Online Safety Policy

Contents

Online Safety Policy

Section 1: General

Policy Aims

The School recognises that Information Technology, (IT) and the Internet are excellent tools for learning, communication and collaboration and can bring many benefits to students, staff and parents. The Internet is used to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the School's management functions and the School will endeavour to equip students with all the necessary IT skills for them to progress confidently between the key stages, into further education, or into a professional working environment once they leave the School. It is also an important part of the School's pastoral care programme to ensure that students are provided with the education and resilience needed to protect themselves and their peers from online dangers.

Technology is advancing rapidly and is now a large part of everyday life, education and business. However, it is important that all members of the school community are aware of the potential dangers of using the internet and understand the importance of using it appropriately.

The School has a 'duty of care' towards any staff, students or members of the wider school community, to educate them on the risks and responsibilities of online safety and this policy governs all individuals who are given access to the school's IT systems e.g. staff, governors and students. However, sections of this policy may not be relevant to certain individuals due to their position, job role or subject to the age of the student.

The School understands that some adults and young people will use technologies to harm children and there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating IT activity in School and providing members of the School community with a good understanding of appropriate IT use outside of school hours.

Online safety does not just cover the Internet and available resources, but all different types of devices and platforms, both school and privately owned (e.g. Smartphone devices, laptops, wearable technology and other electronic communication technologies). These are accessible within the school for enhancing the curriculum, to challenge students, and to support creativity and independence.

Related Policies

Due to the nature of online safety the policy needs to cover a broad area of technology. Some of these technologies and processes are already detailed in our other School Policies. This policy will reference these where applicable and includes, Safeguarding and Child Protection Policy, Acceptable Use of ICT Policy – Students, Acceptable Use of ICT Policy – Staff, Chromebook Acceptable Use Policy, Behaviour and Discipline Policy (including searching and confiscation), Anti-Bullying Policy, Educational Visits Policy, Permanent Exclusion and Removal: Review Procedure and Staff Code of Conduct.

Roles and Responsibilities

Online safety is the responsibility of the whole school community. The Governing Body of the School, in conjunction with the Senior Leadership Team, are responsible for ensuring the safety of all those in the School Community, especially students, and for responses to online safety incidents that occur both in and outside of school on school business, whether on personal or school networks or devices.

The Designated Safeguarding Lead alongside the Director of IT have overall responsibility for this policy. He / she will work closely with the Head of PSHE and senior pastoral and academic staff in this regard.

The Governing Body undertakes a regular review of the School's safeguarding procedures and their implementation, which will include consideration of how students may be taught about safeguarding, including online safety, through the School's curricular provision, ensuring relevance, breadth and progression.

Training

Staff

The School provides online safety guidance to staff to better protect students and themselves from online risks and to deal appropriately with online safety incidents when they occur. Ongoing staff development training includes training on online safety together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles within the organisation, legal changes and requirements.

The IT Strategy Group meets regularly in school to discuss all matters relating to Online Safety and wider aspects of technology use at Leighton Park.

Students

Digital safety is a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum. A broad Online Safety curriculum is provided in the following ways:

- A planned Online Safety curriculum is provided as part of Computing / PSHE / other lessons and is regularly revisited - visiting speakers also contribute to the programme as appropriate.

- Key Online Safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities;

- Students are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information;

- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;

- Students are helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school;

- Staff act as good role models in their use of digital technologies, the internet and mobile devices

- In lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.;

- Where students are allowed freely to search the internet, staff are vigilant in monitoring the content of the websites they visit;

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result

in internet searches being blocked. In such a situation, staff can request that the Technical Staff temporarily remove those sites from the filtered list for the period of study. Any request to do so should be in writing, with clear reasons for the need to relax filters, to the IT Department who will consult with the DSL.

Parents/ Carers and Guardians

Parents, carers and guardians play an essential role in the education of their children and in the monitoring / regulation of their children's on-line behaviours. It is easy to underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and parents may be unsure about how to respond.

