Lammack Community Primary School
ICT Online Safety Policy

Using new learning technologies effectively and safely

This policy deals specifically with the educational and curriculum element of online safety. Guidance and procedure relating to infrastructure, networking and appropriate use of technology by staff are contained in the ICT security policy. Our online safety Policy has been written by the school, building on the Blackburn with Darwen policy guidance. It has been agreed by the senior leadership team and approved by Governors.

Writing and reviewing the online safety policy

The online safety Policy relates to other policies including those for ICT, ICT security, anti-bullying and for child protection.

- The Computing Curriculum Leader is the online safety lead
- The SENCO is the child protection co-ordinator.

Scope of the Policy

This policy applies to all members of the Lammack community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.
The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils 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 online-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.

Why the Internet and communication technology use is important

'Technology offers unimaginable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile, and pupils are using technology at an ever earlier age…' Ofsted 2013.

The safe use of technology is a part of the statutory curriculum and the internet a necessary tool for staff and pupils.

Ofsted guidance for schools 2013 recommends that all schools:

- provide an age-related, comprehensive curriculum for online safety that enables pupils to become safe and responsible users of new technologies

- audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies
- work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school
- use pupils' and families' views more often to develop online safety strategies.

The DfE Keeping Children Safe in Education statutory guidance requires Local Authorities, Multi Academy Trusts, and schools in England to ensure learners are safe from harm:

> *"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to* ***online safety*** *empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate"*
>
> *"Governing bodies and proprietors should ensure* ***online safety*** *is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how* ***online safety*** *is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement"*

The DfE Keeping Children Safe in Education guidance also recommends:

> ***Reviewing online safety*** *… Technology, and risks and harms related to it, evolve, and change rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. A free online safety self-review tool for schools can be found via the* 360 safe self-review tool.

The DfE Keeping Children Safe in Education guidance suggests that:

> *The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:*
>
> ***content:*** *being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.*
>
> ***contact:*** *being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.*

conduct: *online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and*

commerce: *risks such as online gambling, inappropriate advertising, phishing and or financial scams.*

School and community involvement in online safety policy and practice

At Lammack Primary School we believe that by involving representatives from all the school community in evaluating, formulating and reviewing online safety policy and practice, our children and staff will be the safest they possibly can be.

Involving children in policy, practice and educating others
The school has a pupil online safety group, 'Digital Leaders'. Part of their role will be to contribute to online safety policy and practice and inform parents and peers of online safety issues on a regular basis. This is being developed by the school.

Roles and Responsibilities
The following section outlines the online safety roles and responsibilities of individuals and groups within the 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:

- meetings and correspondents with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meetings

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 Lead*.
- 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.
- *The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Lead 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 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.*

Online Safety Lead

- leads the Online Safety 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.
- provides training and advice for staff
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- meets with the Online Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- reports to Senior Leadership Team

Technical staff

The 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 *Local Authority / other relevant body* 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
- *the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*
- 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 / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher; Online Safety Lead* for investigation / action / sanction
- *that monitoring software / systems are implemented and updated as agreed in school policies*

Governors

The DfE guidance "Keeping Children Safe in Education" states:

> "Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".
This review will be carried out by the lead online safety governor who themselves and other members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- **regular meetings with the Designated Safeguarding Lead / Online Safety Lead**
- **regularly receiving (collated and anonymised) reports of online safety incidents**
- **checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)**
- **Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.** (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- **reporting to relevant *governors group/meeting***
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- *membership of the school Online Safety Group*

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safeguarding Lead:
Keeping Children Safe in Education states that:

"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."
They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"
*They (the DSL) "*can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

While the responsibility for online safety is held by the DSL and cannot be delegated, the school may choose to appoint an Online Safety Lead or other relevant persons to work in support of the DSL in carrying out these responsibilities. It is recommended that the school reviews the sections below for the DSL and OSL and allocate roles depending on the structure it has chosen

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
- online-bullying
- monitoring improvement actions identified through use of the 360 degree safe self-review tool.

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Students / Pupils:

- are responsible for using the *school* digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's* Online Safety Policy covers their actions out of school, if related to their membership of the 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.* Parents and carers will be encouraged to support the *school* in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student / pupil records

Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme.
This will be provided through:

- HRE programmes
- A mapped cross-curricular programme
- assemblies
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to The Headteacher for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are 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
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are 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*
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies

- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

IT Provider

The DfE Filtering and Monitoring Standards says:

"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."

