blog, particularly in association with photographs that connect them directly to the school.

6.8 Misuse

Leighton Park will not tolerate illegal activities or activities that are inappropriate in a school context and will report illegal activity to the police. If the school discovers that a child or young person is at risk because of online activity, it may seek assistance from the Area Safeguarding Adviser, the Area Online Safety Adviser or CEOP. Any online safeguarding concerns should be reported to the Designated Safeguarding Lead.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures. The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy, or any other computer misuse where applicable.

7. Monitoring

Behaviour and safeguarding issues related to online safety for students must be recorded on MyConcern.

This policy will be reviewed every year by the DSL and DDSL in charge of online safety. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks students face online.

8. Links with other policies

Safeguarding and Child Protection Policy
Behaviour and Discipline policy
Staff Code of Conduct
Data Protection Policy and Privacy Notices
Complaints Procedure
IT Acceptable Use Policy

Author: Nicky Hardy, Deputy Head Pastoral; Alex Leighton DDSL Online Safety
Sign off: Matthew Judd, Head
Date of last review: Feb 2023
Date of next review: Feb 2026
Publication: https://portal.leightonpark.com/