The School therefore seeks to provide information and awareness to parents and carers through:

- Newsletters, and the Parent Portal
- Occasional seminars organised by the DSL and the team
- Reference to the relevant web sites / publications

e.g. o www.saferinternet.org.uk

o http://www.childnet.com/parents-and-carers

Policy availability and communication

Online safety is integrated into the curriculum as well as being specifically addressed in the PSHE curriculum. On joining the School, new students and staff are required to agree to comply with the IT Acceptable Use Policy.

Systems and security

The School is responsible for reviewing and managing the security of the IT services and networks that it operates and takes the protection of School data and personal protection of the School community seriously. This means protecting the School network, (as far as is practicably possible), against viruses, hackers and other external security threats. The security of the School information systems and users will be reviewed regularly by the IT Support team and other third parties engaged with the School and led by the Director of IT. Anti-Virus and Malware protection software is updated regularly. Other safeguards that the School takes to secure computer systems include:

- Making sure that unapproved software is not downloaded or installed to any School computers and that files held on the School network are regularly checked for viruses;
- Ensuring that the use of user logins and passwords to access the School network is enforced and unique;
- Requiring that portable media containing School data or programmes are encrypted and not taken off-site without specific permission from member of the Senior Management Team.
- The use of VPNs to circumvent IT security filters are not installed on any machine or in use on the School's network regardless of device.

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for students, (some age specific). The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a School computer or device connected to the School network.

Safeguarding Technology and the School Environment

Digital Technology forms a central part of education at Leighton Park School. We use computers in class, and the incidence of social media and smart devices impacts on the daily lives of the entire School Community. However, electronic ways of working and communication afforded by the School and personal devices present considerable dangers and risks, not least in respect of the personal safety of students, general treatment of others and security of data. To address such matters, the School has the following systems and processes in place:

- Filters to ensure that inappropriate sites are not accessible via the internet. The filters may be adjusted, where justified for educational purposes, and systems are in place to prevent over blocking (excessive filtering) to ensure that this does not lead to unreasonable restrictions as to what children can be taught online. The level of filtering is determined by a risk assessment addressing safeguarding issues, including the Prevent Duty;

- A change to the filtering level may be requested by any member of the School Community. This change request goes to the Director of IT who will research the request and then make a recommendation to the DSL who will decide if the change should be made. Users are not permitted to use any programme or software that might allow them to bypass the filtering/security systems in place and all users have a responsibility to report immediately to the DSL and/or the Director of IT any infringements of the filtering policy, or access to improper sites, of which they become aware;

- Monitoring systems which oversee internet use and inappropriate communication, and which flag up potential concerns quickly to the DSL Team. No filtering system can guarantee complete protection against access to unsuitable sites, and the School therefore monitors activities of users and usage of its internet without prior notification to, or authorisation from, users. Users of the School's e mail and internet services cannot expect privacy in connection with anything they create, store, send or receive using the School's systems;

- Online Safety and security education for students and training for staff;

- Oversight of use of technology during lessons;

- Reporting systems where there are incidents or concerns involving inappropriate use of technology, where there are safeguarding concerns;

- A clear policy for the use of a wide variety of School-supplied and personal devices/equipment (please see above);

- The proper use of passwords, protection of data and regular reviews and audits of the safety and security of the School's technical systems;

- Appropriate security measures to protect servers, firewalls, routers, wireless systems, workstations, and mobile devices from accidental or malicious attempts

which might threaten the security of the School systems and data. These are tested regularly. The School's infrastructure and individual workstations are protected by up to date virus software;

An IT partner is responsible for working with the School to ensure that the School's technical infrastructure is secure and is not open to misuse or malicious attack. The IT partner is responsible for ensuring that:

- The School meets the required Digital Safety technical requirements;
- Users may only access networks and devices through a properly enforced password protection policy, which requires that passwords be changed regularly;
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- It is all users' responsibility to alert the Director of IT if any inappropriate sites can be (or have been) accessed;
- The School is kept up to date with digital safety technical information in order to effectively carry out the digital safety role and to inform and update others as relevant;
- The use of the School network / internet / remote access / email is regularly monitored and that monitoring software / systems are implemented and updated as required.