"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."

"The IT service provider should have technical responsibility for:

- *maintaining filtering and monitoring systems*
- *providing filtering and monitoring reports*
- *completing actions following concerns or checks to systems"*

"The IT service provider should work with the senior leadership team and DSL to:

- *procure systems*
- *identify risk*
- *carry out reviews*
- *carry out checks"*

"We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within the school, college, or trust. However, it must be clear who is responsible, and it must be possible to make prompt changes to your provision."

Online safety Education and Training

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Current guidance stipulates that it is not sufficient to keep pupils safe in school. It is our responsibility

therefore, to ensure they have opportunities to learn how to stay safe and deal with the risks associated with the internet and communication technology in the world around them. Keeping our children safe involves educating all members of our school's community, including governors, parents and all staff working in school.

Educating pupils

Our online safety curriculum
At Lammack Primary School we ensure that children have access to a progressive online safety curriculum across all year groups.

Early Years Foundation Stage, Early Learning Goal

> Children recognise that a range of technology is used in places such as homes and schools. They select and use technology for particular purposes.

In order to safely select and use technology we believe that children in the Foundation Stage need to be taught an age appropriate online safety curriculum. When working towards this Early Learning Goal we will ensure our children use technology safely so that by the time they leave the Foundation Stage they are ready to access the key stage 1 curriculum

The National Curriculum 2014 for Computing stipulates that pupils:

- In key stage 1 are taught to use technology safely 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.
- In key stage 2 are taught to use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

To ensure pupils have access to an age-appropriate online safety curriculum that is flexible, relevant and engages pupils' interest; that is used to promote online safety through teaching pupils how to stay safe, how to protect themselves from harm, we:

- Introduce age appropriate school and classroom rules each year and reinforce them regularly
- Use progressive statements within the Computing curriculum scheme of work, to ensure that areas of online safety relating to communication, information, creating and presenting ideas, and Computer Science are covered regularly. These are planned into either computing, PSHE or the general curriculum as appropriate. The Computing scheme can be found on the curriculum in the subject area in staff shared. This scheme also defines the knowledge pupils should have acquired pre key stage 1
- Deliver online safety messages in assembly in response to need, to reinforce national initiatives and agendas such as Safer Internet Day and anti-bullying week.
- Before using a new device or online resource, pupils are taught how to use it safely and appropriately. This is reinforced regularly.
- Teach pupils to tell a trusted adult should they be worried of upset by anything they encounter online or using communication technology. (All staff are made aware of what to do should a pupil confides in them.)

The need to keep login details and other personal information private will be reinforced regularly when using the schools network, learning platform and any other methods of communication agreed by the headteacher.

Pupils will be taught how to evaluate Internet content appropriate to their age.

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what Internet use is responsible and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation appropriate to their age group.
- Pupils will be taught about the dangers of radicalisation and extremism at an appropriate level for their age.

Educating parents

Children often seem more at home in the digital world than their parents. To ensure that children are the safest they possibly can be, we must educate parents about the risk of using the internet and communication technology for their children and the potential for their own use of technology to place themselves or their child at risk.

We ensure parents receive information and training by:

- Providing links to information and resources for parents on our school website/Facebook page
- Providing regular updates to parents through newsletters
- Inviting parents to safety workshops
- Providing online safety information during events such as parents evenings
- Encouraging parents to act as role models when using technology

The school will share with parents and children, our belief that:

- The unsupervised use of social network spaces intended for adults outside school is inappropriate for pupils of primary age.
- PEGI and BBFC ratings are good indicators of how appropriate the levels of violence, sexual content, bad language and the portrayal of drug taking and criminal acts are.
- Family friendly filtering can help to keep children safe, however education and the opportunity to develop safe practice is essential for keeping children safe
- Pupils who use the internet and other communication technology may be at risk of being groomed or radicalised. It is important that parents understand that secrecy is a possible factor in both of these.
- What pupils do online now, can affect their future life.

- If a child is happy to tell a parent or carer when they are worried, they are the safest they can possibly be; therefore we encourage parents to nurture a sense of trust between them and their child when talking about using technology.

