Online Safety Policy

DOCUMENT CONTROL

Version history

Version	Date	Comments
V1.1	03/10/2016	Written by Rebecca Terry
V1.1a	07/03/2018	Re written by Ingrid Lowis
V1.2	24/3/2019	Alterations by Louise Duirwyn/Elspeth Mukerji

Changes since last version

Version	Description
V1.1a	**Changes taking into account the GDPR (General Data Protection Regulation)**
V1.2	**Changes regarding the use of personal devices for taking images to be in line with our Safeguarding policy, Acceptable Use agreement**

Reviewers

Name	Role
Sara Nobili	**Safeguarding Trustee**
Rachel Theobald	**DSL**
Elspeth Mukerji	**Deputy DSL**
Date of Next Review	**March 2020**

Issue control

Owner	Lancaster Steiner School
Author	Ingrid Lowis
Trustee with responsibility	Sara Nobili
Signature	*Sara Nobili*
Sign off Date	27th March 2019

POLICY STATEMENT

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education (Sept 2018) and its advice for schools on preventing and tackling bullying. It also refers to the Department's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

This Online Safety Policy has been agreed by the College of Teachers, Trustees and Safeguarding leads.

Safeguarding is taken very seriously and this document outlines and clarifies to the way in which Online Safety is to be addressed by both pupils and staff at Lancaster Steiner School (LSS).

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 foreseeable harm to students, staff, parents, users and the wider school community or liability to the school.*

This policy is available for anybody to read and is available on the LSS website, upon review all members of staff will sign as read and understood both, the online Online Safety Policy, Whole School Behaviour Policy and the Acceptable Use Policy (AUP).

Online safeguarding, known as Online 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 online safety incident, whichever is sooner.

GLOSSARY

For clarity, the Online Safety policy uses the following terms, unless otherwise stated;

Lancaster Steiner School: LSS

SGT: Senior Governance Team includes the Trustees, Education and Teacher Coordinators, Early Years Lead and the School Manager

Management Team: Education and Teacher Coordinators, Early Years Lead and the School Manager

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.

Pupils: Kindergarten, Lower School Class T to 5,

School: Any school business or activity conducted on or off the school site, e.g. visits, meetings, school trips etc.

Wider school community: Parents, visitors & relatives

Data Protection Officer: (DPO) Heather Holt

Trustee with responsibility for Safeguarding: Sara Nobili Park

Designated Safeguarding Leads: (DSL) Rachel Theobald & (Deputy) Elspeth Mukerji

Local Authority Designated Officer: LADO

ROLES AND RESPONSIBLITIES

SCHOOL GOVERNANCE TEAM (SGT)

The SGT has overall responsibility for monitoring this policy and holding the management team to account for its implementation. The Trustee with responsibility for Safeguarding will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor any online safety concerns as provided by the designated safeguarding lead (DSL). All trustees will:

• Ensure that they have read and understand this policy

• Agree and adhere to the terms of Acceptable Use of the school's ICT systems and the internet

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

Details of the school's designated safeguarding lead (DSL) are set out in our safeguarding policy.

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

• Supporting the management team in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

• Working with the staff, as necessary, to address any online safety issues or incidents

• Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

• Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the Whole School Behaviour policy

• Ensuring that staff undertake and regularly update training on online safety

• Liaising with other agencies and/or external services if necessary

• Providing regular reports on online safety in school to the Trustee with responsibility for Safeguarding

The school provides the following measures to ensure reasonable steps are in place to reduce the risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Regular staff training in Child Protection, PREVENT, Online Safety and Peer on Peer Abuse Awareness Training accessed on Educare, as outlined in the rolling training programme (any additional training, such as Child Sexual Exploitation, will be accessed on Educare as deemed necessary by the DSL)
- Clear reporting guidance including responsibilities, procedures and sanctions
- Issuing all staff with an LSS Staff Handbook, and our Code of Conduct and the Employee Handbook which includes Social Media Policy, the use of Computer and Electronic devices

- Ensuring all staff read and sign our Bring Your Own Devices and Acceptable Use agreements

STAFF

All staff are expected to

- read and sign the Acceptable Use Policy and Online Safety Policy before using any school ICT resources
- lead by example, and have an up to date awareness of Online Safety matters, current school policies and practices
- familiarise with current issues and guidance through organisations such as, CEOP (Child Exploitation and Online Protection) and ChildNet (forwarded by DSL)
- report misuse or problems to DPO for investigation
- understand that digital communications with pupils on roll are not permitted
- deliver our online safety curriculum
- keep electronic devices in the staff room or office at all times
- ensure that all digital communications with staff and parents should be on a professional level
- register their electronic devices on an Acceptable Use agreement. Members of staff can then use their device to capture children's work, but only class teachers and the admissions officer can use their devices for capturing images of children and only when they have registered their device with a Bring Your Own Devices agreement and their device is not linked to to any virtual storage such as icloud or googlemail. The office must be notified prior to taking the device into an area where the children are situated, all pictures will be TRANSFERRED by the staff member onto the school hard drive, and then all photos must be deleted before leaving the school premises with their device. (For more information see the Use of Image Policy)
- abide by the Social Media Policy (Employee Handbook)
- keep parents regularly updated about online safety

SCHOOL MANAGER

The School Manager will coordinate office staff to

- maintain a current record of anyone who are granted access to the school' s electronic communications
- carry out inductions with all new volunteers, staff and trustees
- ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- ensure that users may only access the school's computers through a properly enforced password protection policy, in which passwords are regularly changed

- keep up to date with technical information, in order to effectively carry out their role
- keep abreast of current issues and guidance through organisations such as, CEOP (Child Exploitation and Online Protection) and ChildNet.

