E-SAFETY UMBRELLA POLICY

PART I: INTRODUCTION, PURPOSE AND SCOPE OF THE POLICY

The e-safety policy for the LTC organisation is an umbrella policy consisting of various policies and procedures which together encompass the e-safety environment for all schools and the charity.

This policy is to be read in conjunction with other school-based and LTC-wide policies, paying particular attention to the following:

School-Based Policies

- Anti-bullying Policy
- Behaviour Policy
- Mobile Phone Acceptable Use Policy
- Photography Policy
- Safeguarding and Child Protection Policy

LTC-Wide Policies

- LTC Bring Your Own Device Policy
- LTC Data Protection Policy
- LTC e-Content and Social Media Policy
- LTC e-safety Monitoring Policy
- LTC Online Safety Monitoring Policy
- LTC Passwords and Security Policy
- LTC Student Acceptable Use Policy

Whilst performing their role at LVS Oxford, staff may be required to use digital and electronic resources. These resources, owing to their nature, may be subject to rapid change and development. All staff (including volunteers and self-employed staff) are to operate under this policy. Any visitors using LTC digital equipment or resources also fall under this policy for the relevant period.

All staff must ensure that they are aware of and have read the above listed policies and are aware of how to report e-safety incidents. While all policies are current, by nature they are organic and thus subject to an on-going process of review and adjustment. Reviews, adjustments and amendments are communicated to all staff to ensure updated knowledge. At a point to be determined, staff will be required to sign a register stating they have read and understand these documents.

In discharging their role and working with the required resources, staff must be aware of and adhere to the laws of this country, their employment terms and conditions, their professional code(s) of conduct and, where applicable, all school policies, procedures and operational guidance. If a member of staff is unsure of these aspects, they must immediately notify their line manager or the HR department.

Everyone is responsible for e-safety – both the school and students. The school is responsible for providing (a) a well-managed and maintained technical infrastructure that allows for the safe and reasonable use of digital technology and (b) age-appropriate education of the students in how to

safely and reasonably use digital technology. E-safety is not only about monitoring digital behaviour; it is about educating pupils about their digital lives.

RESPONSIBILITIES

As a shared responsibility, e-safety is only effective when every member of the organisation, is aware of their responsibilities. There is a network of individuals involved in e-safety at every level, each with particular responsibilities:

The e-safety Governor/Trustee is responsible for

- Approval of the e-safety and related policies and for reviewing their effectiveness and receiving regular information about e-safety incidents through the e-safety Committee.

The e-safety Committee (composed of the safe guarding, Head of Centre, Deputy Head, Head of Sixth Form and Assistant Head a representative from IT, Marketing and any further representatives required by the Committee) is responsible for

- Establishing effective e-safety
- Advising changes to e-safety policy
- Recommending further initiatives for e-safety

The Internet Filtering Committee is responsible for

- Discussing any changes to filtering requirements
- Enacting any points from the e-safety Committee
- Advising on initiatives for internet filtering and feedback to relevant parties
- Updating any changes to the Internet Filtering categories

The Head of each school is responsible for

Ensuring the e-safety of the school community by ensuring all members of staff receive suitable and relevant training to enable them to carry out their e-safety roles. The Head must also ensure there is a system in place to allow for monitoring and support of those in school who carry out the e-safeguarding role.

The Deputy Head (Pastoral) of each school is responsible for

- Taking day to day responsibility for e-safety issues,
- Operation of the e-safety incident process
- Operation of the e-safety monitoring policy
- Receiving/enacting and compiling reports on e-safety incidents and ensuring that they are logged where appropriate.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place and that staff are trained and advised on e-safety issues.
- Liaising with school ICT technical staff.
- Reporting regularly at each e-safety Committee

Teaching and Support Staff are responsible for ensuring:

- They have an up-to-date awareness of e-safety matters and of the current school e-safety policies and procedures, including those related to the use of digital devices.
- They have read, understood and signed the school's Staff Acceptable Use Policy for Staff.
- They report any suspected e-safety misuse or incidents to the e-safety Coordinator
- Digital communications with pupils (including email) are on a professional level and only carried out using official school accounts and systems.
- E-safety is part of curriculum planning or other school activities where relevant.
- They help pupils understand and follow the school e-safety rules and AUP.
- They monitor ICT activity in lessons, extra-curricular and extended school activities.
- In lessons where internet use is pre-planned, they guide pupils to sites checked as accessible through the school systems and suitable for their use; and that they report any unsuitable material that is found.
- Their personal behaviour does not put them, their pupils, the school or their professional reputation at risk.