There are some excellent online tools for reporting concerns, such as the Report Abuse button which can be found on the https://www.thinkuknow.co.uk/ site and Childline http://www.childline.org.uk .

Children are also encouraged to report their concerns via a member of staff or trusted adult.

Educating staff and the wider school community

- We ensure that all new staff receive online safety training as part of their induction
- All school staff have access to basic online safety training regularly
- The online safety lead have access to a higher level of training, updates and information to ensure that they have the skills and knowledge necessary to lead all areas of online safety.

Basic training includes

- Online safety issues for pupils
- Reporting procedures
- Guidance on appropriate use of communication technology by staff and pupils
- Guidance for staff on how to stay safe
- Expectations in terms of passwords and data security
- Expectations in terms of professional conduct including the use of social media
- Teaching pupils to minimise the screen if they see something that makes them feel uncomfortable.

Online safety training references and complements guidance in the Safer Working Practices document.

Keeping staff and pupils safe in school

All access to the internet is filtered by Straight Talk. For further details on networking and filtering and how access to inappropriate sites can be monitored refer to the ICT Security Policy.
The school will work with the LA, and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the online safety Lead who will inform the LA where appropriate so that they can take appropriate action.

All users will be taught how to care for devices in terms of health and safety. This includes avoiding placing food or liquids near to electrical devices, carrying equipment and rules around charging and electrical sockets.

The school internet access is designed expressly for pupil use and includes appropriate filtering.

Sanctions for inappropriate use of the internet and communication technology follow sanctions set down in the behaviour policy. A record of any misuse kept by the Computing Leader.

At Lammack Primary School staff do not use their own personal devices/accounts to contact parents and pupils. To protect staff and pupils, the school provides a mobile phone for contacting parents when on trips and visits and school email addresses. Cameras are provided for recording school related activities. Images of children should not be stored on personal devices.

Acceptable use agreements

A home school agreement concerning access to the internet and communication technology will be signed by pupils and parents When they join Lammack Primary School and kept on record by the office staff.

- Class rules agreement
- Acceptable use agreement for school staff (see the ICT Security Policy)

Passwords security

Pupils are encouraged to keep their password private. Parents are encouraged to ask children to logon to their accounts and show them what they have been doing rather than ask children to share their passwords.

- Pupils will be taught to tell an adult immediately about any offensive communications they receive or any inappropriate content they may encounter using digital technology.
- Children will be taught to click on Hector should they encounter anything that makes them feel uncomfortable.
- Pupils may only use approved digital methods of communication on the school system. E.g. communication tools in the Learning platform.
- Pupils and staff will use equipment responsibly.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location or arrange to meet anyone without specific permission.

Reporting online safety concerns

Children are encouraged to report their concerns via a member of staff. We also encourage the children to use national resources such as childline and CEOP.

Detail below systems for reporting online safety concerns. This should build on any systems for behaviour and safeguarding already in school. It should include:

- *A record of online safety incidents is kept in the Online safety record in the Computing Leader's File.*
- *The nature of the incident and action taken are recorded with and any consequences e.g. additional online safety input; discussion with parents restricting access etc.. This includes access to inappropriate resources (intentional or otherwise), inappropriate use of school technology, online safety and cyberbullying disclosures.*

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

> *"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:*
>
> - *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"*

Published content - This will also be referenced in the in the ICT Security Policy

Any information that can be accessed outside the school's intranet should be classed as published whether in electronic or paper format.

- Electronic communication sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- General contact details should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. (This may be through education and guidance, as directly reading everything is impractical)
- Where pupils publish work, there will be systems in place to check the content and pupils will be given clear guidelines about what can be published.

Publishing pupil's images and work

- Staff and pupils using digital cameras, video recorders, iPads or sound recorders will ensure that they inform others before recording them and always use equipment in a respectful manner. (In the Foundation Stage this may not be practical when capturing a child in the process of learning, however should be modelled as often as possible.)
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere, particularly in association with photographs. (some schools may wish to use first names, where there is no photograph, but staff should be aware of the risks associated with this and take appropriate precautions)
- Written permission from parents or carers will be obtained before photographs or video of pupils are published.
- Where pupil's work is published the school will ensure that the child's identity is protected.
- Where school events are being publicised, care will be taken not to reveal information that may put children or staff at risk e.g. the date and location of a trip

Parents using still or video cameras at school

- In line with the Information Commissioner's Office, the school allows parents to record video and images during performances for person use only. We advise parents of this before each event.