PUPILS

Phones are only to be brought into school only when absolutely necessary, with prior agreement parents are to inform the school in writing stating the reason. In this instance pupils are to hand their phone in to the office at the beginning of the school day, and it will be kept in the office till needed.

Any devise brought without permission during the school day, will be confiscated and stored in the office ready to return at the end of the school day.

If pupils are using devices with their class teacher as part of the curriculum then they are expected to only access the resources /materials they have been asked to use under direct supervision

PARENTS, CARERS AND VISITORS

Parents are expected to;

- inform school immediately of any concerns regarding Online Safety
- support the ethos of the school – which stresses the importance of the human relationship and the spoken word in the primary years – and to protect individual privacy, we strongly ask parents/carers not to use mobile phones in school when dropping off or collecting children
- make sure their own use of ICT, for example mobile phones, laptops, and cameras when in school or with school on trips, festivals, walks and visits is appropriate as outlined in the school Acceptable Use agreement
- ensure that no pictures of pupils other than their own children are posted on social networking sites without direct permission from the parent of the pupils concerned
- follow the complaints procedure rather than posting complaints on social networking sites
- not post malicious or fictitious comments on social networking sites about any member of the school community.
- any comments on social media sites that could be interpreted as bringing the school into disrepute will be handed to the Local Authority Legal Team who will decide on an appropriate course of action.
- leave all electronic devices with the school office or staff room if staying in school.

Parents are informed of their responsibilities regarding this Online Safety policy during the Educational Interview for their child. This information is also in the Parent Handbook.

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

UK Safer Internet Centre: https://www.saferinternet.org.uk/advicecentre/parentsand-carers/what-are-issues

Hot Topics, Childnet International: http://www.childnet.com/parents-and-carers/hottopics

Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parentsfactsheet-09-17.pdf

The government also provides an online reporting tool for concerns about online ,material that promotes extremism or terrorism which both staff and parents can use http://www.gov.uk/report-terrorism

COMMUNITY USERS

Community Users of the school are not given access to any of the school's IT equipment. They are informed of the school photograph policy.

CURRICULUM

We have an Online Safety Curriculum Framework (see Appendix 2) which will form part of our PSHE curriculum that begins in Kindergarten and covers all aspects of internet use introduced at an age appropriate level.

Pupils are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline.

DEALING WITH INCIDENTS

CYBER BULLYING

Cyber bullying can be defined as the use of information and communications technology particularly mobile phones and the internet, deliberately to upset someone else. Cyber bullying that occurs while pupils are under the school's direct supervision will be dealt with in line with this policy, the Safeguarding Policy and the Whole School Behaviour Policy.

In cases where cyber bullying occurs while pupils are outside our direct supervision (i.e. at home), parents will be encouraged to report these incidents to the Police as criminal laws (such as those pertaining to harassment, threatening and menacing communications) may apply. Parents are also encouraged to report such bullying to the school. If the alleged perpetrator is a member of this school community, the school will act in line with the Whole School Behaviour Policy and procedures. The school will, wherever possible, support parents in this and may impose a sanction upon the bully where this individual is recognisable.

The school can take action against incidents that happen outside school, when;

- actions could have repercussions for the orderly running of the school,
- actions pose a threat to another pupil, college of staff, trustee, parent or member of the public which could adversely affect the reputation of the school.

Acts of cyber bullying can include:

- name-calling;
- mocking;
- making offensive comments;
- inappropriate text messaging, emailing or 'posting' on social media sites;
- sexting;
- sending offensive or degrading images by phone or via the internet e.g. via Social media sites;
- excluding people from groups;
- spreading hurtful and untruthful rumours.

ACCEPTABLE USE OF THE INTERNET IN SCHOOL

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We reserve the right to monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the Acceptable Use Policy.

The school takes all reasonable precautions to ensure that users access only appropriate material online including the use of filters. However, it is not possible to guarantee that unsuitable material will never appear on a school computer.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990

RESPONSE TO A BREACH OF POLICY

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

LINKS TO OTHER POLICIES AND DOCUMENTS

This policy forms part of Lancaster Steiner School's policy for safeguarding children. It should also be read alongside:-

- Safeguarding Policy
- Whole School Behaviour Policy
- Data Protection Policy and GDPR 2018
- Keeping Children Safe in Education 2018
- Acceptable Use Policy and Bring Your Own Device Agreements
- Use of Image Policy

APPENDIX 1

Online Safety Declaration

I_____(full name) confirm I have read and understand the Lancaster Steiner School Online Safety Policy. If I have any questions I should speak to the Safeguarding Lead, Rachel Theobald.

Signed:

Date: