Lampard Community School

ONLINE SAFETY POLICY

Online Safety Policy

Lampard Community School is committed to providing a caring, friendly and safe environment for all of our students to enable them to learn in a relaxed and secure environment. Part of providing security is keeping students safe online and teaching them about using digital technology in a responsible way.

This policy should be read in conjunction with the school Child Protection and Safeguarding policy, Behaviour and Physical Contact policy, Anti Bullying policy, Acceptable Use of ICT agreements and the Data Security Policy.

Development / Monitoring / Review of this Policy

This policy was developed by the Assistant Head - Care and Safeguarding in consultation with the Headteacher and ICT Technical staff. It will be monitored by the Assistant Head - Care and Safeguarding who is also the Designated Safeguarding Lead and Online Safety co-ordinator. This policy will be reviewed annually or when updates/amendments are required.

Schedule for Monitoring and Review

This online safety policy was approved by the *Governing Body on:*	*June 2019*
The implementation of this online safety policy will be monitored by the:	*Governing Body, Senior Leadership Team, Designated Safeguarding Lead, ICT & PLS Curriculum Co-ordinators, Online Safety Working Group*
Monitoring will take place at regular intervals:	*Annually*
The *Governing Body* will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
The Online safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*June 2020*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*Headteacher, ICT Technical staff, Police, LADO*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited/attempted to access)

- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students
  - parents / carers
  - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.
The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individual and groups within Lampard Community School.

Governors:

Governors are responsible for the approval of the Online Safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of online safety Governor. The role of the online safety Governor will include:

- regular meetings with the Online Safety co-ordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / committee / meeting

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety co-ordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Headteacher / Senior Leaders are responsible for ensuring that the online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Group will receive regular monitoring reports from the Online Safety co-ordinator.

Online Safety Lead:

- Leads the online safety working group.
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Co-ordinates training and advice for staff .
- Liaises with the Local Authority / relevant body.
- Liaises with school technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments .
- Meets regularly with Online safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- Attends relevant meeting / committee of Governors .
- Reports regularly to Senior Leadership Team.

Technical Staff:

The ICT Technical staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required online safety technical requirements and any Online safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- that they 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.
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader / Online safety Coordinator for investigation / action / sanction.
- that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff:

- Have an up to date awareness of online safety matters and of the current school Online Safety policy and practices.
- Have read, understood and signed the Staff Acceptable Use Policy Agreement and additional IPad Acceptable Use Agreement where applicable..
- Report any suspected misuse or problem to the Headteacher and Online Safety co-ordinator for investigation / action / sanction.
- All digital communications with students / parents / carers should be on a professional level and only carried out using official school systems .
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Students understand and follow the school online safety policy and the Acceptable Use Policy.
- Carefully supervise all ICT activity in lessons, extra curricular and extended school activities.
- Are aware of online safety issues related to the use of digital technologies, mobile devices, cameras etc and that they monitor and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Students are not allowed unsupervised access to the internet.

Designated Safeguarding Leads:

Should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data .
- access to illegal / inappropriate materials.
- inappropriate on-line contact with adults / strangers.
- potential or actual incidents of grooming.
- cyber-bullying.

Online Safety Focus Group:

Members of the online safety working group will assist the Online Safety co-ordinator with:

- the production / review / monitoring of the school online safety policy / documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Students:

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Are responsible for using the school digital technology systems in accordance with the student Acceptable Use Agreement.
- Where appropriate need to know and understand school policies on the use of mobile phones, digital cameras and hand held devices such as IPads. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school.

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature.

Education - Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of Lampard Community school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Online safety will form part of the 'digital literacy' curriculum that is delivered through Personal Life Skills. Online safety will also be delivered through ICT and other appropriate curriculum areas.
- Online safety should be discussed wherever appropriate when using the internet and as part of lessons
- Staff should deliver online safety messages at the level the student is able to understand
- This will cover both the use of ICT and new technologies in school and outside of school
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities

- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information. This will be delivered at an appropriate level for their understanding.
- Students should be helped to understand the need for the students Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites pre-checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents/carers through:

- Letters and newsletters home.
- Access to a range of materials such as Digital Parenting magazine.
- Website – links to CEOP, advice on keeping safe.
- Parents/Carers evenings and engagement events.
- Online safety workshops.
- Campaigns such as Safer Internet Day.
- Reference to the relevant websites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Staff will have access to regular online safety updates and training. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
- The Online Safety Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / online safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).

- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the ICT Technical staff who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every year.
- The " administrator" passwords for the school ICT system, used by the internal ICT technical staff must also be available to the outsourced ICT support.
- The ICT Technical staff are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / students etc).
- School technical staff regularly monitor and record the activity of users on the school technical systems relating to web browsing and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person. The system for this is to email a ticket to support@lampard.devon.sch.uk to alert the ICT Technical staff.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems can be arranged with for short term access with restrictions.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. This is outlined in the Acceptable Use Policy for Staff and the Data Security Policy.

Mobile Devices

Mobile technology devices may be school owned/provided and include: tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile devices in a school context is educational. The use of mobile devices should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents/carers will be obtained before photographs of students are published on the school website/local press.
- Student's work can only be published with the permission of the student and parents/carers.

General Data Protection Regulations 2018

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.

The school must ensure that:

- It has a Data Protection Policy
- It has paid the appropriate fee to the Information Commissioners Office (ICO)
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.

- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected.
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).
- the device must offer approved virus and malware checking software .
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the Online Safety co-ordinator / ICT Technical staff – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents/carers (eg email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media – Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Lampard Community School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to students, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

Use of Mobile Phones in School

This guidance is given to safeguard staff and students at Lampard.

- Do not use a mobile phone during the working day unless it is a break or lunch time when you are not on duty, and you are not in an area where there are any students.
- Keep your phone away and out of sight at all other times.
- If you need your phone for emergencies or important calls, be discrete and aware. Do not use the phone in places where there are students.
- Do not let students have access to your phone at any time.

Unsuitable / inappropriate activities

Lampard Community school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X	X		
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce				X		

File sharing			X		
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting eg Youtube			X		

