Achieving together

Light Oaks
Junior School

E-Safety policy

Written by: Z Wilkinson
Date: December 2014
Revised: February 2015
Revised: June 2017, June 2019

Ratification by Governors				
Committee:	***Full Governing Body***	***Standards***	***Welfare, Inclusion & Pupil Support***	***Resources***
Date :	10th June 2019	**Review Date:**	June 2021	
Ratified by:	O Goodall			
Signature:	O Goodall			

Rationale:

Light Oaks Junior School believes that the use of information and communication technologies in schools brings great benefits. Recognising the e-Safety issues and planning accordingly will help all users to ensure appropriate, effective and safer use of electronic communications.

Introduction:

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

The 2014 curriculum states that at KS2 pupils should be taught to*; use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.*
These curricular changes have been incorporated into our computing lessons to make sure pupils stay safe at home and at school.

At Light Oaks Junior School we are aware that there must be a balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. We are aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Therefore children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an e-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that everyone is aware of the offline consequences that online actions can have.

At Light Oaks Junior School all staff are aware of the legal obligations to safeguard and protect children on and offline and the accountability of these decisions sit with the Head Teacher and the Governing body.

- Light Oaks Junior School has appointed an e–Safety Coordinator.
- The e–Safety Policy and its implementation will be reviewed annually.
- Our e–Safety Policy has been written by the school, building on the Salford e–Safety Policy and government guidance.

- Our School Policy has been agreed by the Senior Leadership Team and approved by governors and other stakeholders.
- The School has appointed a member of the Governing Body to take lead responsibility for e-Safety
- E-safety is incorporated into the computing curriculum at Light Oaks Junior School.

The School e-Safety Coordinator is Mrs Z Wilkinson

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school

Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community
- The Headteacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

E-Safety Coordinator/Officer:

- leads the e-safety committee and/or cross-school initiative on e-safety
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports regularly to Senior Leadership Team

Network Manager / Technical staff: (RM Education)

is responsible for ensuring:

- that the school’s ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Salford City Council Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school’s networks through a properly enforced password protection policy

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator or Headteacher for investigation/action/sanction

Designated person for child protection/Child Protection Officer

should be trained in e-safety issues and be aware of the potential for serious child Protection issues to arise from:

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

E-Safety Committee

Members of the E-safety will assist the E-Safety Coordinator/Officer with:

- the production, review and monitoring of the school e-safety policy

Students/pupils:

- are responsible for using the school ICT systems and mobile technologies in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents/Carers

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student/Pupil Acceptable Use Policy
- accessing the school ICT systems or Learning Platform in accordance with the school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems or Learning Platform as part of the Extended School provision will be expected to sign a Community User Acceptable Use Policy (AUP) before being provided with access to school systems.

Safety Education and Training

Education – students / pupils

E-Safety education will be provided in the following ways:

A planned e-safety programme will be provided as part of computing/PHSE/other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school

- Key e-safety messages will be reinforced as part of a planned programme of assemblies and class activities
- Students/pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Safer Internet Day in February will be a focus of whole school learning and reinforcement of safety messages

Education & Training – Staff

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

- *A planned programme of formal e-safety training will be made available to staff. This will include at least one annual update for the whole staff. An audit of the e-safety training needs of all staff will be carried out annually. It is expected that some staff will identify e-safety as a training need within the performance management process.*
- *All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies*
- February will be a focus of whole school learning and reinforcement of safety messages

Education & Training – parents and carers

In order to support parents to keep their children safe and give them advice and help with e-safety, school will:

- Always discuss with parents any concerns about unacceptable use that is brought to its attention, whether inside school or at home
- Provide parents with leaflets and other information (e.g. on the school website), about e-safety and where help can be found online
- Run information sessions for parents to attend
- It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

Communication devices and methods

The following table shows the school's policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

	Staff & other adults				**Students/Pupils**			
Communication method or device	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
	☑	⚠	⚠	☒	☑	⚠	⚠	☒
Mobile phones may be brought to school*	✓						✓	
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on personal mobile phones or other camera devices				✓			✓	
Use of personal hand held devices eg PDAs, PSPs	✓				✓			
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails			✓				✓	
Use of chat rooms / facilities	✓						✓	
Use of instant messaging (text only)		✓					✓	
Use of social networking sites		✓					✓	
Use of blogs	✓						✓	
Use of instant messaging (images)		✓					✓	

