Lime Tree Primary Academy
e-Safety Policy

Created on: 22nd July 2015
Updated 30th January 2020
e-Safety Officers: Natasha Benton, Debbie Rea

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents, FoLT (PTA).

Safeguarding is a serious matter; at Lime Tree Primary Academy we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Lime Tree Academy School website and school blog; upon review all members of staff will sign as read and understood both the e-Safety Policy and the Staff Acceptable Use Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Head of School: Clare Larkin Date: 30th January 2020

Chair of Governors: Daniel Jagger Date: 30th January 2020

The practical application of this policy will be reviewed every 24 months or when the need arises by the coordinator, the Head of School and the nominated governor.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of e-Safety at the school who will.

    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Head Teacher in regards to training, identified risks and any incidents.
    - Chair the e-Safety Committee

Our appointed governor is: Daniel Jagger

Head of School

Reporting to the governing body, the Head of School has overall responsibility for e-Safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer and our e-Safety team (made up of pupils, parents and governors)

The Head of School will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

e-Safety Officer

The day-to-day duty of e-Safety Officer is devolved to *Debbie Rea (Child Protection Officer) and Natasha Benton (Computing Coordinator)*
The e-Safety Officers will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Head of School.
- Advise the Head of School, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.

- Make him/herself aware of any reporting function with technical e-Safety measures, i.e. internet filtering reporting function; liaise with the Head of School and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff
Jamie Bates, ESI Tech
Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Head of School.
    - Passwords are applied correctly to all users regardless of age. Passwords for children will be a three or four letter word (based on a tree) with a number. These are changed if there is a compromise.
    - The IT System Administrator password is to be changed in the case of a breach.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Head of School.
- Any e-Safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made via CPOMS), or in his/her absence to the Head of School. If you are unsure, the matter is to be raised with the e-Safety Officer or the Head of School to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

e-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, school newsletters, school blog and regular updates with parents regarding any incidents, parents will be taught strategies to ensure that students are empowered.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

e-Safety Committee

Chaired by the Governor responsible for e-Safety, the e-Safety Committee is responsible:

- to advise on changes to the e-safety policy.
- to establish the effectiveness (or not) of e-safety training and awareness in the school.
- to recommend further initiatives for e-safety training and awareness at the school.

Established from volunteer students, parents, e-Safety Officer, responsible Governor and others as required, the e-Safety Committee will meet on a termly basis.

Technology – protecting children online from inappropriate content

Lime Tree Primary Academy uses a range of devices including PC's, laptops, Apple Macs and iPads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – We use a Netsweeper firewall appliance, this is cloud based and is managed by ESI Tech and overseen by the school. This prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Computing Lead, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head of School.

Internet Monitoring – Netsweeper flags up any inappropriate searches to our Head of School and e-Safety coordinator via email notification. In order to access the internet, all children and staff have a unique login. The exception to this is in EYFS and KS1 where children use a generic log in for their year group and are observed using equipment by an adult. This allows for the Head of School to see what has been searched online and by whom.

The Head of School and e-Safety officer will look at the content and what was searched prior to it. Appropriate action will be taken to determine the context of this search. The schools Child Protection Policy will be followed if need be at this point. We also conduct a monthly test on or around 15th of each month where we test our Netsweeper effectiveness as well as looking at reports on Netsweeper.

Email Filtering – we use Google Apps which removes known spam / virus emails from the users mailbox. It prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that leave site do not hold personal data, staff store this data in the cloud using the school's Google Apps, the documents on here have passwords that only relevant staff are made aware of. No data is to leave the school on an un-encrypted device. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Head of School immediately. The Head of School will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's. All staff iPads are password protected.