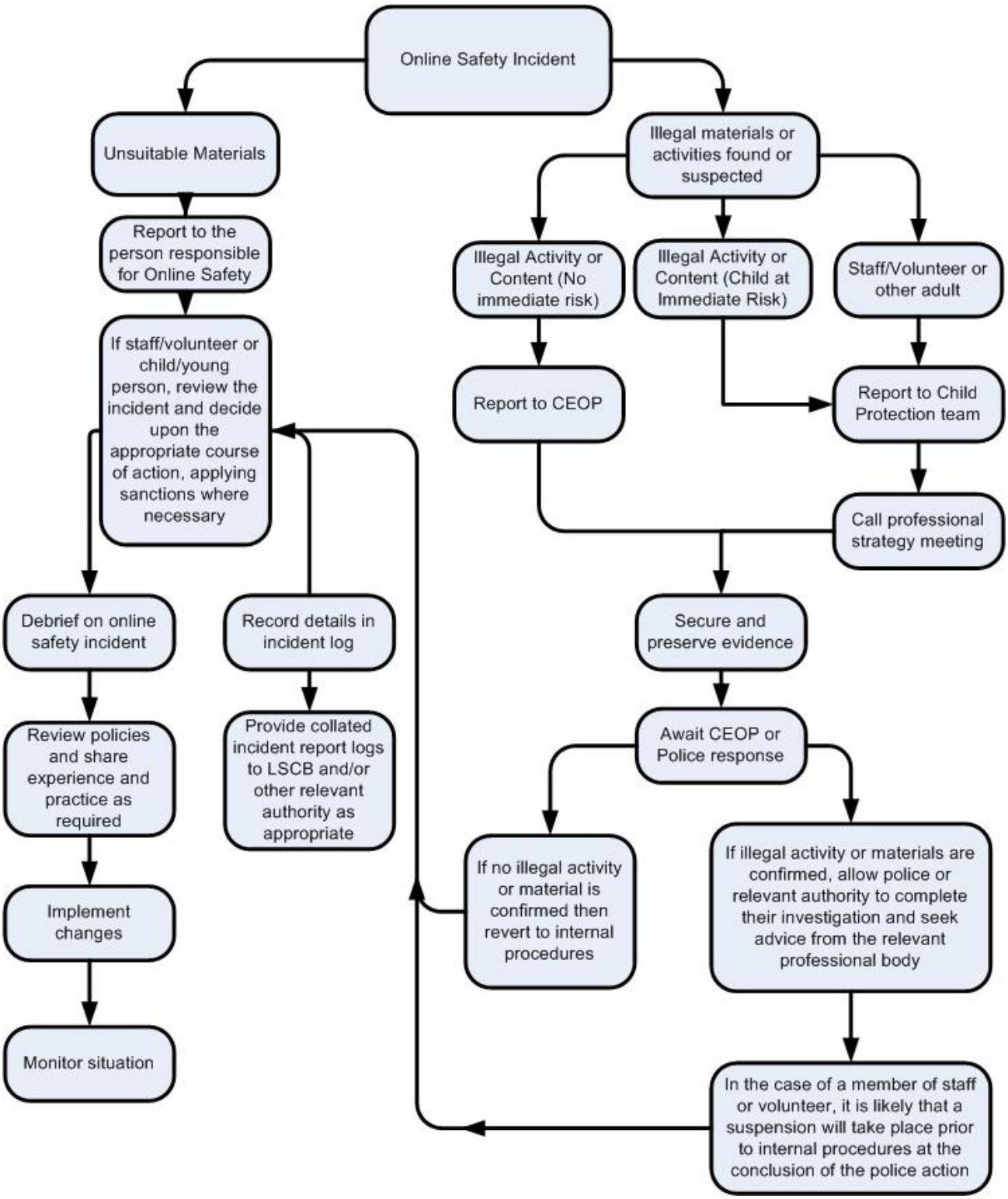
Responding to incidents of misuse

It is hoped that all members of the Lampard School community 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 / volunteer 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.
- 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 or national / local organisation (as relevant).
    - Police involvement and/or action
- **<u>If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately.</u>**
- 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 as best you can. Any change to its state may hinder a later police investigation.

It is important that all of 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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes.



School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students — Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X	X	X			
Unauthorised use of non-educational sites during lessons	X								
Unauthorised use of mobile phone / digital camera / other mobile device	X								
Unauthorised use of social media / messaging apps / personal email	X								
Unauthorised downloading or uploading of files	X								
Allowing others to access school network by sharing username and passwords	X				X				
Attempting to access or accessing the school network, using another student's / pupil's account	X				X				
Attempting to access or accessing the school network, using the account of a member of staff	X				X				
Corrupting or destroying the data of other users	X				X				
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X			X	X		X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X								
Using proxy sites or other means to subvert the school's / academy's filtering system	X				X				
Accidentally accessing offensive or pornographic material and failing to report the incident	X				X				
Deliberately accessing or trying to access offensive or pornographic material	X	X			X				
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X				X				

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X			X
Inappropriate personal use of the internet / social media / personal email		X			X			
Unauthorised downloading or uploading of files					X			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account					X			
Careless use of personal data eg holding or transferring data in an insecure manner		X			X			
Deliberate actions to breach data protection or network security rules		X			X			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students		X	X					
Actions which could compromise the staff member's professional standing		X						X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X						X
Using proxy sites or other means to subvert the school's / academy's filtering system					X			
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X			
Deliberately accessing or trying to access offensive or pornographic material		X	X		X			X
Breaching copyright or licensing regulations					X			
Continued infringements of the above, following previous warnings or sanctions		X			X			

Appendices:

Appendix One: **Acceptable Use Agreement – staff**

Appendix Two: **IPad Acceptable Use Agreement – staff**

Appendix Three: **Acceptable Use Agreement (including IPads) – students**

Appendix Four: **Parent/Carer Agreement**

Appendix Five: **Guidance for staff on Social Media and Mobile Devices**

Appendix One:
Acceptable Use Policy Agreements-Staff

Use of the Internet, E-mail and ICT

Acceptable Use Policy Agreement– Staff

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by

the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff Name:_____

Signed: _____

Date:_____

Appendix Two:
IPad Acceptable Use Policy-Staff

Version 1

You have been provided with an IPad to assist with planning and delivering curriculum areas. This can be used at school and at home.

Data Protection and Security

• All school staff must have their device enrolled into the schools 'Mobile Device Management' system. At no point should a member of staff attempt to remove their device from this system.
• All school devices are managed by an appointed person, Barney Prosser. Do not try to manage your staff device yourself via iTunes or any other management software.
• Do not use your personal Apple ID on this device.
• Do not set up your personal email address on this device.
• Do not link up personal third party apps or services, such as Dropbox or other storage; on demand TV; other media streaming services.
• Do not to sign into your personal social media accounts, e.g., Twitter; Facebook; LinkedIn.
• Staff must set an enhanced password on their iPad device.
• The password for your iPad device must be unique, and must not be recorded. If a password is forgotten, it can be reset through the school's device management system.
• Back up your iPad and it's content on a regular basis. Items deleted from your iPad cannot be recovered.
• You must not jailbreak your device, or otherwise hack, or tamper with it including DFU.

