Registered Charity No. 230011

Effective Date: 17th September 2018	Title: Acceptable Use Policy
	Pages: Page **1** of **17**
Supersedes Date: 14th December 2017	Originator: A. McGarry

PURPOSE

The appropriate use of the email system, the internet and network within the Charity is essential, as it facilitates effective communication and improves efficiency. Used correctly, it is a facility that is of assistance to many employees, stakeholders and users. Its inappropriate use, however, causes many problems ranging from minor distractions to legal claims against the Organisation. This policy sets out the Organisation's view on the correct use of these facilities and explains how this can be achieved, as well as the Organisation's response to inappropriate use.

PROCEDURE

Authorised Use for staff

The email system, the internet and network are available for communication on matters directly concerned with the business of the Charity and the Schools. Employees using these systems should give particular attention to the following points.

1. **The standard of presentation.** The style and content of an email message, learning platform, social networking posting or blog must be consistent with standards that the Charity and the Schools expect from written communications.

2. **The extent of circulation.** Email messages should only be sent to those employees for whom they are particularly relevant.

3. **The appropriateness of email.**

    a. Email should not be used as a substitute for face to face communication; If a decision is made in a face to face conversation a follow-up email confirming the decision should be sent.

    b. "Flamemails" (emails that are abusive) or "trolling" on social networking posts can be a source of stress and can damage work relationships. Hasty messages, sent without proper consideration, can cause misunderstandings.

4. **The visibility of email, learning platform, social networking postings or blogs.** If the message is confidential, the user must ensure that the necessary steps are taken to protect confidentiality. The Charity and Schools will not be liable for any defamatory information circulated either within the Charity and the Schools or to external users of the system.

5. **Data Protection.** All users shall have read, understood and accepted the Data Protection Policy. The information you access is provided on a priviledged basis, is secure, audited and should not be reproduced outside of our networks, unless specifically authorised. This includes printed information.

6. **External access to networks and services**. You may be required to access the network or services remotely. Please see the section Appendix 5 Remote Access on how to access, operate and keep the information you access secure.

7. **Email contracts**. Offers or contracts transmitted via email are as legally binding on the Organisation as those sent on paper and must not be entered into without appropriate prior authorisation.

Guidance and responsibilities are also detailed in the Social Media Policy
Any failure to follow these guidelines and policies satisfactorily, may result in disciplinary action including summary dismissal.

Authorised Use for other users

Users who are not staff, students or trustees may be granted access to portions of our network, internet and email, provided they sign and agree to the terms of this acceptable use policy.

Unauthorised Use

1. The Charity will not tolerate the use of the system for any of the following: (this is not an exhaustive list)

    a. Any message that could constitute bullying or harassment (e.g. on the grounds of sex, race, disability or sexual orientation)
    b. Personal use, e.g. social invitations, blogs, personal messages, jokes, cartoons or chain letters
    c. Joke email forwarding. Such emails may cause offence and are a common source of computer viruses which can cause damage to the Organisation's systems.
    d. On-line gambling and gaming
    e. Accessing pornography
    f. Being in possession of downloading or distributing copyrighted information, files and/or software.
    g. Posting confidential information about other employees, the Charity, the Schools or its members

Any unauthorised use of email or the Internet may result in disciplinary action including summary dismissal.

Implementation of the Policy

1. The Director ICT will be available for advice on all aspects of the policy.

2. All staff will be trained to use the email system, learning platform, the internet and network on an in-house basis. Line managers are required to ensure that all new employees are aware of the policy and are trained in the use of the email and internet system.

3. The Charity reserves the right to monitor email, server logs, instant messaging communications and any other network communication under specific circumstances. Printed copies of messages may be used as evidence in disciplinary proceedings.

4. All users will be asked to create a password on their first login to the network *(please see appendix 2 for guidance on passwords and security)*. Passwords must always be kept confidential to the user. Access to the system using another user's password is a breach of this policy and may result in disciplinary action.

