E-Safety Policy
(Staff use of computers, email & internet)

Orchard Education Ltd
1 Sargon Way
Great Grimsby Business Park
GRIMSBY
North East Lincolnshire
DN37 9PH

01472 898498

COMPANY POLICY

We make computers, computer equipment, internet services and email available to our employees as a business tool to help them perform their job role more effectively. Whilst we acknowledge the benefits that the use of such technology can have for our organisation, it is vital that it is used reasonably, professionally and for appropriate purposes. This policy sets out rules for the use of computers, email and the internet and explains our monitoring of such systems. The rules in this policy are very important and as such we expect them to be complied with at all times. A serious violation of this policy may result in summary dismissal for gross misconduct.

PERSONAL USE

You are strictly forbidden from using Company computers, software and computer equipment for personal use. You should not use our computer systems, internet services or Company email account for any matter you wish to be kept private from the Company.

SECURITY

The security of our systems and data is of great importance to the Company. If it is compromised it could harm our business or expose it to the risk of harm. To prevent this from occurring, you are required to comply with the security measures detailed below.

UNAUTHORISED SOFTWARE

Software other than that provided by the Company is not to be downloaded or installed onto Company computers unless specifically authorised by your manager.

EXTERNAL DEVICES AND EQUIPMENT

No external devices or equipment should be attached to our computers or computer equipment without the prior approval of your manager.

COMPUTER VIRUSES

Whilst the Company has anti-virus software and spam filters in place, it is still expected that employees will take reasonable care to ensure that our systems do not become infected. If you are suspicious that an email or an attachment may have a virus, you should not open it. You should report it to your manager immediately. If you become aware of a virus or any other programme in our computer system that could cause harm, whether to the computer system itself, its security or our data, you must report this immediately to your manager.

SMARTPHONE AND TABLET APPLICATIONS

If you have been provided with a smartphone or other portable internet enabled device, you must not download or install any applications on to it without authorisation from your manager. Any applications you are authorised to download must be obtained from an approved source, irrespective of their availability elsewhere.

CONFIDENTIAL PASSWORDS

Passwords are confidential and must not be given to another person without prior permission from your manager. If you are preparing to leave your position with this Company for any reason (for example because you have resigned), you must immediately make any passwords used in the course of your employment known to your manager.

SECURING YOUR COMPUTER TERMINAL /COMPUTER DEVICE

You are required to secure your computer terminal if you are leaving it unattended. You must either log off or lock your system. This is to maintain the security of our systems and data. If you are using a laptop computer or any other mobile computing device it is your responsibility to ensure that it is kept secure at all times. Particular care must be taken whilst away from the workplace. All mobile computing devices must be password protected. When it is not actively in use, you must switch off or lock your device to prevent unauthorised access being gained to our systems or data. In the event of loss or theft of a device, you must report this immediately to your manager.

You are permitted to use memory sticks to store information when it is required by your role or by the Company. Any information stored on a memory stick must be secure; this means it must be password protected with a strong password. You are responsible for ensuring that the memory stick is not lost or stolen whilst in your possession. If loss or theft does occur, you must immediately report this to your manager and provide a description of the information on the device.

MODIFICATION OF COMPANY EQUIPMENT

You must not make any modifications to computer equipment or computer software (including removing software) without first obtaining permission from your manager.

USE FOR PROHIBITED CONDUCT

The Company's computers and computer equipment are provided for the legitimate business purposes of this Company. As such, their use for prohibited conduct will be treated very seriously and may result in your dismissal without notice. The examples of prohibited conduct detailed below are non-exhaustive. The Company strictly prohibits the use of our computers, computer equipment, office equipment, email or internet systems to **access, view, create, post, download, store, send, print, copy or distribute:**

- Illegal material;
- Pornographic material of any kind or material of a sexual nature;
- Obscene material;
- Discriminatory, defamatory, harassing, derogatory or insulting material;
- Offensive material (that is material likely to cause offence, upset or embarrassment if it is received, seen or discovered to have been accessed);
- Confidential or sensitive Company material unless authorised to do so.

The following actions are also prohibited:

- Generating or otherwise participating in the distribution of a virus;
- Copying software;
- Using Company programs and software for any unauthorised use;
- Using Company software or design programs for unauthorised use;
- Uploading, downloading, opening or distributing unauthorised software;
- Infringing the trademark and/or licencing rights of this Company or any other individual or organisation;
- Infringing the copyright of any individual or organisation.
- Allowing unauthorised staff/learners to access your device
- Not locking devices when left unattended

EMAIL

The Company recognises that email is a useful business tool. However, it is crucial that it is used in a professional manner at all times, whether being sent from a computer or mobile computing device such as a smartphone or tablet. All employees are required to comply with the rules set out below. At no time should email be used for Prohibited Conduct.