User Responsibility

• Your iPad device must be in a protective case at all times.
• Handle your device with care and respect. Do not throw, damage, place heavy items on, or intentionally drop your device.
• Only approved cleaning materials can be used to clean your device, such as laptop or tablet sprays and cloths.
• Do not keep, or leave your iPad unattended in vehicles. Do not leave your IPad in direct sunlight for extended periods of time. Do not use your IPad in extreme environments such as the bathroom or the beach.
• Keep your iPad safe and secure at all times. You should know where your iPad is at all times.
• Ensure your battery is charged, and ready for school use each and every morning.

Lost, Damaged, or Stolen Devices

• If your device becomes lost or stolen, report it to Barney Prosser or Marcus Nutting as a matter of urgency.
• If your device has become damaged, report it to Barney Prosser or Marcus Nutting and hand over the device to them.
• You must not carry out repairs on any school-owned device.
• You must not solicit any individual or company to repair a school-owned device on your behalf.

Safeguarding and Online Safety

• All device usage is subject to the rules and guidelines of the school's Online Safety policy. Anyone in breach of this policy may be subject, but not limited to disciplinary action, confiscation, removal of content, or referral to external agencies.
• Do not tamper with iPad devices belonging to other members of staff. Anyone found trying to access another staff member's device or associated content will be subject to disciplinary action.

• If an iPad is found, return it immediately to Barney Prosser or Marcus Nutting.
• Do not take photographs of others using your IPad without their express permission.
• As with all other school devices, outlined within our ICT and Safeguarding policies, you are strictly forbidden from using your device to create, store, access, view, download, distribute, send, upload inappropriate content or materials.
• You are forbidden from utilising your iPad to partake in illegal activities of any kind.
• Do not use your iPad to post images, movies, or audio to a public facing part of the internet.
• Your iPad and any content are subject to routine and ad-hoc monitoring by Barney Prosser and Marcus Nutting. You must hand over your device upon request by any member of SLG or ICT team.
• You must ensure compliance with the Online Safety policy when using your iPad.

Personal Use

• Your iPad device is not permitted for personal use. It has been provided for work-related use only. The school maintains ownership of the device.
• Outside of school, on other wifi networks, the device will still be filtered using Smoothwall.
• Do not grant access to anyone, unless expressly authorised to do so by the head teacher.
• Staff are prohibited from taking or storing personal photos/videos on school devices as these may be seen in school by students or other staff.

Staff IPad Acceptable Use Agreement

I have read, understood and agreed to comply with the school's IPad Acceptable Use Agreement.

Signed:_____

Name:_____

Date:_____

Appendix Three:

Acceptable Use Agreement - Student

Use of the Internet, E-mail and IPads

Students are responsible for their use of school computer systems, including iPads, which are provided to support their education. The rules of acceptable use will be explained to students by their tutor in an accessible format.

The following are **not allowed**:

- Damaging iPads, computer equipment or systems.
- Stealing or taking home equipment.
- Accessing systems or areas without permission.
- Deliberately introducing computer viruses onto the school system.
- Accessing web sites which are considered unsuitable or introducing inappropriate material onto school systems.
- Harassing, insulting or attacking others using Internet, Email, Blogs, Mobile Phones, Interactive Gaming or any other electronic system.
- Cyberbullying, sending or displaying offensive or malicious messages or pictures via Internet, Email, Blogs, Mobile Phones, Interactive Gaming or any other electronic system.
- Posting fake or anonymous messages and forwarding junk mail.
- Using offensive language.
- Breaking copyright laws – for example, copying computer software without permission.
- Using somebody else's username and password.
- Intentionally wasting resources – for example, downloading and saving lots of videos or images not related to school work.
- Using school systems to access websites which are not appropriate to view at school.
- Signing in to personal social media accounts.
- Taking photos and videos without permission.
- Using or taking someone else's IPad.
- Taking an IPad, mobile device or camera into a toilet or changing room.
- Taking an IPad out of its case.

The school may examine or delete files held on its computer system and monitor any internet sites visited, emails sent or any other digital content.
IPads will only be used in learning environments, which are supervised by staff.
The IPads are owned by the school.
All iPads must be returned to the class teacher at the end of the lesson.

Students failing to comply may have their access to some or all areas of the system removed.

I agree to comply with the above policy.

Student signature:

_____

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / IPads.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer / IPad.