For the avoidance of doubt, any safeguarding concerns arising from the use of technology in the school environment, or in connection with school activities, are to be reported/actioned in accordance with the School's Child Protection and Safeguarding Policy and the Staff Code of Conduct. Please also see Annex 1 below for more specific safeguarding information relating to Online Safety.

Cyberbullying

Cyberbullying can be defined as "the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others" (Belsey, http://www.cyberbullying.org/). It is an aggressive, intentional act carried out repeatedly over time, often against a victim who cannot easily defend himself / herself.

Cyber-bullying could involve communications by various electronic media, including, (but not limited to):

- Texts, instant messages or calls on mobile phones;
- The use of mobile phone camera images to cause distress, fear or humiliation;
- Posting threatening, abusive, offensive or humiliating material or comments on websites (including blogs, personal websites and social networking sites such as Facebook, Instagram, Twitter or YouTube);
- Using e-mail to message others in a threatening or abusive manner; or
- Hijacking/ cloning e-mail accounts.

Cyberbullying, as with any other form of bullying, is taken very seriously by the School and will be managed through the School's Anti-Bullying Policy, which should be read alongside this

policy and which sets out specific strategies to prevent and tackle bullying. All our students are encouraged to tell a member of staff at once if they know or suspect that bullying is taking place.

It is made very clear to all members of the School community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

By law, the Head and staff, to such extent as is reasonable, are granted powers to regulate the behaviour of students when they are off the School site as well as on it, and to impose disciplinary penalties for inappropriate behaviour. Powers are also given to School staff about the searching of electronic devices and the deletion of data in appropriate circumstances. Such powers will be exercised in relation to incidents of cyber-bullying, or other online safety incidents covered by this policy, the School's Behaviour Policies and/or Anti-Bullying Policy, even where such incidents take place outside of the school, if they are linked to membership or activities of the School.

Section 2: Guidance for Students and Staff

E-Mail

Email is an essential part of School communication.

The School has the right to monitor emails and attachments where there is suspicion of inappropriate use and access in school to external personal email accounts may be blocked. Further guidance and procedures for administrators are detailed within the Conduct for IT Administrators Policy.

School email accounts and appropriate use

Staff should be aware of the following when using email in School:

- Staff should only use their School email accounts for school-related matters, contact with other professionals for work purposes and to communicate with students, parents or guardians. Personal email accounts should not be used to contact any of these people.

- Emails sent from School email accounts should be professional and carefully written. Staff are always representing the School and should take this into account when starting any email communications.

- The School permits the incidental use of staff School email accounts to send personal emails if such use is kept to a minimum and takes place substantially out of normal working hours. The content should not include or refer to anything which is in direct competition to the aims and objectives of the School nor should it include or refer to anything which may bring the School into disrepute. Personal emails should be labelled 'personal' in the subject header. Personal use is a privilege and not a right. If the School discovers that any member of staff has breached these requirements, disciplinary action may be taken.

- For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by their Head of Department or a senior member of staff.

- Staff must tell their Head of Department or a member of the Senior Management Team if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

- The forwarding of chain messages is not permitted in School.

- Incoming email should be treated as suspicious and attachments not opened unless the author is known.

The full protocol for staff use of the Internet and email is set out in the IT Acceptable Use Policy - Staff.

Students should be aware of the following when using email in School:

Students are informed to follow these guidelines through the IT curriculum and in any instance where email is being used within the curriculum or in class:

- All students are provided with a School email account and students may only use approved email accounts on the School system during School hours.

- Students are warned not to reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission. Excessive social emailing can interfere with learning and in these cases, will be restricted.

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

- The forwarding of chain messages is not permitted in School.

- Incoming email should be treated as suspicious and attachments not opened unless the author is known.

The full protocol for student use of the Internet and email is set out in the IT Acceptable Use Policy**.**

Social Media

Social media sites have many benefits, however both staff and students should be aware of how they present themselves online. Students are informed about the risks and responsibility of using social media, including the dangers of uploading personal information and the difficulty of taking it down completely once uploaded (often referred to as a “digital tattoo”).