* please ensure you are aware of the acceptable use of mobile phones (below)

Unsuitable/inappropriate activities

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

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
User Actions	☑	⚠	⚠	☒	☒
child sexual abuse images					☒
promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					☒
adult material that potentially breaches the Obscene Publications Act in the UK					☒
criminally racist material in UK					☒
Pornography					☒
promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability					☒
promotion of racial or religious hatred					☒
threatening behaviour, including promotion of physical violence or mental harm					☒
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				☒	
Using school systems to run a private business				☒	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and / or the school				☒	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				☒	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				☒	
Creating or propagating computer viruses or other harmful files				☒	

Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				☒	
On-line gaming (educational)	✓				
On-line gaming (non educational)		✓			
On-line gambling				✓	
On-line shopping / commerce		✓			
File sharing	✓				
Use of social networking sites		✓			
Use of video broadcasting eg Youtube	✓				
Accessing the internet for personal or social use (e.g. online shopping)		✓			
Using external data storage devices (e.g. USB) that have not been checked for viruses				✓	

Policy Decisions

Internet access
At Light Oaks Junior School:

- All staff read and sign the School Acceptable Use Policy.
- All staff and pupils with accounts have internet access.
- Parents are asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- esafety policy is discussed with new staff and volunteers as part of their induction.

How risks are assessed.

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Salford LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How school responds to any incidents of concern.

- All members of the school community are informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the e-Safety log and/or in any relevant areas e.g. Bullying or Child protection log.
- The Designated Person for Child Protection will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- Staff will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- Staff will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, staff will debrief, indentify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the LA e-Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other schools in Salford.

Incident Management

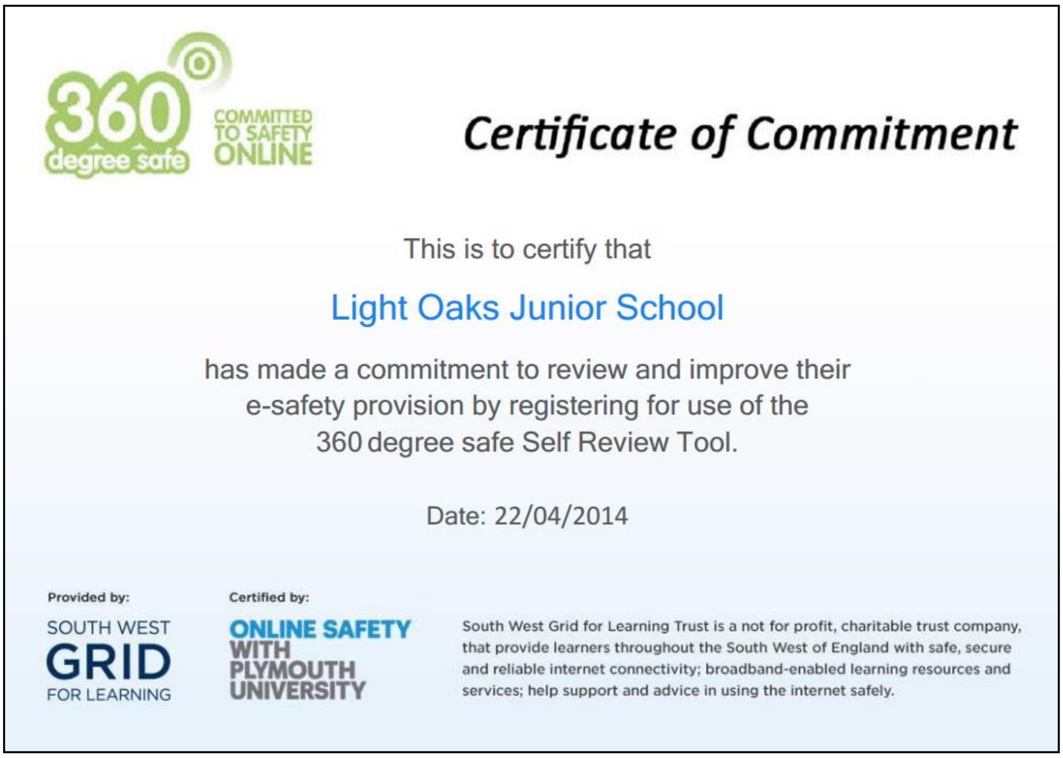
Incidents (students/pupils): ✓ *definite consequence* ***P*** *potential consequence*	Class teacher	Assistant or Deputy Head	Headteacher	Refer to Police	Refer to RM or website	Inform parents / carers	Removal of access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal			✓	**P**	✓	✓	✓		✓
Unauthorised use of non-educational sites during lessons	✓	**P**				**P**	**P**	✓	**P**
Unauthorised use of mobile phone/digital camera / other handheld device		✓				✓	**P**	✓	**P**
Unauthorised use of social networking/ instant messaging/personal email	✓	**P**			✓	✓	**P**	✓	**P**
Unauthorised downloading or uploading of files	✓	**P**				**P**	**P**	**P**	**P**
Allowing others to access school network by sharing username and passwords	✓	✓				**P**	**P**	**P**	**P**
Attempting to access or accessing the school network, using another student's/pupil's account	✓	✓				**P**	**P**	**P**	**P**
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓				✓	**P**	✓	**P**
Corrupting or destroying the data of other users	✓	**P**			✓	**P**	**P**	✓	**P**
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓		**P**		✓	**P**		✓
Continued infringements of the above, following previous warnings or sanctions		✓	✓	**P**		✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓			✓	**P**		✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	**P**			✓	**P**	**P**	✓	**P**
Deliberately accessing or trying to access offensive or pornographic sites		✓	**P**		✓	✓	**P**		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	**P**				**P**		✓	
Incidents happening outside school that have safeguarding implications or could lead to problems in school		✓	**P**	**P**		✓		✓	**P**