Appendix Four:
Acceptable Use Agreement - Parents/Carers

Parent/carer Consent Form – Use of the Internet

Name of Child:_____

Class:_____
As the parent/carer of the above student, I give permission for my son/daughter* to use computer systems to access the internet and email. I have read the attached information and understand that the school will endeavour to take all reasonable steps to restrict access to unsuitable material on the internet. I know that I can ask to see the school's Acceptable Use policy and understand that students will be held accountable for their own actions.

Signed ..... Parent/Guardian
Date .....

I do/do not* give my permission for information regarding my son/daughter to be published and made publicly available on or via links from the school website.
Examples of information that may be published include: student's name, tutor group, photographs or videos.

Name of Child:_____

Class:_____

Signed ..... Parent/Guardian
Date .....

*Please delete as appropriate

Use of the Internet – Lampard Community School
The internet has become a major source of information used widely by schools giving educational opportunities across the whole curriculum. During the school week your child will be given access to the internet and email providing them with links to a world of virtual experiences, information and communication.
There are well publicised concerns regarding access to material on the internet that would be considered unsuitable for students. While it is impossible to ensure that a student will not access such material, the school, in liaison with Devon Education Authority, are taking all reasonable steps to minimise the risk of student access by:
Filtering the internet service to prevent access to internet sites that contain unsuitable material e.g. : pornography, violence, abuse or drug information.
All internet access during school hours will be supervised by a member of staff.
"Keep safe" education for all students is provided as part of the Personal and Life Skills and ICT curriculum.
Education of students as to the potential legal consequences of accessing certain types of material.
Real-time monitoring of student email accounts and internet use.
The School has an Acceptable Use Policy. All users of school computer equipment are expected to abide by this policy. Users not abiding by the policy may have their rights to use the system partially or completely withdrawn. A

copy is available from the school office.

The school is also developing its website to include many aspects of school life. The school may publish pictures or work relating to your child. We hold a list of students who cannot be included in any published materials: please indicate on the form overleaf if you would like your child to be added to this list.

Appendix Five:

Social Networking & Use of Mobile Technology

Guidance for Staff

A copy of this document can be found in the staffroom and in the 'safeguarding' folder of the handbook.

We are committed to keeping students and staff safe on line. Since many young people, families and staff connected with our school have an active presence on social networking systems, we believe it is important to support staff in making appropriate decisions regarding their own social media use. It is very important that you follow this guidance.

Do:

- Always think before you post – comments/status updates can be taken out of context.
- Ensure your privacy settings are in place. On Facebook, select a 'friends' setting for every option on your account so you control who can see your content.
- Use strong passwords and log out of any social media systems after using.
- On Twitter, set your account to private by selecting 'protect my tweets'.
- Remove any 'friends' whose access to your content may compromise your position, for example parents with children at Lampard.
- Think carefully before you post on your friends' walls – your posts may be visible to everybody.
- Be mindful of how you present yourself, for example your profile image, the pages you 'like' or the groups you join.
- Ensure that your geolocation services are only visible to your friends. You can disable the 'checking in' function in your privacy settings.
- Consider removing previous online content that might compromise your professional reputation.
- Untag yourself from possibly compromising photos.
- Google yourself – searching your name regularly on public search engines can be a useful way to monitor your online content or digital identity.
- Tell the school if you feel you are a victim of cyberbullying by colleagues, students or families of students.
- Tell the Safeguarding team at Lampard if you become aware of any inappropriate use of social network sites by Lampard students (including being under age).

We strongly recommend:

- Do not accept friend requests from Lampard students, recent ex-students or their parents. On most services, the sender of the request will not be notified if you select ignore/delete.
- Not to put your home address on your profile.
- Do not post derogatory comments about students, parents, colleagues or the school.
- Do not post pictures of yourself or colleagues taken whilst at work. This gives a bad impression of our professionalism.
- Not to post photos containing images of Lampard students or their families.
- Don't have discussions about your job on an online environment – comments can easily be taken out of context.

Use of Mobile Technology in School

This guidance is given to safeguard staff and students at Lampard.

- Do not use a mobile phone during the working day unless it is a break or lunch time when you are not on duty, and you are not in an area where there are any students.
- Keep your phone away and out of sight at all other times.

- Do not use your camera function on your personal devices to take photos of students.
- If you need your phone for emergencies or important calls, be discrete and aware. Do not use the phone in places where there are students.
- Do not let students have access to your phone at any time.

Please be aware that inappropriate use of social media systems and mobile technology can be serious and may be dealt with through school disciplinary procedures.

This guidance is to be read in conjunction with the Online Safety policy, Acceptable Use Agreement and Safeguarding Policy.

Signed:_____

Print Name:_____

Date:_____