The IT Department under the leadership of the Director of IT will control access to social networking sites via the School network dependant on the age of the student. In addition, the School encourages parents with Children under the ages of 13 to follow the guidance of social media sites such as Facebook and not give their child access.

Please refer to the School’s Social Media Policy for further details.

School website and external marketing

The School website is viewed as a useful tool for communicating School ethos and practice to parents and the wider School community.

A team of staff, under the leadership of the Director of Marketing and Admissions, are responsible for publishing and maintaining the content of the School website.

Staff and Students are not permitted to publish anything on the internet that could bring the school into disrepute.

Use of digital images

Photographs and students' work bring the School to life, showcase students' talents, and add interest to publications both online and in print that represent the School. However, the School acknowledges the importance of having safety precautions in place to prevent the misuse of such material. Please see the School's Taking Storing and Using Images of Children Policy for full guidance.

Internet Usage

Evaluating Content

With so much information available online, it is important that students learn how to evaluate internet content for accuracy and intent. This is approached by the School as part of digital literacy across all subjects in the curriculum and students are taught to be critically aware of materials they read and shown how to validate information before accepting it as accurate, (eg. "fake news").

Copyright and Plagiarism

Students are taught to acknowledge the source of information used and to respect copyright. The School will take any intentional acts of plagiary very seriously.

Managing emerging technologies

Technology is progressing rapidly, and innovative technologies are emerging all the time. The School will risk-assess any new technologies before they are allowed in School and will consider any educational and pedagogical benefits that they might have. The School keeps up-to-date with modern technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Digital footprint

Students and Staff are made aware of the digital footprint that they create when using the internet and social media and the possible consequences of building up a negative digital footprint.

Personal data

Personal data is recorded, processed, transferred and made available according to the Data Projection Act 2018 and EU General Data Protection Regulation. Please see the School Data Protection Policy and relevant Privacy Notices for further guidance.

Concerns

If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's Safeguarding Policy and Child Protection Procedures (available on the School website).

If staff or students discover unsuitable sites then the URL, time, date and content must be reported to the IT Department or any member of staff, (who will report this to the IT Department). Any material found by members of the School community that is believed to be unlawful will be reported to the appropriate agencies via the Director of IT or a member of the Senior Management Team. Regular checks will take place to ensure that filtering services and online safety processes are in place, functional and affective. The responsibility of this falls to the Director of IT and Designated Safeguarding Lead, however the responsibility may be delegated to others within those teams. Reports are produced automatically from the IT security systems to members of the to the Designated/ Deputy Safeguarding Leads, (DSLs) for Students and HR Department for staff. It is the responsibility of the DSL Team to action items in those reports and to request any sanctions if required.

Related Legislation and Guidance

Legislation

The Education and Inspections Act (2006)

The Independent Schools Standard Regulations (2014)

The Equality Act (2011)

The Education Act (2011)

The Children Act (2004)

Protection from Harassment Act (1997)

Malicious Communications Act (1988)

The Communications Act (2003)

Public Order Act (1986)

Sexual Offences Act (2003)

Protection of Children Act (1999)

General Data Protection Regulation (2018)

Guidance

Handbook for the Inspection of Schools – a commentary (ISI) (September 2018)

Keeping Children Safe in Education (Dfe September 2018)

Preventing and tackling bullying - Advice for headteachers, staff and governing bodies (Dfe October 2014)

Cyberbullying: Advice for headteachers and school staff (Dfe 2014)

Supporting Children who are bullied (Dfe 2014)

Mental Health and Behaviour in schools (Dfe March 2016).

Behaviour and discipline in Schools (Dfe 2016)

Prevent Duty Guidance (2015)

Counselling in schools: a blueprint for the future (February 2016)

Working Together to Safeguard Children (2018)

Sexual Violence and Sexual Harrassment between Children in Schools and Colleges (Dfe May 2018).