APPROPRIATE USE OF EMAIL

You should correspond by email only when it is appropriate for you to do so. In any email sent in the course of employment you must ensure that:

- The tone and content is appropriately professional;
- You identify yourself in an appropriate manner;
- You include the Company's standard disclaimer when sending emails.

CONFIDENTIAL INFORMATION

You are responsible for ensuring that you do not use email to reproduce, replicate, duplicate or distribute confidential or sensitive Company information to an inappropriate party. You are strictly prohibited from transferring confidential or sensitive information to your personal email account.

CREATING CONTRACTUAL COMMITMENTS

It is important to remember that contracts and contractual obligations can be created by email. You must not create a contract or any contractual obligations with a third party unless it is the Company's intention to do so and you have the appropriate authority. If you require further information regarding this, please contact your manager.

USE OF EMAILS IN COURT PROCEEDINGS

Emails can be disclosed in legal proceedings. Employees must bear this in mind when drafting, responding to or forwarding emails. Even if emails are deleted, it is likely that they are recoverable and as such capable of being disclosed.

GROUP EMAILS

If you are sending a group email to clients/potential clients (for example for marketing purposes) you must ensure you protect the confidentiality of our client list and the privacy of clients/potential clients.

JOKES

Using email for the receipt and distribution of jokes and banter is not permitted. Email is one of the least secure methods of communication. What may seem like a joke to you may be offensive to someone else.

JUNK MAIL (SPAM) AND CHAIN EMAILS

Sending and responding to junk email chain letters/emails is forbidden.

POLITICAL AND CHARITABLE DONATIONS

You are prohibited from using email to request or respond to a request for political or charitable donations.

MANAGING YOUR EMAIL ACCOUNT

It is your responsibility to ensure that you have sufficient space in your 'Inbox' to enable you to receive emails at all times. You should regularly electronically archive old emails to ensure that your email account is able to function efficiently. You must use the 'out of office' function on our email system when you are out of the office. If you are unsure who to forward your emails to in your absence, contact your manager. The 'out of office' message received by those who contact you must be professional. It should include the following information the date/time when you will next be contactable and who will be dealing with your emails in your absence. If necessary for business purposes, the Company may access your emails in your absence.

INTERNET

The Company provides internet access as a tool to assist employees to perform their roles. It must be used in a reasonable and professional manner at all times. You must not engage in any Prohibited Activity, or act in a manner which breaches any Company policy or term. It should be remembered that 'cookies' and similar tracking devices may be left on website visits and these can be traceable to the Company. As such you must not visit any websites or carry out any activity on the internet which would be inappropriate in a business environment.

If, as part of your role you are permitted to make 'postings' (or carry out similar actions) on the internet on behalf of the Company, you will receive additional guidance from your manager regarding what is and what is not acceptable to the Company. Any

breach of this part of the policy will be treated seriously and may result in your dismissal. The Company reserves the right to block access to any website it deems inappropriate for employees to access using its systems.

WATCHING LIVE TELEVISION ON THE INTERNET

This Company does not hold a television license. As such you are strictly prohibited from watching or recording live television at our premises using our equipment.

INTERNET GAMBLING

At no time are employees permitted to use the Company's computers, computer equipment or internet to participate in on line gambling of any kind.

MONITORING

Use of our computers and IT systems (including internet and email) are monitored. This also includes personal use of them. Monitoring is carried out lawfully and to the extent that it is necessary for business purposes. To ensure monitoring is justified, the Company has carried out an impact assessment. The Company reserves the right to carry out monitoring for the following (non-exhaustive) purposes:

- To prevent or detect crime;
- To comply with any legal obligations;
- To monitor compliance with this policy;
- To ensure compliance with Company procedure;
- To monitor the quality of work;
- To investigate alleged or suspected wrongful acts;
- To secure effective system operation.

Monitoring is carried out using automated software. Monitoring can consist of random spot checks. Monitoring of emails is usually confined to address or heading, unless it is necessary for good reason to access the content. The directors have authority to carry out monitoring.

Information obtained by monitoring may be used as part of disciplinary, capability or other Company procedures.

Also see Social Media Policy and Safeguarding Policy.

This policy will be reviewed annually by SMT/SLT member or area specific school advisory panel member .

	Initial	Review 1	Review 2	Review 3	Review 4
Signed		Dave Melia	Dave Melia	Dave Melia	L.Griffen
Position		Director	Director	Director	Welfare & Transitions Manager
Date		03.08.17	04/09/2019	30/08/2020	01/09/21