5. Users must ensure that critical information is not stored only within the email system. If necessary, documents must be password protected.

6. Users are required to be familiar with the requirements of the Regulation (EU) 2016/679 (the General Data Protection Regulation, or "GDPR"), The Privacy and Electronic Communications (EC Directive) Regulations 2003 (or "PECR"), Communications Act 2003, Computer Misuse Act 1990, Data Protection Act 2018, Copyright, Designs and Patents Act 1998 (& Copyright and Trade Marks (Offences and Enforcement) Act 2002), Protection from Harassment Act 1997, Protection of Children Act 1978 (and 1999 amendment), Sexual Offenses Act 2003, Obscene Publication Acts 1969 and 1964 and Public Order Act 1986 (and 1994 amendment), Digital Economy Act 2010 and to ensure that they operate in accordance with the requirements of these acts or related acts.

7. Employees who feel that they have a cause for complaint as a result of email communications should raise the matter initially with their immediate line manager. If necessary the complaint can then be raised through the Grievance Procedure.

8. There are guidance notes in appendix 1 of this document, which advise on best practice when compiling emails, and appendix 3 guidance on preventing viruses and spyware. Please note that these notes form part of this policy document.

ACCEPTANCE

I have read and understood this document and agree to comply with the policies that this document defines, by signing the below agreement. The Licensed Trade Charity, reserves the right to modify this policy or any related policies at any time without prior notice.

Signed: .....

Print: .....

Date: .....

APPENDIX 1

Guidance notes on the use of email, internet and networks

1. Use of organisational email is encouraged

The organisation encourages the use of email for work-related activities and respects the privacy of users.

2. Communications, in relation to email, learning platform, social networking or other media, is to be used for job-related and professional purposes only (with specific exceptions listed below)

Line Managers have a duty to ensure that IT investments and resources are being used for appropriate purposes and that additional investments are not required to support non-work related activities.

Permission to send email to all email users is limited to 90 recipients, any message over this limit is defined as “mass-mailing”; mass-mailing must be approved by either the SMT of the school or a member of the executive team. To reiterate, use of mailing lists such as “All Staff Ascot Hassocks and Oxford” may only be used with approval of the individual email by a member of SMT or the executive committee. Smaller mailing lists such as “English Dept” or “All Junior School Teachers” will still be allowed.

Hard limits are in place once you exceed your 2Gb email limit, where you will not be able to send or receive any further emails until you have reduced your emails below the 2Gb limit.

Training documentation is available on how to housekeep your email data located here *IT Training - 6 Tips to help you reduce the size of your inbox*

The Organisation accepts that there may be some exceptions to the above restrictions:-

I. urgent or emergency emails. Taking a common sense analogy of phone usage, the urgent or emergency email would include anything that you would normally expect to be allowed (by your line manager) to conduct by phone.
II. use of organisation computing resources for personal use is allowed for colleagues, so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity.

3. Communications are not routinely monitored on a regular basis, but random spot checks will operate as detailed in our e-Safety monitoring policy. Management also reserves the right to monitor communications under specific circumstances

Subject to the requirements for authorisation (specified below), the organisation may deny access to its email services and may inspect, monitor, or disclose email, instant messaging, social networking or other communications where such activities are required to carry out the following:

- preventing or detecting criminal activity
- preventing the unauthorised use of the computer systems - i.e. ensuring colleagues do not breach the organisation's acceptable use policy
- recording evidence of business transactions
- ensuring compliance with regulatory or self-regulatory guidelines
- maintaining the effective operation of the organisation's systems (e.g. preventing viruses or spam)

In order to conduct any of the activities above, prior documented approval is required from any one of the following:-

- Chief Executive LTC
- A Director of the LTC
- Head Teacher LVS Senior School
- Head Teacher LVS Junior School
- Head Teacher LVS Hassocks School
- Head Teacher LVS Oxford School
-

4. There are some recommended rules for communicating via email and other electronic communication tools

As you write email, be sure to use formality appropriate for the situation and realise that emails, like print, are permanent.