Passwords – All staff and students will be unable to access any computer and iPad without a unique username and password. Staff and student passwords will change if there has been a

compromise. The Computing Coordinator and IT Support will be responsible for ensuring that passwords are changed. When using Safari, children will need to log in using their own personal log in. An exception to this is EYFS, Year 1 and Year 2 who will have adult supervision whilst using the internet. They will log in with a first name but with no password. Staff using their 'Teacher Macbook' are responsible for changing their own passwords and their internet usage is monitored when onsite. Staff use at home is outlined in the Staff AUP.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Head of School if there are any concerns. All USB peripherals such as keydrives are not used in school, If ever there is a need to use it must be scanned for virus's first.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Radicalization - Individuals, groups and organisations with extremist and radicalised views use the internet to exert influence on young people. Staff and students are prohibited from accessing any websites or social network pages that promote such views. The school has systems and filtering in place to block extremist material and monitor those who attempt to access it. Any persons deemed to be accessing extremist material will be reported to the relevant authorities. Children are taught within the curriculum about propaganda.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – There are many social networking services available; Lime Tree Primary Academy is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Lime Tree and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officer who will advise the Head of School for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school.
- Twitter – used by the school as a broadcast service (see below).
- Facebook – used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place. The only exception to this is on Twitter where teachers will follow schools or other trusted accounts that are associated with education.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Head of School. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and an online report must be logged, no matter how small the incident may appear, using CPOMS.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Lime Tree Primary Academy will have an annual programme of training which is suitable to the audience. This is part of the school's September INSET training day.

e-Safety training for Children- e-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. Lime Tree Primary Academy have adapted a set of skills trackers, based on the National Curriculum for Computing. This outlines what must be taught each year by the Class Teacher.

As well as the programme of training, we will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Head of School and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Head of School for further CPD.

Being online and Child Protection

Online sexual violence and sexual harassment between children

- Our *Head of School* and DSL have accessed and understood the DfE "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2019.
    - Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our child protection policy.
- Lime Tree Primary Academy recognises that sexual violence and sexual harassment between children can take place online. Examples may include;
    - Non-consensual sharing of sexual images and videos

    - Sexualised online bullying
    - Online coercion and threats
    - 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence
    - Unwanted sexual comments and messages on social media
    - Online sexual exploitation
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of any concerns relating to online sexual violence and sexual harassment, we will:
    - immediately notify the DSL and act in accordance with our child protection and anti-bullying policies.
    - if content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
    - implement appropriate sanctions in accordance with our behaviour policy.
    - inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make referrals to partner agencies, such as Children's Social Work Service and/or the police.
    - if the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, the DSL (or deputy) will discuss this with the police first to ensure that investigations are not compromised.
    - review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.
- Lime Tree Primary Academy recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Lime Tree Primary Academy recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, Lime Tree Primary Academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment by implementing a range of age and ability appropriate educational methods as part of our curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

11.2 Youth produced sexual imagery ("sexting")

- Lime Tree Primary Academy recognises youth produced sexual imagery (also known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and the local KSCMP guidance: "Responding to youth produced sexual imagery".
    - Youth produced sexual imagery or 'sexting' is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
    - It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.
- Lime Tree Primary Academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding the taking and sharing of youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
    - view any suspected youth produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so.
        - If it is deemed necessary, the imagery will only be viewed where possible by the DSL, and any decision making will be clearly documented.
    - send, share, save or make copies of content suspected to be an indecent image/video of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - act in accordance with our child protection policies and the relevant local procedures.
    - ensure the DSL (or deputy) responds in line with the UKCIS and KSCMP guidance.
    - Store any devices containing potential youth produced sexual imagery securely
        - If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If a potentially indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
    - implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
    - consider the deletion of images in accordance with the UKCIS guidance.

        - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved and are sure that to do so would not place a child at risk or compromise an investigation.
    - review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

- Lime Tree Primary Academy recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL (or deputy), in line with our child protection policy.
- Lime Tree Primary Academy will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target learners, and understand how to respond to concerns.
- We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community. This can be accessed on our school website.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
    - act in accordance with our child protection policies.
    - store any devices containing evidence securely.
        - If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
    - if appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a learner is at immediate risk.
    - carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or police.

- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL (or deputy).
- If members of the public or learners at other settings are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- Lime Tree Primary Academy will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
    - act in accordance with our child protection policy and the relevant KSCMP procedures.
    - store any devices involved securely.
    - immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - ensure that the DSL (or deputy) is informed.
    - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
    - ensure that any copies that exist of the image, for example in emails, are deleted.
    - report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
    - ensure that the DSL (or deputy) is informed.
    - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
    - inform the police via 101 or 999 if there is an immediate risk of harm, and Children's Social Work Service, as appropriate.
    - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
    - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children on *Lime Tree* provided devices, we will:

- ensure that the Head of School and DSL is informed in line with our managing allegations against staff policy.
- inform the Local LADO and other relevant organisations in accordance with our managing allegations against staff policy.
- quarantine any devices until police advice has been sought.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Lime Tree Primary Academy. Full details of how we will respond to cyberbullying are set out in our anti-bullying policy. See our bullying policy on our school website.