Guidance for taking photographs and video during school performances and assemblies.

Information Commissioner's Office
http://www.ico.org.uk/for_organisations/sector_guides/~/media/documents/library/Data_Protection/Practical_application/TAKING_PHOTOS_V3.ashx

Managing emerging technologies

- The educational benefit of emerging technologies and any potential risks will be considered and shared with staff before they are used in school.

Protecting personal data

See the ICT Security Policy for guidance

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Responsible ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

- Parents will be asked to sign and return a consent form for their children to access the internet.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Blackburn with Darwen LA can accept liability for the material accessed, or any consequences of Internet access. Any inappropriate access whether intentional or unintentional will be reported to the e safety co-ordinator and to the LA where necessary.
- The school will audit ICT provision to establish if the online safety policy is adequate and that its implementation is effective.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by the Headteacher and where appropriate inform the LA.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure on request.

For further information, please see the ICT Security Policy

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how a school protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities 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.

The 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 / pupils, 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* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- *A process for approval by senior leaders*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *A code of behaviour for users of the accounts, including*
- *Systems for reporting and dealing with abuse and misuse*
- *Understanding of how incidents may be dealt with under school disciplinary procedures*

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
- *The school permits reasonable and appropriate access to private social media sites*

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

Communications Policy

Introducing the online safety policy to pupils

- Online safety rules will be posted in all rooms where pupils may access the internet and discussed with the pupils at the start of each year. Where possible images and symbols will be used to help make them accessible to young children.
- Pupils will be informed that network and Internet use will be monitored and can be monitored and traced to the individual device or login.

Introducing the policy to parents

Parents' attention will be drawn to the School online safety Policy and practice:

- in newsletters,
- in the school brochure
- on the school website

Staff and the online safety policy

- All staff will be given the School online safety Policy and its importance explained.
- Staff should be aware that internet traffic may be monitored and traced to the individual device or login. Discretion and professional conduct is essential.
- The school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.

Technology

The DfE Filtering and Monitoring Standards states that "Your IT service provider may be a staff technician or an external service provider". If the school has an external technology provider, it is the responsibility of the school to ensure that the provider carries out all the online safety and security measures that would otherwise be the responsibility of the school. It is also important that the technology provider is fully aware of the school Online Safety Policy/acceptable use agreements and the school has a Data Processing Agreement in place with them. The school should also check their local authority/other relevant body policies on these technical and data protection issues if the service is not provided by the authority and will need to ensure that they have completed a Data Protection Impact Assessment (DPIA) for this contract.

The school is 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. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection. (Schools will have very different technical infrastructures and differing views as to how these technical issues will be handled – it is therefore essential that this section is fully discussed by a wide range of staff – technical, educational, and administrative staff before these statements are agreed and added to the policy). A more detailed technical security policy template can be found in the Appendix.

Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states: "It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…

The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility

the filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

· checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced e.g. using SWGfL Test Filtering

Filtering

- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix for more details).
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- the school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle
- the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.

- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

Please see the ICT Security Policy for further information

Annual Safety Audit

This quick self-audit will help the senior management team (SMT) assess whether the online safety basics are in place to support a range of activities that might include those detailed within Appendix 1.