Incidents (staff and community users): ✓ *definite consequence* ***P*** *potential consequence*	Line manager	Head teacher	LADO / LA	Refer to Police	Refer to RM or website	Removal of access rights	Warning	Conduct Procedures
Deliberately accessing or trying to access material that could be considered illegal		✓	✓	**P**		**P**		**P**
Unauthorised use of non-educational sites during lessons	✓	✓	**P**			**P**	✓	**P**
Unauthorised use of mobile phone/digital camera / other handheld device	✓	**P**	**P**	**P**		**P**		**P**
Unauthorised use of social networking/ instant messaging/personal email	✓	**P**	**P**	**P**	**P**	**P**	✓	**P**
Unauthorised downloading or uploading of files	✓						✓	
Sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	**P**			**P**		✓	**P**
Careless use of personal data eg holding or transferring data in an insecure manner	✓	**P**	**P**		**P**		✓	**P**
Deliberate actions to breach data protection or network security rules		✓	✓	**P**	✓	**P**		**P**
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	**P**	**P**		**P**		**P**
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓	**P**		**P**		✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		✓	✓	**P**		**P**		✓
Actions which could compromise the staff member's professional standing	✓	**P**	**P**			**P**	✓	**P**
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	**P**				✓	**P**
Accidentally accessing offensive or pornographic material and failing to report the incident	✓				✓		✓	
Deliberately accessing or trying to access offensive or pornographic sites		✓	✓	**P**	✓	**P**		✓
Breaching copyright or licensing regulations	✓			**P**			✓	
Continued infringements of the above, following previous warnings or sanctions		✓	✓	**P**		**P**		✓
Incidents happening outside school that have safeguarding or professional implications or could lead to problems in school	✓	**P**	**P**	**P**			✓	**P**

Appendix 1: Schools e-Safety Audit

Light Oaks Junior School uses the 360^0 Safe Audit tool and updates this termly. (http://www.360safe.org.uk).

We currently hold a certificate of commitment and a certificate of progress towards the e-safety mark.