Online hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Lime Tree Primary Academy and will be responded to in line with existing policies, including child protection, anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or the police.

Online radicalisation and extremism

- As listed in this policy, we will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a learner or adult may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the *Head of School* will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this policy sheet.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-Safety incident, reported to the e-Safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the e-Safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device. Your laptop must have a unique password that you have set.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Head of School who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of mobile phones – Mobile phone usage is permitted in school but is limited to the staff room or rooms away from children (or classrooms when children are not present). No images should be taken or stored on a personal mobile phone. Personal mobile phones may be used on school trips for phone calls and text messages.

Use of WIFI – No personal devices should be connected to the school WIFI.

Monitoring of Internet Usage – All internet usage is monitored by the Head of School and e-Safety Officer. Any material accessed on school devices may also be monitored.

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Head of School. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the e-Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to the e-Safety officer as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

Incident reporting - I understand that I must report any concerns about e-Safety to the e-Safety coordinator, the Child Protection Officer or the Head of School, logging incidents using CPOM.

Signed_____ Name: _____ Date:_____

Staff Signatures for Acceptable Use Policy

Name	Signature	Date

Acceptable Use Policy – Students

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online ; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

I understand – that for my safety, internet activity may be monitored in order to ensure as much as possible that I am not exposed to illegal or inappropriate websites.

Signed (Parent) :

Signed (Student) :

Date :

LIME TREE
PRIMARY ACADEMY
TO NURTURE, TO GROW, TO DREAM

Lime Tree Primary School
Budworth Road, Sale,
Cheshire M33 2RP
T 0161 905 0790

office@limetree.trafford.sch.uk
www.limetree.trafford.sch.uk
Head of School: Clare Larkin
Executive Principal: Simon Beswick

Dear Parent/Guardian

Use of the Internet in school is a vital part of the education of your son/daughter. At Lime Tree we use the internet to gather information, collaborate and communicate.

You will be aware that the Internet is host to a great many illegal and inappropriate websites, and as such we will ensure as far as possible that your child is unable to access sites such as this. We are able to do this using advanced software known as an Internet filter. This filter categorizes websites in accordance with their content; the school allows or denies these categories dependent upon the age of the child.

The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school. As a result, we may occasionally monitor these logs. We will inform you if this occurs.

At the beginning of each school year we explain the importance of Internet filtering to your child. Furthermore we explain that there has to be a balance of privacy and safety; we also inform them that we can monitor their activity. All children are given the opportunity to ask questions and give their viewpoint. We would like to extend that opportunity to you also; if you have any questions or concerns please arrange to speak with Mrs Benton (our e-Safety Officer).

Once you have read this letter and the Acceptable Usage Policy on the next page, please can you sign and return to school no later than _____.

Yours Sincerely

Mrs Benton

I have read this letter and understand that my child's Internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion, and to ask questions. I agree to the Acceptable Usage Policy for students at Lime Tree.

Year of child:_____ Name of child: _____

Name of parent/guardian:_____

Signature: _____ Date:_____

Risk Log

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	2	2	e-Safety Officer IT Support
2.	Internet browsing	Access to inappropriate/illegal content - students	1	2	2	
3.	Blogging	Inappropriate comments	2	1	2	Class Teachers (Administrators)
4.	Blogging	Using copyright material	2	2	4	Class Teachers E_Safety Officer
5.	Twitter	Unknown or inappropriate followers	2	2	4	Class Teachers
6.	Twitter	Images of children under child protection or without permission	1	3	3	Class Teachers
7.	Twitter	Slanderous or negative comments posted online	2	3	6	Class Teachers Head of School

Likelihood: **How likely is it that the risk could happen (foreseeability).**
Impact: **What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)**

