The Lancaster School

THE LANCASTER SCHOOL

E-Safety Policy

April 2018

To be reviewed annually

Introduction

Safeguarding is a serious matter; at The Lancaster School we use technology and the Internet 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.

The primary purpose of this policy is:

- To ensure the requirement to empower the whole school 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 Lancaster School website; Staff and Students must sign the Acceptable Use Policy when they join the school.

Roles & Responsibilities

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 school.

Reporting to the governing body, the Headteacher 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 as indicated below.

The Headteacher 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.
- All E-Safety incidents are dealt with promptly and appropriately.

The day-to-day duty of the E-Safety Officer will be:

Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for academy and home use.

- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all E-Safety matters.
- Engage with parents on E-Safety matters at the 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.
- Attend appropriate training
- Provide support and training for staff on Online Safety.
- Liaise with the Safeguarding Lead as appropriate.
- Ensure any technical E-Safety measures in the 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 Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

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 Headteacher.

All 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 Headteacher.
- Any E-Safety incident is reported to the E-Safety Officer (and an E-Safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the E-Safety Officer or the Headteacher to make a decision.

All students are to be made aware of the E-Safety agenda. The boundaries of use of ICT equipment and services in this school are given in the Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

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 academy environment. Through parents evenings, newsletters and annual E-Safety days the school will keep parents up to date with new and emerging E-Safety risks, and will involve parents in strategies to ensure that students are empowered.

Responsible individuals are fully aware of their role and any incidents are dealt with on an individual basis. This will be reviewed annually.

Counter-Terrorism/Prevent Duty:

More information regarding the Prevent Duty policy can be found at the following website. http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

The Lancaster School and Avalon IT constantly monitor on-going internet activity in relation to counter terrorism. Emails, internet activity are monitored daily through staff supervision, anti-virus malware, sporadic checks by Avalon IT and e-safety mentoring. As part of e-safety education, the children are taught how to keep themselves safe from 'Culture' behaviour. 'Culture' behaviour is defined as: Young people becoming caught up in a pack mentality and becoming involved in appropriate anti-social behaviour. As schools have a more important role to play in relation to prevention, staff at The Lancaster School have been made aware of resources to aid in educating the children about radicalisation. These can be found at the following website. http//www.saferinternet.org.uk/

Technology

The Lancaster School uses a range of devices including PC's 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 internet filtering that prevents unauthorized 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 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 Headteacher.
Email Filtering –that 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.
Passwords – all staff and students will be unable to access any device without a unique username and password.
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 Headteacher if there are any concerns.

Keeping Children Safe in Education, Sept 2016 has established that, whilst schools and Trusts should do all that they can to protect children from potentially harmful and inappropriate online material, the measures that are taken should be reasonable, and they should not 'over block' the information available to children.

Safe Use of Technology
Internet – Use of the Internet in the school is a privilege, not a right. Internet use will be granted: to staff upon signing 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.
Photos and videos – Digital media such as photos and videos are for sole use in the school. Parents will be asked for consent for photos to be published on the school website. In addition, the following is to be strictly adhered to:

- Permission slips must be consulted before any image or video of any child is uploaded to the website.
- There is to be no identification of students using first name and surname.

Social Media
All staff have read and signed the staff code of conduct and AUP relating to the use of technological equipment outside of school including Facebook, Twitter etc. In the case of inappropriate use on the Internet the Head Teacher will follow the staff conduct procedures.

The school recognises that many staff will actively use Facebook, Twitter and other such social networking sites. Staff must not post, material (including text or images) which damages the reputation of the school or which causes concern about their or any other member of staff suitability to work with children. Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks. It is never acceptable to accept a 'fiend request' from pupils, as in almost all cases children of infant age using networks will be breaching terms and conditions of use of those networks. It is never acceptable to initiate a friend request with a pupil. It is advisable to accept friend requests from ex-pupils. It is advisable or staff to accept or initiate a friend request with a parent or carer on social networking sites.

Due to the age of our children in school Facebook is not permitted.
Parents are informed at all events in school that photographs and videos should only be of their own child and these should not be published on any social media site.

Parents are informed to only take photographs and videos of their child at the end of an event with accompanying that images are not to be shared online.
Any incidents should be reported to the Head Teacher or E-Safety Officer for further investigation.

Mobile Phones
Children do not bring mobile phones or game devices into school.
As part of the AUP staff must keep mobile phones in the staff room and are not to be brought into the classroom. They must not be used to take photographs.

Training and Curriculum
It is important that the school 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.
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.