Searching, screening and confiscation – Dfe 2018

Related Websites

https://www.saferinternet.org.uk/advice-centre/teachers-andprofessionals/appropriate-filtering-and-monitoring

www.kidscape.org.uk

www.childnet.com

www.gov.uk/government/publications/preventing-and-tackling-bullying

https://www.thinkuknow.co.uk/ (CEOPs)

Annex 1: Identifiable Risks

Inappropriate contacts and non-contact sexual abuse

Concerns may be raised about a child being at risk of sexual abuse as a consequence of their contact with an adult they have met over the internet. If reported to the School, students and parents are advised on how to terminate the contact and change contact details where necessary to ensure no further contact. Parents are advised to be vigilant of their child's internet use and report any concerns or incidents.

Children may also be sexually abused online through video messaging such as Skype or Oovoo. In these cases, perpetrators persuade the child concerned to carry out sexual acts while the perpetrator watches/records them. The perpetrators may be adults but may also be peers. In the event of such an incident, the child should be taught how to use the CEOP "Report Abuse" button (displayed on the school website homepage) parents should contact the police to report the incident. The School also encourages students to use Toot Toot to report concerns about themselves or other peers.

Staff and parents should contact either Windsor and Maidenhead Safeguarding Children Board on **01628 683234** or Reading Safeguarding Children Board on **01189 373269** (or if outside working hours), the Reading Emergency Duty Team on **01344 786543** or Windsor and Maidenhead Emergency Duty Team on **01628 683234** for advice on making a referral where there are concerns that the child:

- is being groomed for sexual abuse
- is planning or has arranged to meet with someone they have met on-line
- has already been involved in making or viewing abusive images
- has been the victim of non-contact sexual abuse.

If staff or parents are aware that a child is about to meet an adult they have made contact with on the internet, they should contact the police on 999 immediately.

Online Child Sexual Exploitation (CSE)

CSE describes situations where a young person takes part in sexual activity either under duress or in return for goods, food or accommodation. A key element of CSE is that there is a power imbalance in the relationship, for example often the perpetrator is much older than the child, who may not be aware that they are being abused.

Staff should be aware that children can be sexually exploited online, for example posting explicit images of themselves in exchange for money or goods.

If staff are concerned that a child they work with is being sexually exploited online, they should inform the Designated Safeguarding Lead immediately, who may make a multi-agency referral.

Contact with violent extremists

Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

The Channel project is part of the government's Prevent strategy to divert young people away from extremism, and the Designated Safeguarding Leads have received training.

Staff need to be aware of those students who might be targeted by or exposed to harmful influences from violent extremists via the internet. Young people should be warned of the risks of becoming involved in such groups and it is against the School's rules to access such sites.

The School ensures that adequate filtering is in place and reviews the filtering process whenever there is any incident of a student accessing websites that advocate violent extremism.

The DSL records and reviews all incidents in order to establish whether there are any patterns of extremist groups targeting the service and where relevant would contact the relevant agencies to report the situation.

If there is evidence that a young person is becoming deeply enmeshed in extremist narrative, staff would seek advice on accessing programmes under the Channel project to prevent radicalisation via their email address: **counter.extremism@education.gsi.gov.uk** or call **020 7340 7264.**

Websites advocating extreme or dangerous behaviours

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

The School can provide young people with an opportunity to discuss issues such as self-harming and suicide in an open manner and support any young person who is affected by these issues.

Staff receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.

Where staff are aware that a young person is accessing such websites and that this is putting them at risk of harm, they should consider making a referral to the relevant Children's Services (depending on which county the child li

Annex 2: Internet Usage

Staff and students must agree to comply with IT Acceptable Use Policies before being permitted to access the School IT systems. Signatures are not required for requirement to adhere to the policies but are sought in order to ensure all users are aware of their responsibilities.

The School maintains a current record of all staff and students who are granted access to the school ICT systems.

Annex 3: TAKING, STORING AND USING IMAGES OF CHILDREN POLICY

1. This Policy

This Policy is intended to provide information to students and their parents, carers or guardians (referred to in this policy as "parents") about how images of students are normally used by Leighton Park School ("the School"). It also covers the School's approach to the use of cameras and filming equipment at school events and on school premises by parents and students themselves, and the media.