Likelihood and Impact are between 1 and 3, 1 being the lowest.
Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE: **1 – 3 = Low Risk**
4 – 6 = Medium Risk
7 – 9 = High Risk

Owner: **The person who will action the risk assessment and recommend the mitigation to Head of School and Governing Body.**
Final decision rests with Head of School and Governing Bod

Risk Assessment

Risk No.	Risk
1	Internet Browsing - Access to inappropriate/illegal content - staff
LIkelihood 1	Staff take their laptops home for planning and making resources. They may link up to their own ISP (internet service provider). They may have different filters. This means some inappropriate or illegal sites could be accessed.
Impact 2	The impact to the school reputation would be high. Staff could access illegal or inappropriate sites and this could lead to the school network being compromised (through virus').
Risk Assessment	Low Risk
Risk Owner/s	e-Safety Officer IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Laptop is to be locked down using software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the user will receive the same level of Internet filtering at home as he/she gets whilst in school. Education: Staff are informed of acceptable usage of their laptop at home and will sign an agreement.

Approved / Not Approved (circle as appropriate) **Date:**

Signed (Headteacher) : **Signed (Governor) :**

Risk No.	Risk
1	Internet Browsing - Access to inappropriate/illegal content - students
LIkelihood 1	We have a filtering system preventing inappropriate searches. Sometimes sites and images can still pass through this system. This could mean that children see inappropriate images or websites.
Impact 2	The impact to the school reputation would be medium risk. Parents and children may be distressed by what has been seen.
Risk Assessment	Low Risk
Risk Owner/s	e-Safety Officer IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: We have a filtering system that is age appropriate for the users of the computers. In the event that a website has been accessed, this will be reported immediately to our technical support staff who will block the site. Education: Parents are made aware of systems school has in place. Parents would be contacted should an incident arrive.

	Children have to log in to use the internet and so searches can be traced.

Risk No.	Risk
3	Inappropriate comments on blog site
LIkelihood	Although comments require mediation, there could be instances of comments being approved which are not appropriate.
2	
Impact	The impact to the school reputation would be low risk. If this were to happen it could offend people who view the blog site.
1	
Risk Assessment	Low Risk
Risk Owner/s	e-Safety Officer IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: All comments are moderated by the blog administrator. Education: Children are made aware that all comments are moderated and staff are to be vigilant when approving comments.

Risk No.	Risk
4	Use of copyright material on blog site.
LIkelihood	All staff have access to post on the school blogs. Staff have access to upload videos, documents and images. Staff could upload images that have copyright protection.
2	
Impact	The school could face legal action if copyright is breached.
2	
Risk Assessment	Medium Risk
Risk Owner/s	e-Safety Officer IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Staff are trained and informed on how to check for copyright images. The blog site has 'Compfight' allowing staff to use copyright free images. Education: Children are not able to upload images onto the blog. The only exception is our 'Digital Leaders' who are taught how to ensure images do not have copyright. Children are also supervised when doing this.

Risk No.	Risk
5	Inappropriate followers on Twitter
LIkelihood	All staff have access to their own Twitter account for their class. As a result, people could follow classes, staff and parents may then have access to Twitter pages that are inappropriate.
2	
Impact	Staff and parents could be contacted by inappropriate Twitter pages.
2	
Risk Assessment	Medium Risk