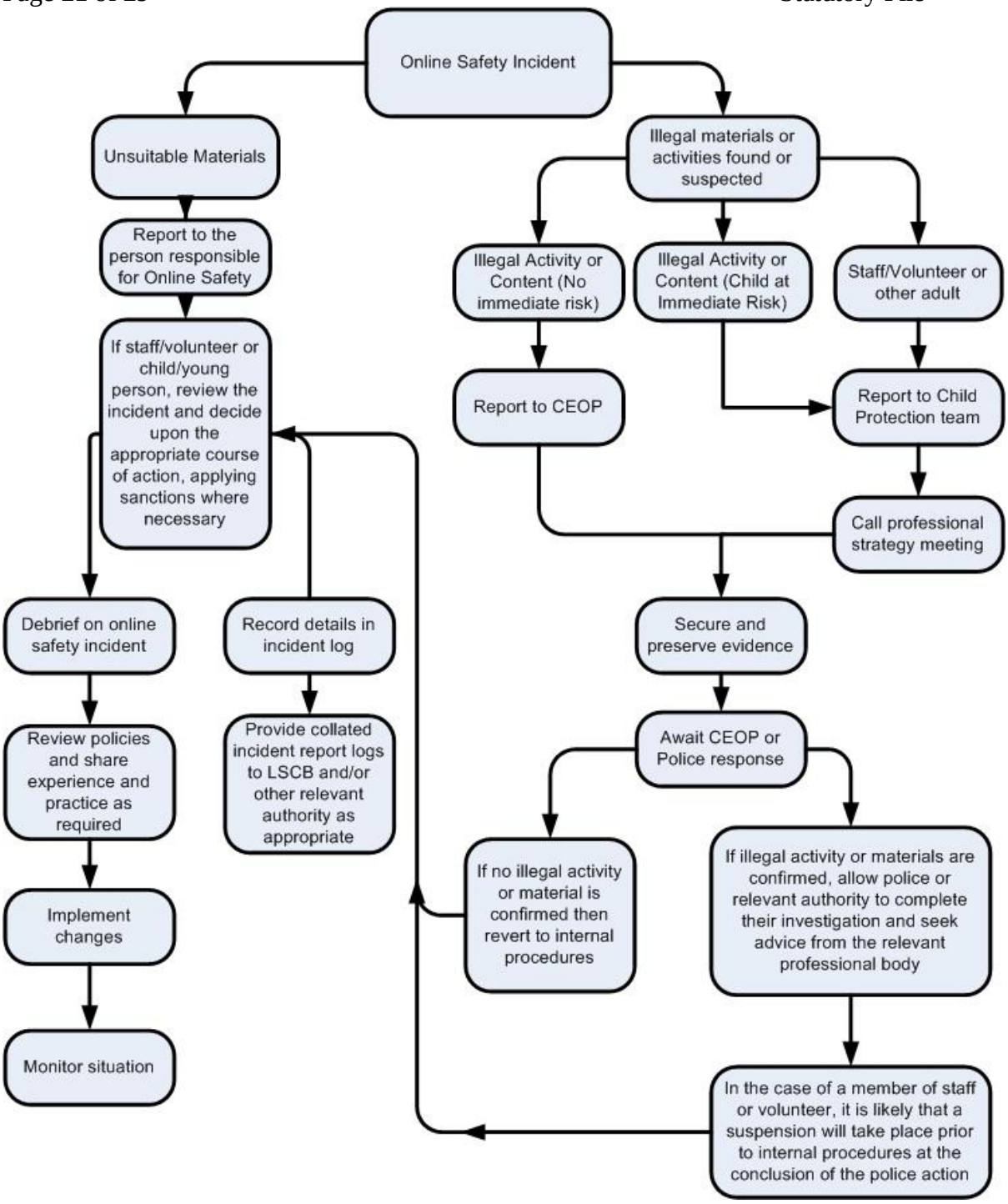
Does the school have an online safety policy and ICT Security Policy and reflects current practice?	
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The Designated Child Protection Coordinator is:	
The online safety Coordinator is:	
Has annual online safety training been provided for all school staff?	
Have all governors received online safety training?	
Is there a named online safety governor?	
Do all staff sign an ICT Code of Conduct on appointment?	

Do parents sign and return an agreement that their child will comply with the School online safety Rules?	
Have school online safety Rules been set for students?	
Are these Rules displayed in all rooms with computers?	
Is the online safety curriculum flexible, relevant and does it engage pupils' interest?	
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access	
Has an ICT security audit been initiated by SMT, possibly using external expertise?	
Is personal data collected, stored and used according to the principles of the Data Protection Act?	
Does the schools' ICT Security policy compliment the online safety policy	

A more comprehensive checklist is available through the E learning Support Service. A more comprehensive review tool is available at http://www.360safe.org.uk/

Responding to incidents of misuse – flow chart

Lammack Community Primary School
ICT Online Safety Policy



Lammack Community Primary School
ICT Online Safety Policy

Reporting Log
Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Lammack Community Primary School
ICT Online Safety Policy

Online Safety Governance Checklist
This guidance links to 'Making Sense of…Keeping Children Safe in Education 2020'