It applies in addition to the School's terms and conditions, and any other information the School may provide about a particular use of student images, including e.g. signage about the use of CCTV; and more general information about use of students' personal data, (e.g. the School's Privacy Notices). Images of students in a safeguarding context are also dealt with under the school's Safeguarding Policy and Child Protection Procedures.

Certain uses of images are necessary for the ordinary running of the school; other uses are in the legitimate interests of the school and its community and unlikely to cause any negative impact on children. The school is entitled lawfully to process such images and take decisions about how to use them, subject to any reasonable objections raised.

Parents who accept a place for their child at the School are invited to agree to the School using images of them as set out in this policy, by signing the Consent Form sent out with the School's Terms and Conditions (see Appendix 1). However, parents should be aware of the fact that certain uses of their child's images may be necessary or unavoidable (for example, if they are included incidentally in CCTV or a photograph).

We hope parents will feel able to support the School in using student images to celebrate the achievements of students, sporting and academic, promote the work of the School, and for important administrative purposes such as identification and security.

Any parent who wishes to limit the use of images of a student for whom they are responsible should contact the Director of Marketing and Communications in writing. The School will always respect the wishes of parents/guardians (and indeed students themselves) wherever reasonably possible, and in accordance with this policy.

Parents should be aware that from around the age of 12 and upwards the law recognises students' own rights to have a say in how their personal information, including images, are used.

2. Use of Student Images in School Publications

Unless the relevant student or his or her parent has requested otherwise, the School will use images of its students to keep the School Community updated on the activities of the School, and for marketing and promotional purposes, including:

- on internal displays (including clips of moving images) on digital and conventional notice boards within the School premises;
- in communications with the School Community (parents, students, staff, Governors and alumni) including by email, and by post;

- on the School's website and, where appropriate, via the School's social media channels, e.g. Twitter and Facebook. Such images would not normally be accompanied by the student's full name; and

- in the School's prospectus, and in online, press and other external advertisements for the School. Such external advertising would not normally include students' names and in some circumstances the School will seek the parent or student's specific consent, depending on the nature of the image or the use.

The source of these images will predominantly be the School's marketing department and other appropriate staff (who are subject to policies and rules in how and when to take such images) in relation to school events, sports or trips. The School will only use images of students in suitable dress and the images will be stored securely and centrally.

3. Use of Student Images for Identification and Security

All students are photographed in September each year, and annually thereafter, for the purposes of internal identification. These photographs identify the student by name, year group, house and form/tutor group.

CCTV is in use on school premises and will sometimes capture images of students. Images captured on the School's CCTV system are used in accordance with the relevant Privacy Notice, and any other information or policies concerning CCTV which may be published by the school from time to time. Please see The School's CCTV Policy for further information, (Annex 9 of the Online safety Policy).

4. Use of Student Images in the Media

For events or school activities in which students are participating where the media is expected to attend, we will make every reasonable effort to ensure that any student whose parent or carer has refused permission for images of that student, or themselves, to be made in these circumstances are not photographed or filmed by the media, nor such images provided for media purposes.

The media often asks for the names of the relevant students to go alongside the images, and these will be provided if consent has been given.

5. Security of Student Images

Professional photographers and the media are accompanied at all times by a member of staff when on School premises. The School uses only reputable professional photographers and requires that makes every effort to ensure that any images of students are held by them securely, responsibly and in accordance with the School's instructions.

The School takes appropriate technical and organisational security measures to ensure that images of students held by the School are kept securely on School systems, and protected from loss or misuse, and in particular will take reasonable steps to ensure that members of staff only have access to images of students held by the School where it is necessary for them to do so.

All staff are given guidance on the School's Policy on Taking, Storing and Using Images of Students, and on the importance of ensuring that images of students are made and used responsibly, only for school purposes, and in accordance with the School's policies and the law.

6. Use of Cameras and Filming Equipment (including mobile phones) by Parents

Parents are welcome to take photographs of (and where appropriate, film) their own children taking part in school events, subject to the following guidelines, which the School expects all parents to follow:

When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and filming devices with consideration and courtesy for cast members or performers on stage and the comfort of others.

Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; the School therefore asks that it is not used at indoor events.