To use email effectively, you should know the basics of netiquette - etiquette on a network.

- Take care with your writing style. Although email is informal, don't embarrass yourself by sending messages that you have not proofread. Text-editing functions on email systems are more limited than in Word. Use uppercase and lowercase letters as you do in other forms of correspondence - UPPER CASE GIVES THE IMPRESSIONS THAT YOU ARE SHOUTING.

- Skip lines between paragraphs.

- Mail should have a subject heading which reflects the content of the message.

- If you think the importance of a message justifies it, immediately reply briefly to let the sender know you have received it, even if you will send a longer reply later.

- Do not send large amounts of unsolicited information to people.

- Messages and articles should be brief and to the point. Don't wander off-topic, don't ramble and don't send messages solely to point out other people's errors in typing or spelling. When someone makes a mistake - whether it is a spelling error, a stupid question or an unnecessarily long answer - be kind about it. If it is a minor error, you may not need to say anything.

- Avoid sending messages or posting articles which are no more than gratuitous replies to replies.

- When quoting another person, edit out whatever is not directly applicable to your reply. Don't let your mailing automatically quote the entire body of messages you are replying to when it's not necessary. Take the time to edit any quotations down to the minimum necessary to provide context for your reply. Nobody likes reading a long message in quotes for the third or fourth time, only to be followed by a one line response: "Yeah, me too."

- Pay attention. Read all outgoing email carefully, checking for errors in both grammar and spelling. Be professional and careful what you say about others. Email is easily forwarded.

Other forms of communication, including (but not limited to) blogs, SMS, Instant Messaging, forum based threads, chat can be handled with a little less formality, but be aware that etiquette is still the key to careful communication, together with knowing the wider implications of shared messages reaching a greater population then you may at first intend!

5. User responsibilities

This Policy specifies the actions permitted and prohibited for users of the Organisation's email and internet services.

By using our services you agree to comply with our policies. You are expected to use the services with respect, courtesy, and responsibility, giving due regard to the rights of other service users. We expect you to have a basic knowledge of how the service functions, the types of uses that are generally acceptable and the types of uses that are to be avoided. Common sense is the best guide as to what is

considered acceptable use.

The following are unacceptable uses. Illegal activities in any form, including but not limited to:

- unauthorised distribution or copying of copyrighted software (which includes freeware, shareware and public domain software) or other copyrighted material
- harassment
- fraud
- trafficking in obscene material
- drug dealing
- violation of U.K. export restrictions

The provisions of this Policy are intended as guidelines and are not intended to be exhaustive. Generally, conduct that violates law, regulation, or the accepted norms of the Internet community, whether or not expressly mentioned in this Policy, is prohibited.

The user acknowledges that the Organisation is unable to exercise control over the content of the information passing through the Organisation's Network. Thus the Charity and Schools are not responsible for the content of any message whether or not the posting was made by a user of the Organisation. You as the user must state this in your description fields in any social media account associated with the organisation.

The user may not circumvent user authentication or security of any host, network, or account (referred to as "cracking", "hacking" or "proxy avaiodance"), nor interfere with service to any user, host, or network (referred to as "denial of service attacks").

Violations of system or network security are prohibited, and may result in criminal and civil liability. The Organisation will investigate incidents involving such violations and will involve and co-operate with law enforcement if a criminal violation is suspected.

Examples of system or network security violations include, without limitation, the following:

- Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorisation of the owner of the system or network

- Unauthorised monitoring of data or traffic on any network or system without express authorisation of the owner of the system or network

- Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks

- Forging of any IP packet header or any part of the header information in an email or a newsgroup posting

- Forging or manipulation of data

- Unauthorised attempt to mask your network traffic through use of anonymity software or proxy redirection

When the Organisation becomes aware of an alleged violation of this Policy, a thorough investigation will be undertaken. During the investigation the Organisation may restrict users' access in order to prevent further potential unauthorised activity. Depending on the severity of the violation, the Organisation may, at its sole discretion, restrict, suspend, or terminate users' accounts and/or pursue other civil remedies. If such violation is a criminal offence, the Organisation will notify the appropriate law enforcement department of the violation.