Pupils are responsible for:

- Understanding, signing and adhering to the relevant Acceptable Use Policy
- Doing everything they can to keep themselves safe.
- Doing everything they can to keep others safe.

Parents/Carers are responsible for:

- Understanding, signing and adhering to the relevant Acceptable Use Policy
- Supporting their child in the safe and reasonable use of digital technology
- Alerting the school to any concerns they may have about their own child or any other member of the school community.

The Director of ICT is responsible for supporting the school's implementation of the e-safety policy and ensuring reasonable and safe use of digital technology is accessible by the entire community.

The Network Administrator is responsible for ensuring the network, remote access and email are functional and regularly monitored, in order that reasonable and safe use of digital technology is accessible by the entire community.

PART II: ACCEPTABLE USE POLICIES

Acceptable Use Policies exist to ensure safe, responsible use of IT resources both in and out of school. It is essential that all staff and students adhere to these policies, and thus they must read, understood and sign the relevant AUP. Parents are expected to understand, endorse and support their child(ren)'s adherence to the relevant AUP.

PART III: GENERAL ONLINE SAFETY

General online safety … specifically cyberbullying, monitoring of use, Bring Your Own Device (BYOD) and responsible use of social media.

- **CYBERBULLYING**

    - Bullying is not tolerated at the School: every person has the right to feel safe and secure. All members of school staff should be alert to the possibility of signs of bullying, including cyberbullying. Cyberbullying can be (but is not limited to): intimidation and abuse via electronic means (text, e-mail, social networking sites).

        - To counter cyber-bullying, pupils must be made aware that:
        - They must never share their password with anyone
        - They must not send pictures of others electronically
        - No pupil is allowed to take pictures or video on their phone of another pupil or member of staff, whether on school premises or not.

    - Further information about cyberbullying and bullying in general is here: ***Anti-bullying Policy Whole School***.

- **MONITORING OF USE**

    - Monitoring is done by IMPERO, which will be effective across the sites from September 2018. Impero alerts are sent to relevant staff members …

    - All internet connectivity is filtered under a categorised system, for user groups pertaining to "All staff", Pre-sixteen" and "Post-sixteen", listed at ***Internet Filtering Categories***. In line with the "Prevent" duty, it is imperative all students are safe from terrorist and extremist material when accessing the internet within the school's systems.

    - The Filtering Committee will make decisions regarding access via the network to international sites, including – but not limited to – social media sites in Russia and China. Boarding students must be able to communicate via social media with their families at home, but this need does not override the necessary safeguards that must be satisfied for implementation of an app or programme into the system.

    - Students will receive e-safety help and instruction as part of the wider school curriculum, but may contact a member of school staff for help and advice, or make them aware of any concerns or issues as appropriate.

- **BYOD**
    - Digital technology is a reality in the classroom and LVS recognises the advantage in allowing students online access via their personal devices (BYOD). There is a specific BYOD policy found at this link: ***LTC Bring Your Own Device Policy***.

- **SOCIAL MEDIA**

    - Social Media is a part of life; members of the school community are no exception. The LTC has a specific policy about the responsible use of social media which provides common-sense guidelines and recommendations for using social media responsibly and safely. The policy is at this link: ***LTC e-Content and Social Media Policy***

PART IV: DATA PROTECTION

Implementation of the e-safety Policy and associated policies falls under the auspices of the LTC Data Protection Policy, found here: ***LTC Data Protection Policy*** and the LTC Data Protection Breach Policy, found here: ***LTC Data Protection Breach Policy.*** All staff must complete the LTC Modules on GDPR to ensure fully understanding and compliance with the relevant aspects of this directive.

Last reviewed:	**04.12.2018**
Reviewed by:	**Nigel Beales**
Review no later than:	**04.12.2019**