Online Safety Policy

Lampard Community School

Approved by:	Governing Body	**Date:** November 2020
Last reviewed on:	November 2020	
Next review due by:	November 2021	

Contents

---

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The Governing Body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead/Deputy DSL's

Details of the school's DSL and deputy DSL's are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT technical staff and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT Technical staff

The ICT technical staff are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a frequent basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that students follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents and Carers

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood, and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating students about online safety

Students will be taught about online safety as part of their curriculum.

Our students will be taught and supported to:

- *Use technology safely, responsibly and respectfully, keeping personal information private*
- *Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies*
- *Recognise acceptable and unacceptable behaviour*
- *Identify a range of ways to report concerns about content and contact*
- *Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy*
- *Recognise inappropriate content, contact and conduct, and know how to report concerns*
- *To understand how changes in technology affect safety, including new ways to protect their online privacy and identity*
- *How to report a range of concerns*

In addition to the above:

- Online safety will be discussed wherever appropriate when using the internet and as part of lessons
- Staff will deliver online safety messages at the level the student is able to understand
- Key online safety messages will 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 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.

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

The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents and carers about online safety

The school will raise parents' awareness of online safety in letters or other communications home such as the 'Digital Parenting magazine' and NSPCC resources such as 'Share Aware'. There is useful online safety advice and links to relevant organisations in our Online Safety pages on our school website. These are regularly updated. This policy will also be shared with parents.

Online safety information will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

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

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

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

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

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

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

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

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

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

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

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2).

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Students using mobile devices in school

Students may bring mobile devices into school but are not permitted to use them during the school day. Students will hand their devices to the office for safe keeping.

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour Support, Anti-bullying, Acceptable Use agreements and Safeguarding and Child Protection policies. Action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff Code of Conduct/Acceptable Behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and Deputy DSL's will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour Support policy
- Anti-bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1:

Student Acceptable Use Agreement

Use of the Internet, E-mail and iPad

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.
iPad will only be used in learning environments, which are supervised by staff.
The iPad 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 / iPad.
- 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 2:

Staff Acceptable Use Agreement

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 3:

Staff Social Media & 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 online. 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 and protecting their online presence.

It is very important that you follow this guidance.

- Always think before you post – comments/status updates can be easily taken out of context.
- Ensure your privacy settings are robust - use strong passwords and log out of any social media systems after using.
- Remove any friends whose access to your content may compromise your position or limit their access to what they see from your account, for example friends who are also parents with children at Lampard.
- Think carefully before you post on your friends' accounts– your posts may be visible to everybody.
- Be mindful of how you present yourself, for example your profile image, the pages you 'like', the posts you share 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 on social media accounts.
- 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.
- If offensive or hurtful information is posted about you online, for instance, by a student or parent, never retaliate to the message. Make copies of the offensive comment, including screenshots and URLs and take them to your employer.
- If offensive material has been posted about you online, you can use the reporting procedures of the site involved to get the material removed. The UK Safer Internet Centre can help professionals with this and has a helpline dedicated to providing advice for professionals: 0844 381 4772 or helpline@saferinternet.org.uk
- 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).

Please 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.
- Put your home address on your profile.
- Post derogatory comments about students, parents, colleagues or the school.
- Post pictures of yourself or colleagues taken whilst at work. Consider yours and others professionalism.
- Post photos containing images of Lampard students or their families.
- Have discussions about your job on an online public environment – comments can easily be taken out of context.
- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances from your workplace
- No reference should be made in social media to students/pupils or parents/carers

Key points to remember:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private

- Regularly review your connections – keep them to those you want to be connected to
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

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 personal mobile devices 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:_____

Appendix 4:

Online safety and remote education in school – COVID 19

Lampard Community School will continue to provide a safe environment, including online. This includes the use of an online filtering system. Where students are using computers in school, appropriate supervision will be in place. We have a small number of notebooks that can be loaned to students who would not have access to technology for their learning. We have tracking systems, school loan of equipment agreements and quarantine/cleaning systems in place for these items.

Children and online safety away from school and college
It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk or suffering abuse. Any such concerns should be dealt with as per the Safeguarding and Child Protection Policy. Referrals should still be made to MASH/social worker and as required, to the police. Online learning should follow the same principles as set out in the code of conduct.

Lampard Community School will ensure any use of **online learning tools** such as MyMaths, Lexia Power Up, Lexia Core 5, Discovery Education, Skills Forward and systems are in line with privacy and data protection/GDPR requirements.

Lampard Community School is committed to ensuring the safety of staff and students during periods of remote education. Weekly contact with parents and carers during this time can be used to reinforce the importance of children staying safe when accessing any online content. Staff delivering remote education should be aware that the same principles set out in the school's Staff Behaviour Policy will apply. This incorporates telephone and email contact as well as passive and interactive online learning activities.

Communicating with parents, carers and students including by email

Where education is having to take place remotely due to coronavirus (COVID-19), it's important for our staff and students to maintain professional practice as much as possible. When communicating via email and /or telephone with parents and students, staff should follow these guidelines:

- communicate within school hours as much as possible (or hours agreed with the school to suit the needs of staff)
- communicate through the school channels approved by the senior leadership team
- use school email accounts (not personal ones)
- use school devices over personal devices wherever possible
- do not share personal information.

Virtual lessons

Our current offer is the printed Home Learning Packs. In the future, if we decide to provide elements of remote education using pre-recorded videos, we will seek guidance from the National Cyber Security Centre (NCSC) on using video conferencing platforms safely. We will also follow guidance from the UK Safer Internet Centre on safe remote learning.

Additional Pastoral Care

In addition to the weekly calls made to each family, there may be exceptional individual circumstances where an online pastoral care session is provided for a student. Such calls would always follow the school's guidelines on safer working practices. This must be discussed and approved by the senior leadership team to assess any risks before taking place.

Below are some things to consider when delivering virtual sessions, especially where webcams are involved:

- No 1:1s, groups only, unless as a result of risk assessments confirmed with the Headteacher. This may for example involve having the parent in the room.
- Staff and children must wear suitable clothing, as should anyone else in the household.

- Any computers used should be in appropriate communal areas, for example, not in bedrooms.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms agreed by school leaders
- Staff should record the length, time, date and attendance of any sessions held.

Personal Data and GDPR

Lampard Community School will continue to follow the guidance outlined in the data protection: toolkit for schools when managing personal data and will consider:

- taking care not to share contact details when emailing multiple people
- being careful when sharing usernames and other personal data for access to online resources
- providing access to school data systems safely.

Online safety at home

School will continue to support parents, sharing online safety information, websites and resources for them to utilise on the school website and in school communications and updates. E.g. links to CEOPs, ThinkUKnow.

Appendix 5: online safety incident report log

Date	Issue	Action	Resolution/outcome