- It is explicitly prohibited to send unsolicited bulk mail messages ("junk mail" or "spam") of any kind (commercial advertising, political tracts, announcements) etc.

- It is explicitly prohibited to permit others to send unsolicited bulk mail messages either directly or by relaying through the user's systems. Users may not forward or propagate chain letters nor malicious email.

- A user may not solicit mail for any other address other than that of the user, except with full consent of the owner of the referred address.

- A user is explicitly prohibited to share their password, logon details or allow any other user to use their logon details, unless specific access is requested through HR procedures sanctioned by the Chief Executive.

- You shall be held liable for any and all costs incurred by the Organisation as a result of your violation of these terms and conditions.

APPENDIX 2
Guidance on Passwords and Security

The security of information within the organisation is of the highest priority. All personnel who work in or for the organisation including Licensed Trade Charity, Licensed Victuallers' Schools are instructed to read, understand and follow this policy.

Password security

Passwords should be at least 8 characters in length and consist of both alphabetic upper and lowercase, numeric or special characters. Current best practice is to use passphrases rather than passwords, which facilitate longer more secure passwords which are easy to remember. Upon changing your password please use a different password, as the system will remember your last three passwords.

Unattended PCs

Users shall not leave a PC unattended. If you need to leave a PC for a short period of time, ensure that you have LOCKED the PC *(Activated by pressing **<CTRL-ALT-DELETE>** keys together and clicking the **"LOCK workstation"** button)*.

If you must leave the PC unattended for a lengthy period of time please ensure that you save all current documents and close all applications before **"LOGGING-OFF"** the PC.

PLEASE NOTE: Any person utilising a shared machine who leaves it in a LOCKED state for a lengthy period of time, will find that a systems administrator policy will log the machine off, effectively losing all work open in the current session. (Please have consideration for other users, as well as the security of information).

Administrator Security

System, network or PC administrators' security: All persons with access to an administrator password for any network or PC within the organisation are advised never to leave a PC unattended for the reasons stated above. This is especially important since administrator accounts can have unlimited access to information and user-related security, presenting the opportunity for hacking and sensitive information disclosure.

Please note: Administrator access and privileged use by an administrator is logged thoughout the organisation's networks.

Any administrator who does not adhere to this policy will be subject to disciplinary action.

Virus Security

Virus prevention is of high priority. Antivirus alerts and signs of virus infection should never be ignored, but reported immediately to IT Services. Listed below are some definitions and vectors of infection to help users understand where they occur:

Definitions

- Virus: A program that attaches itself to a "host" program, and can cause damage to hardware, software, and files.
- Worm: A stand-alone, self-replicating program that invades computers and consumes memory, thus causing a computer to crash.
- Trojan horse: A computer program that appears to be useful but conceals an unexpected function, which is typically damaging.

Vectors of Infection
The pathways used to spread a virus include:

- Email attachments through Outlook Express and Outlook
- Web based email, such as Hotmail, Gmail
- Accessing files or links via social networking sites
- File and network sharing
- Visits (intentional or unintentional) to malicious web sites
- Downloads of untrusted code or software programs, from unknown or untrusted sites

Laptop Security

Laptop users / owners also please refer to "Laptop protection policy"

APPENDIX 3

General guidance on Spyware and Viruses

Spyware Cleaning

SPYWARE is a generic term for software whose purpose is to collect demographic and usage information from your computer, usually for advertising purposes. The term is also used to describe software that 'sneaks' onto the system or performs other activities hidden to the user. Spyware applications are usually bundled as a hidden component in mislabelled "freeware" and “shareware” applications downloaded from the Internet. Spyware may be active on your computer at this moment without your knowledge. Spyware is almost always installed on the system secretively, suggesting that spyware companies know how users feel about such software and conclude that the best way to ensure its widespread use is to prevent the end-user from discovering it.