At The Lancaster School this includes:

- Key Online Safety messages are reinforced through assemblies, Safer Internet Day (February) and throughout all lessons.
- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies.
- Materials from CEOP, Think you know, Child.net, Internet Matters and NSPCC will be used to deliver our Online Safety Curriculum.
- Each class has a E-Safety champion which make a E-safety committee.
- Websites used in the classroom will be viewed by the staff member prior to the lesson, with regular checks being made of the Internet browser.
- E-safety lessons delivered as part of our termly Keeping Healthy and Safe days.
- E-Safety lessons are planned for in the long and medium term planning.
- E-Safety rules are shared with parents at the induction meeting.
- E-safety rules are clearly stated on homework when using the Internet.
- Pupils will agree to the schools AUP when they join the school and parents and carers will sign this on their behalf.
- Providing and maintain links to up to date information on the school website.
- Recommending support organisations such as Child Exploitation and Online Protection (CEOP)

Protecting personal data
All data is protected in line with the GDPR regulations. Please see GDPR Policy.

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

All staff has E-Safety training to keep them up to date which is done on an annual basis. However, staff are updated regularly at staff meetings and the opportunity to discuss E-Safety is given a high priority.

This policy will be reviewed annually.

Signed:
Date:

Appendix 1
Staff Acceptable Use of the Internet Policy

At The Lancaster School we recognise that practitioners will use online and digital technologies in their personal and social lives. We do not seek to prevent any practitioner from accessing online technologies however we do ask them to sign a Professional Conduct Agreement to ensure there is no confusion between their home and professional roles.

Name:

I agree that through my recreational use of social networking sites or other online technologies that I will:

- not bring The Lancaster School into disrepute.
- observe confidentiality and refrain from discussing any issues relating to work, children and parents/carers.
- not share or post, in an open forum, any information that I would not want children, parents/carers or colleagues to view.
- set privacy settings to block unauthorised access to my Social Media sites
- keep my professional and personal life separate, and will not accept children and young people and parents/carers as 'friends'.
- consider how my social conduct may be perceived by others and how this could effect my own reputation and that of The Lancaster School.
- either avoid using a profile photograph or ensure it is respectable, and an image I would be happy to share with anyone.
- report any known breaches of the above.

I understand that the completion of this form is optional. However, I voluntarily choose to complete it to safeguard my own professional reputation and that of The Lancaster School. I understand I am in a position of trust and my actions outside of my professional environment could be misinterpreted by others, and I am conscious of this when sharing information publicly with others.

Signature:

Date:

Appendix 2

Dear Parent

As part of the framework and programme of activities to support children's learning and development, your child will have the opportunity to access a wide range of Computing resources.

These resources include access to:

- Computers
- Internet
- Email
- Ipads
- Digital cameras
- Recorders and Dictaphones.

We recognise the important contribution and value that such resources play in promoting children's learning and development; however, we also recognise there are potential risks involved. We therefore have rigorous online safety policies and procedures in place.

In order to support us further in developing your child's knowledge and understanding about online safety, please read the Internet rules with your child.
We then ask that you and your child to sign and return the attached form.

We understand that your child is too young to give informed consent on his/her own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful partnership.

Hopefully, you will also find these rules provide you with an opportunity for further conversations between you and your child about safe and appropriate use of the online and digital technologies, both within and beyond the school environment, such at a friend's house or at home.

Should you wish to discuss the matter further, please do not hesitate to contact me.

Yours sincerely

Name:

Child Agreement

Online safety acceptable use agreement return form

- I understand the agreement for using the internet, and I will follow the Internet Rules-

1. **Always ask an adult before using the Internet.**
2. **Zip it. Never give my name or address when using the Internet.**
3. **Always tell an adult if I see something that worries or upsets me on the Internet.**

- I know the adults looking after me will help me to stay safe and check that I am using the computer to help me with my work.

Child signature:
Date:

Parent/Carer Agreement

Online safety acceptable use agreement return form

- I have read and discussed the agreement with my child and confirm that he/she has understood what the rules mean.
- I understand that the setting will use appropriate filtering and ensure appropriate supervision when using online and digital technologies.
- I understand that occasionally, inappropriate materials may be accessed and accept that the setting will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the internet and other online tools outside of the school setting, that it is my responsibility to ensure safe and responsible use with the support of the setting.

Parent/Carer signature:
Date:

Appendix 3

E-Safety Incident Log

Number:	Reported By: (name of staff member)	Reported To: (e.g. Head, E-Safety Officer)	
	When:	When:	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		Date:	
Signature (Governor)		Date:	