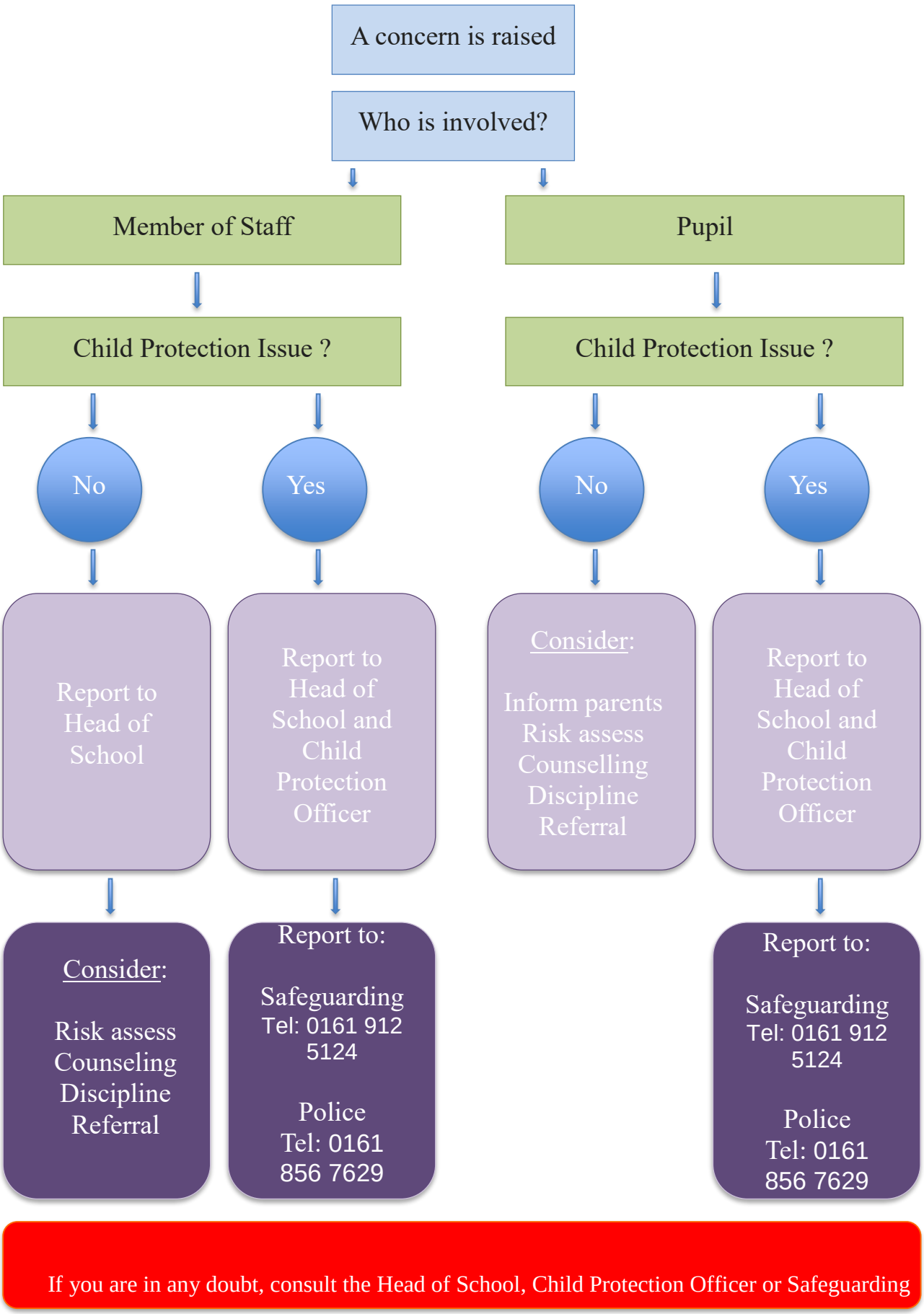
Risk Owner/s	e-Safety Officer IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Staff are to check followers and block if they appear inappropriate. Education: Children are not to post or access twitter under any circumstances. This is a form of communication that is led by the class teacher.

Risk No.	Risk
6	Images of children without permission or under child protection posted online (Twitter or Blog).
LIkelihood 1	Class Teachers and staff are aware of children who are not allowed to have their images online. Images of these children could end up online accidently.
Impact 3	Safety of children under child protection could be compromised.
Risk Assessment	Medium Risk
Risk Owner/s	e-Safety Officer IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Staff are informed during training regarding posting children's images online. Staff are not to use children's names with children's images. Education: Children cannot post images of themselves to the school blog. In the event of an image being posted accidently parents and head teacher to be informed and the image is to be deleted immediately.

Risk No.	Risk
7	Slanderous comments on social media.
LIkelihood 2	Every class and the school have a Twitter Account. Comments and notifications can appear.
Impact 3	School reputation could be affected.
Risk Assessment	Medium Risk
Risk Owner/s	e-Safety Officer IT Support

Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Staff are to monitor comments and delete any inappropriate comments. Staff are to only comment on pages of other school classes or pages used for educational purposes. Education: Children cannot access twitter posts within school.

Inappropriate Activity Flowchart



Illegal Activity Flowchart