360 degree safe
COMMITTED TO SAFETY ONLINE

Certificate of Commitment

This is to certify that

Light Oaks Junior School

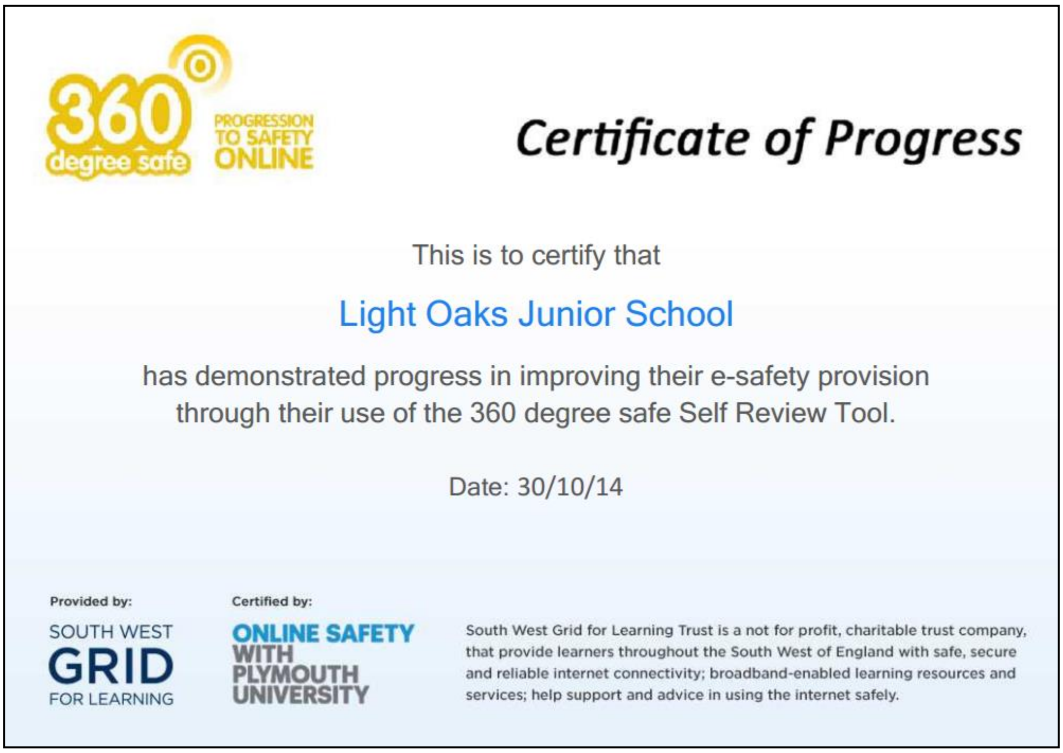
has made a commitment to review and improve their
e-safety provision by registering for use of the
360 degree safe Self Review Tool.

Date: 22/04/2014

Provided by:
SOUTH WEST GRID FOR LEARNING

Certified by:
ONLINE SAFETY WITH PLYMOUTH UNIVERSITY

South West Grid for Learning Trust is a not for profit, charitable trust company, that provide learners throughout the South West of England with safe, secure and reliable internet connectivity; broadband-enabled learning resources and services; help support and advice in using the internet safely.



360 degree safe
PROGRESSION TO SAFETY ONLINE

Certificate of Progress

This is to certify that

Light Oaks Junior School

has demonstrated progress in improving their e-safety provision
through their use of the 360 degree safe Self Review Tool.

Date: 30/10/14

Provided by:
SOUTH WEST GRID FOR LEARNING

Certified by:
ONLINE SAFETY WITH PLYMOUTH UNIVERSITY

South West Grid for Learning Trust is a not for profit, charitable trust company, that provide learners throughout the South West of England with safe, secure and reliable internet connectivity; broadband-enabled learning resources and services; help support and advice in using the internet safely.

Appendix 2: e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

EiS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Schools e–Safety Blog: www.kenttrustweb.org.uk?esafetyblog

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Appendix 3: Good practice guidelines

Email

Best practice

☑ **DO**

Staff and students/pupils should only use their school email account to communicate with each other

Safe practice

⚠

Check the school e-safety policy regarding use of your school email or the internet for personal use e.g. shopping

Poor practice

☒ **DO NOT**

Staff: don’t use your personal email account to communicate with students/pupils and their families without a manager’s knowledge or permission – and in accordance with the e-safety policy.

Images, photos and videos

Best practice

☑ **DO**

Only use school equipment for taking pictures and videos.

Ensure parental permission is in place.

Safe practice

⚠

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

☒ **DO NOT**

Don’t download images from organisation equipment to your own equipment.

Don’t use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don’t retain, copy or distribute images for your personal use unless this is for a valid educational use (e.g. part of a teaching portfolio) ensuring that permission has been sought from the Headteacher and no children can be identified

Internet

Best practice

☑ **DO**

Understand how to search safely online and how to report inappropriate content .

Safe practice

⚠

Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

Poor practice

☒ **DO NOT**

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the e-safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Mobile phones

Best practice

☑ **DO**

Staff: If you need to use a mobile phone while on school business (trips etc), the school will provide equipment for you.