Parents are asked not to take photographs of other students, except incidentally as part of a group shot, without the prior agreement of that student's parents.

Parents are reminded that such images are for personal use only. Images which may, expressly or not, identify other students should not be made accessible to others via the internet (for example on Facebook), or published in any other way.

Parents are reminded that copyright issues may prevent the School from permitting the filming or recording of some plays and concerts. The School will always print a reminder in the programme of events where issues of copyright apply.

Parents may not film or take photographs in changing rooms, the swimming pool or backstage during school productions, nor in any other circumstances in which photography or filming may embarrass or upset students.

The School reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any parent who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images.

The School sometimes records plays and concerts professionally (or engages a professional photographer or film company to do so), in which case CD, DVD or digital copies may be made available to parents for purchase. Parents of students taking part in such plays and concerts will be consulted if it is intended to make such recordings available more widely.

7. Use of Cameras and Filming Equipment (including mobile phones) by Staff (Teaching & Support)

Photographs or video will only be taken by a designated staff member/s. Where photographs are taken by staff to give evidence of students' progress, or to record a trip or sporting event, photographs can only be taken on school equipment. Staff must not use their own camera, mobile phone or tablet. Photographs/video must then be downloaded onto school computers. Photographs or video cannot be used or passed on outside the School.

When taking photographs in School, staff must:

- be clear about the purpose of the activity and what will happen to the photographs when the lesson/activity is concluded;
- ensure that photographs are taken for valid educational purposes and, if in doubt, consult with their line manager;
- ensure that all images are available for scrutiny in order to screen for acceptability;
- be able to justify images of children in their possession;

- avoid making images in one to one situations;
- not have images of students stored on personal cameras, devices or home computers;
- not make images of students available on the internet, other than through the official School network/website with permission from parents and senior leaders.

8. Use of Cameras and Filming Equipment by Students

All students are encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issues to a member of staff.

The use of cameras or filming equipment (including on mobile phones) is not allowed in toilets, washing or changing areas, nor should photography or filming equipment be used by students in a manner that may offend or cause upset.

Students are told they should not film or take photographs of other members of the school community (students and staff), other than where there is a justifiable, educational reason. Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

Where there is an allegation about a student taking inappropriate images, a senior member of the pastoral team may request access to images stored on mobile electronic devices and/or cameras and ask the student to delete the images in question. Photographs of any member of the School community are not permitted to be displayed publicly around the school campus unless in accordance with this Policy.

The misuse of images, cameras or filming equipment in a way that breaches this Policy, or any of the School's other policies including but not limited to the Anti-Bullying Policy, Behaviour, Rewards and Sanctions Policy, Data Protection Policy, and Online safety Policy is always taken seriously, and may be the subject of disciplinary procedures.

Appendix 1

(On headed paper)

Use of photographic images of children: Consent Form

Child's name: _____

House: _____ Year Group _____

We are now required by law to gain parental permission from parents in order to use pictures of children in any publication. This includes the website, social media, the prospectus and articles submitted to the local press.

Sometimes it will be the photograph only that will be used. At other times (particularly in the local press and the school magazine) full names will also be published.

Please answer questions 1 and 2 below, then sign and date the form.

1. May we take photographs of your child and use them (unidentified by their full name):

- In school publications?
- On the School's website?
- On film?

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.