	Online Safety Governor Checklist Action	
	It is the responsibility of the Governor responsible for Online Safeguarding to ensure that **this document is tabled at least annually** at the termly meeting of the full Governing Body **or at the first meeting following any major incident**.	
1 ☐ revised	The School/College's Online Safety Policy is in place and has been reviewed and updated in the last 12 months. Links to related policies are embedded (e.g. Child Protection Policy references Sexting, Peer-on-Peer abuse, GDPR requirements). Comments/Evidence:	Date:
2 ☐	The pupil/student Acceptable Use/Behaviour Policy is in place and has been revised to accommodate developments in technology and online behaviour. Comments/Evidence:	Date:
3 ☐	All staff (teaching/non-teaching/supply/volunteers) are familiar with the Code of Conduct (which includes the use of Social Media and staff/pupil relationships) and have signed the Staff AUP. Comments/Evidence:	Date:

Lammack Community Primary School
ICT Online Safety Policy

	Online Safety Governor Checklist Action	
4 ☐ revised	All new staff understand their responsibilities regarding Online Safety and have received Online Safety training as part of the induction process. Comments/Evidence:	Date:
5 ☐	The School/College has effective and robust reporting mechanisms in place for Online Safety concerns. All Pupils/Students understand their Online Safety Rights & Responsibilities and clearly understand how to appropriately report concerns. Comments/Evidence:	Date:
6 ☐	All staff (teaching and non-teaching), volunteers and supply staff clearly understand what to do if an incident occurs or is reported. Comments/Evidence:	Date:
7 ☐ revised	The School/College regularly engages with parents/carers about Online Safety. They are aware of the School/College's Acceptable Use/Behaviour Policy and have received/returned a copy of the internet access permission form to School/College. Comments/Evidence:	Date:

	Online Safety Governor Checklist Action	
8 ☐	The School/College regularly reviews its Online Safety provision to ensure currency and effectiveness. Comments/Evidence: Date:	
9 ☐	ALL users are aware of and understand the use of filtering and monitoring systems in place in the school/college (including software/hardware-based tools where appropriate). Comments/Evidence: Date:	
10 ☐	The School/College regularly uses the *SWGfL Filter-Check utility* to check and evidence that the chosen filtering system is compliant with the filtering requirements highlighted within the DfE's Keeping Children Safe in Education. Comments/Evidence: Date:	
11 ☐	The School/College has an Online Safety Group which utilises the expertise of staff to contribute to and shape Online Safety arrangements. Comments/Evidence: Date:	
12 ☐ revised	Pupils/students are educated about Online Safety as part of a broad, balanced and progressive curriculum and their views and concerns are reflected in curriculum planning. Comments/Evidence: Date:	

Lammack Community Primary School
ICT Online Safety Policy

	Online Safety Governor Checklist Action	
13 ☐ revised	The School/College has a Designated Safeguarding Lead with an appropriate Job Description who is responsible for, and has robust knowledge of, Online Safety. Comments/Evidence:	Date:
14 ☐	A programme of training for all staff is in place and staff receive regular updates on current and emerging risks. Staff with a specific responsibility for Online Safety (e.g. DSL) have received appropriate training in the last 12 months. Comments/Evidence:	Date:

	Online Safety Governor Checklist Governing Body-specific Actions	
15 ☐	An Online Safety Governor has been agreed and is part of the School/College's Online Safety Group. Comments/Evidence:	Date:

	Online Safety Governor Checklist Governing Body-specific Actions	
16 ☐	Governors are involved in the development of and approve the Online Safety Policy, providing support and critical challenge to the school/college around Online Safety policy and practice. Comments/Evidence:	Date:
17 ☐	All Governors understand what provision the school/college makes to keep pupils/students safe online and assess its effectiveness. Comments/Evidence:	Date:
18 ☐	All Governors have received recent Online Safety education and this is reflected in how the school/college develops its policy and practice. Comments/Evidence:	Date:
19 ☐	Governors have ensured appropriate filtering and monitoring systems are in place, are involved in decisions regarding their procurement and understand what systems are used. Comments/Evidence:	Date:

	Online Safety Governor Checklist Governing Body-specific Actions	
20 revised ☐	All Governors understand the statutory requirements of Keeping Children Safe in Education 2020 and the expectations of Governing Bodies and Proprietors. Comments/Evidence:	Date:

Lammack Community Primary School
ICT Online Safety Policy