Make sure you know about inbuilt software/ facilities and switch off if appropriate.

Safe practice

⚠

Check the e-safety policy for any instances where using personal phones may be allowed.

Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first

Poor practice

☒ **DO NOT**

Staff: Don’t use your own phone without the Headteacher/SLT knowledge or permission.

Don’t retain service student/pupil/parental contact details for your personal use.

Social networking (e.g. Facebook/ Twitter)

Best practice

☑ **DO**

If you have a personal account, regularly check all settings and make sure your security settings are not open access.

Ask family and friends to not post tagged images of you on their open access profiles.

Safe practice

⚠

Don’t accept people you don’t know as friends.

Be aware that belonging to a ‘group’ can allow access to your profile.

Poor practice

☒ **DO NOT**

Don’t have an open access profile that includes inappropriate personal information and images, photos or videos.
Staff:

- Don’t accept students/pupils or their parents as friends on your personal profile.
- Don’t accept ex-students/pupils users as friends.
- Don’t write inappropriate or indiscrete posts about colleagues, students/pupils or their parents.

Webcams

Best practice

☑ **DO**

Make sure you know about inbuilt software/ facilities and switch off when not in use.

Safe practice

⚠

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

☒ **DO NOT**

Don’t download images from organisation equipment to your own equipment.

Don’t use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don’t retain, copy or distribute images for your personal use (see images section above)

Appendix 4: Managing Information Systems

How information systems security are maintained?

- Light Oaks Junior School's ICT is managed by RM.
- RM uses a filtering system which is up dated daily.
- Staff users and pupils must take responsibility for their network use. Flouting electronic use policy is regarded as a reason for dismissal of staff.
- Servers are located securely and physical access is restricted.
- The server operating system is secured and kept up to date by RM.
- Virus protection for the whole network is managed by RM, it is installed and current.
- Access by wireless devices are proactively managed and secured by RM managed service.

Wide Area Network (WAN) security issues include:

- RM Broadband firewalls and local CPEs are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership between schools and RM.
- Permission to access blocked sites must be requested
- The security of the school information systems and users is reviewed regularly by RM.
- Virus protection is updated regularly by RM.
- Personal data sent over the Internet or taken off site is encrypted.
- Portable media may not used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to emails.
- Files held on the school's network are regularly checked by RM managed service.
- The ICT coordinator/network manager will reviews system capacity regularly.
- The use of user logins and passwords to access the school network is enforced.

How email is managed.

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools in both neighbouring and wider areas and in different countries can be created.

At Light Oaks Junior School:

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils are taught not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff email addresses are used for communication outside of the school.
- Staff only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.

How published content is managed.

- The Light Oaks Junior School website enables pupils to publish work.
- Our Website celebrates pupils' work, promotes the school and publishes resources for projects.

- The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information are not published.
- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website complies with the school's and national guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

How pupils' images or work is published.

- Images or videos that include pupils will be selected carefully in order to keep all children safe.
- Pupils' full names are not used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers is obtained annually before images/videos of pupils are electronically published.
- Written consent is kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

How social networking, social media and personal publishing is managed.

- Children do not have access to social media sites, but the school teaches them about internet safety.
- Through e-safety lessons, pupils are advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils are made aware that social network sites should only be used by those over the age of 13.
- Pupils are advised on security and privacy online and are encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils are encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

How filtering is managed.

The school's managed ICT service (RM) filters all unsuitable sites.
School recognises that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g. mobile phone).

At Light Oaks Junior School:

- The school's broadband access includes filtering appropriate to the age and maturity of pupils.

- The school will work with Salford LA and RM team to ensure that filtering policy is continually reviewed.
- The school has a clear procedure for reporting breaches of filtering technician.
- All members of the school community (all staff and all pupils) are aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator / ICT co-ordinator or ICT technician who will then record the incident and escalate the concern as appropriate.
- A request to unblock a site can be made to RM.
- Any material that the school believes is illegal will be reported to RM who will report to the appropriate agencies.
- The school's access strategy is designed by RM to suit the age and curriculum requirements of the pupils.

How emerging technologies are managed.

- Emerging technologies are examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy.
- Pupils are not permitted to use mobile phones at school.

How personal data is protected

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. At Light Oaks Junior School personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.
The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.