Please circle your answer: Yes / No

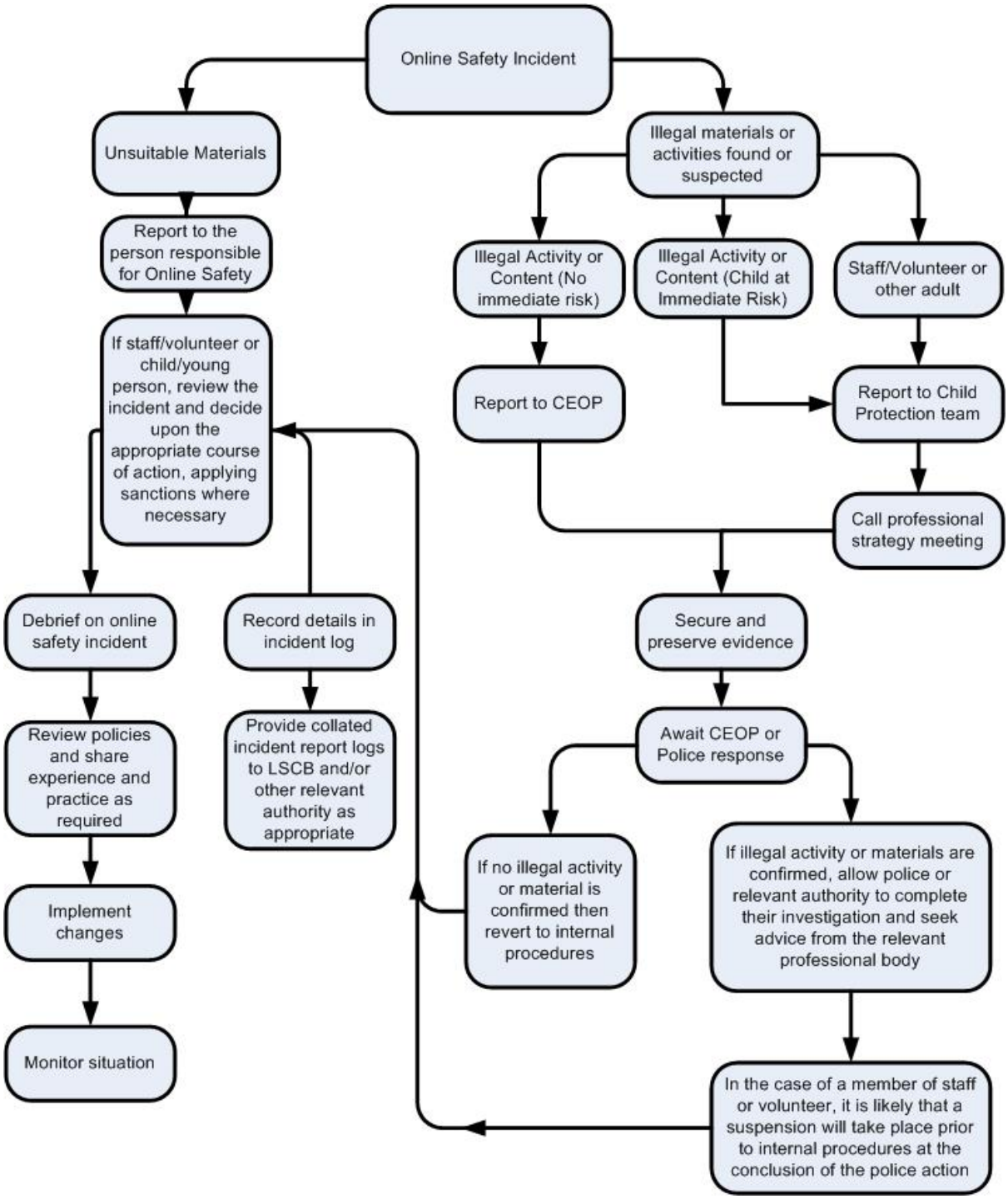
2. Do you consent to your child being photographed by local newspapers and other news media, on the basis that their full names will be published along with the picture?

Please circle your answer: Yes / No

Signed _____ (Parent/Guardian)

Date _____

Annex 4: Illegal Incidents



Annex 5: Other Incidents

It is hoped that all members of the school will be responsible users of 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:

- Have more than one senior member of staff 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 young people 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.
- It is important to ensure that the 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 also 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 the 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 by Local Authority/ Social Services
    - 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
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

- **Isolate the computer/ device in question as best you can. Any change to its state may hinder a later police investigation.**
  It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.

Author:	Eddie Falshaw, Deputy Head
Sign off:	Matthew Judd, Head
Reviewed:	April 2019
Next Review Date:	April 2022
Publication:	Z:\Policies\Current Policies\Online Safety Policy V:\School Policies\Online Safety Policy http://www.leightonpark.com/parents/policies