The charity and school’s use a combination of software from Palo Alto Networks and Microsoft to control spyware.

Viruses

You must prevent intentional intrusions into your computer and network that take the form of viruses. Follow these tips to help prevent virus outbreaks

- You can unwittingly bring viruses into the network by loading a program from a source such as the internet, instant messaging or email attachments.

- Learn the common signs of viruses: unusual messages that appear on your screen, decreased system performance, missing data, and the inability to access your hard drive. If you notice any of these problems on your computer, run your virus-detection software immediately to minimise the chances of losing data.

- Programs on floppy disks or other removable media may also contain viruses. Scan all media before copying or opening files from them, or starting your computer from them.

- You can run Microsoft Defender (which is installed on your computer) regularly to check your computer for viruses. Your laptop is configured to scan your local hard disks every day.

Update of spyware signature files, virus signature files and engine

Your system is set to automatically download the updates from the network. If you have a laptop and have not connected to the network for longer than a week,

please ensure you contact the IT helpdesk to obtain a recent update before reconnecting to the network.

Warning: Non-compliance with this procedure, is liable to cause damage to the network and its users. It is your responsibility to maintain standards in compliance with this policy.

APPENDIX 4

Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

Social Engineering

Staff should be aware of the risks of 'Social Engineering' where they may be manipulated for the purposes of compromising security, or gaining access to confidential information. Often this will take the form of an innocent sounding request for basic information via the telephone or e-mail, but this information can then form the next stage of an attack. When combined together different pieces of seemingly unimportant information provided by several different people within the organisation can become critical.
To mitigate this risk staff should give careful consideration of any request for information, even if it may not be obviously sensitive. If in doubt refer the request to your line manager or director.

Appendix 5

Remote Access

Remote access, is granted in a priviledged basis, for which guidance is provided across training documents, designed to help you access, operate and keep the information you access secure.

For help and assistance in using our different forms of remote access effectively, please read this guide.

Please note: Always consider data protection and information security. Access to remotely print has been restricted under our Data Protection Act 2018 and General Data Protection Regulation requirements.

To print from the remote desktop service, please print to the Xerox Pullprint, which will be saved in a queue for a 72 hour period and can be retrieved when you next log-in to a Xerox unit on any of our sites.

APPROVAL/CHANGE FORM

Approval/Change Form

ORIGINATOR: _____ SIGNATURE: _____
(BLOCK CAPITALS)

WITHIN DEPT.:

REVIEWED BY:	POSITION:	DATE:
_____	_____	_____
_____	_____	_____

EXTERNAL TO DEPT.:

REVIEWED BY:	POSITION:	DATE:
Adrian McGarry	Director ICT	
_____	_____	_____

REVISION NO.	REASON FOR REVISION	**EFFECTIVE DATE**	**Reviewed by**
12	**Adjustment for inclusion of e-Safety Monitoring**	**19 July 2013**	**ACM/JF**
13	**Yearly review and font change**	**18 August 2014**	**ACM**
14	**Addition of LVS Oxford**	**19 Dec 2014**	**ACM**
15	**Legal checking, changes to related policies**	**14 April 2015**	**ACM**
16	**Updates for anonymity,proxy use**	**25 Aug 2015**	**ACM**
17	**Addition of Appendix 4 Social Engineering**	**05 Nov 2015**	**ACM**
18	**Change of logo**	**17 Feb 2016**	**ACM**
19	**Annual Review**	**22nd August 2016**	**ACM**
20	**Annual Review**	**15th August 2017**	**ACM**
21	**Amended Oxford head**	**14th December 2017**	**ACM**
22	**Seperated this AUP from LVS AUP**	**17th September 2018**	**ACM**

Effective Date: 17th September 2018
Reviewed no later than: 16th September 2019