Forfar Education Ltd and Group Schools

ACCEPTABLE USE POLICY

Acceptable use of information technology assets by staff and third-parties

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	28/02/2023	Al Butler	Document first created
0.2	29/03/2023	Al Butler	Added Social Media Guidance
0.3	01/09/2023	Al Butler	Added Mobile Device Guidance
1.0	08/09/2023	Al Butler	Version 1.0 agreed by Al Butler, Jo Storey, Kate Farrell and Christine Pouncett

2 Document Contents Page

3. Acceptable Use of Assets Policy

3.1. Purpose

3.1.1. The purpose of this policy is to make employees and external party users aware of the rules for the acceptable use of assets associated with information and information processing.

3.2. Scope

3.2.1. All employees and third-party users.

3.3. Principle

3.3.1. Use of assets is in line with applicable legislation, company policies and is in place to safeguard the company data, employees, and customers. Each user is to be responsible for their own actions and act responsibly and professionally.

3.4. Individual Responsibility

3.4.1. Access to the IT systems is controlled using User IDs, passwords and/or multi-factor authentication tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the company IT systems.

3.4.2. Individuals MUST NOT:

3.4.3. Allow anyone else to use their user ID/ multi-factor authentication token and password on any company IT system.

3.4.4. Leave their user accounts logged in at an unattended and unlocked computer.

3.4.5. Use someone else's user ID and password to access company IT systems.

3.4.6. Leave their password unprotected (for example writing it down).

3.4.7. Perform any unauthorised changes to company IT systems or information.

3.4.8. Attempt to access data that they are not authorised to use or access.

3.4.9. Exceed the limits of their authorisation or specific business need to interrogate the system or data.

3.4.10. Connect any non-company authorised device to the company network or IT systems.

3.4.11. Use any non-company authorised software, devices or services to carry out business activities and communications.

3.4.12. Store company data on any non-authorised company equipment.

3.4.13. Give or transfer company data or software to any person or organization outside the company without the authority of the company,

3.4.14. Line managers must ensure that individuals are given clear direction on the extent and limits of their authority about IT systems and data.

3.5. Internet and Email Usage

3.5.1. Use of the company internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the company in any way, not in breach of any term and condition of employment and does not place the individual or the company in breach of statutory or other legal obligations.

3.5.2. All individuals are accountable for their actions on the internet and email systems.

3.5.3. Individuals must **not**:

3.5.3.1. Send or store payment card information such as:

3.5.3.1.1. Payment card number (Primary Account Number or PAN)

3.5.3.1.2. Security code (CVV2 etc.)

3.5.3.1.3. Start and expiry dates

3.5.3.2. Use the internet or email for the purposes of harassment or abuse.

3.5.3.3. Use profanity, obscenities, or derogatory remarks in communications.

3.5.3.4. Access, download, send or receive any data (including images), which the company considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libellous material.

3.5.3.5. Use the internet or email to make personal gains or conduct a personal business.

3.5.3.6. Use the internet or email to gamble.

3.5.3.7. Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.

3.5.3.8. Place any information on the Internet that relates to the company, alter any information about it, or express any opinion about the company unless they are specifically authorised to do this.

3.5.3.9. Post comments about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.

3.5.3.10. Send unprotected sensitive, internal, or confidential information externally.

3.5.3.11. Forward the company mail to personal (non-company) email accounts (for example a personal cloud or owned domain account).

3.5.3.12. Make official commitments through the internet or email on behalf of the company unless authorised to do so.

3.5.3.13. Download any copyrighted material such as music media (MP3) files, film, and video files (not an exhaustive list) without appropriate approval.

3.5.3.14. In any way infringe any copyright, database rights, trademarks, or other intellectual property.

3.5.3.15. Download or install or distribute any software from the internet without prior approval of the IT Department.

3.5.3.16. Connect the company devices to the internet using non-standard connections.

3.6. Personal Mobile Phone Usage Guidelines

3.6.1. It is not the company policy to allow 'bring your own device' or use of personal mobile devices by default except in the following circumstances:

3.6.1.1. Personal Mobile Phones must be switched off and not accessed in school areas, apart from staff rooms/break facilities. Apart from to access a Multi-factor authentication prompt.

3.6.1.2. All mobile phones are banned from use within EYFS rooms.

3.6.2. For further guidance in school environments please see the school Mobile Device Policy

3.7. Social Media Responsible Usage Guidelines

3.7.1. You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal e-mail address.

3.7.2. Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

3.7.3. If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views do not represent those of your employer (unless you have been authorised to speak on our behalf). You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

3.7.4. If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager.

3.7.5. If you see social media content that disparages or reflects poorly on us, you should contact your line manager.

3.8. Working Off Site

3.8.1. It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

3.8.1.1. Working away from the office must be in line with the company remote working policy.

3.8.1.2. Laptop and mobile device encryption must be used.

3.8.1.3. Laptop and mobile devices must also be protected at least by a password or a PIN.

3.8.1.4. Equipment and media taken off-site must not be left unattended in public places including on public transport and not left in sight in a car.

3.8.1.5. Laptops and mobile devices must be carried as hand luggage when travelling.

3.8.1.6. Information should be protected against loss or compromise when working remotely (for example at home or in public places).

3.9. Mobile Storage Devices

3.9.1. Mobile devices such as memory sticks, CDs, DVDs, and removable hard drives are not to be used unless authorised. Only company owned, managed, and authorised mobile storage devices with encryption enabled must be used, when transferring internal or confidential data.

3.10. Monitoring and Filtering

3.10.1. All data that is created and stored on company computers is the property the company and there is no official provision for individual data privacy,

however wherever possible the company will avoid opening personal emails.

3.10.2. IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. The company has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, ensuring efficient businesses processes, to protect against misuse, and to safeguard children.

3.10.3. Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000, and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000, the latest version of Keeping Children Safe In Education (KCSIE), and any other applicable legislation.

3.10.4. This policy must be read in conjunction with:

3.10.4.1. Computer Misuse Act 1990

3.10.4.2. Data Protection Act 2018

3.10.4.3. Keeping Children Safe In Education (latest version)

3.11. Reporting

3.11.1. It is your responsibility to report suspected breaches of security policy without delay to your line management, the IT department, the information security department, or the IT helpdesk.

3.11.2. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with company disciplinary procedures.

4. Policy Compliance

4.1. Compliance Measurement

4.1.1. The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and/or external audits, and feedback to the policy owner.

4.2. Exceptions

4.2.1. Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3. Non-Compliance

4.3.1. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4. Continual Improvement

4.4.1. The policy is updated and reviewed as part of the continual improvement process.

5. Areas of the ISO27001 Standard Addressed

Acceptable Use Policy Relevant ISO27001 Controls Mapping

ISO27001:2022	ISO27002:2022	ISO27001:2013/2017	ISO27002:2013/2017
ISO27001:2022 Clause 5 Leadership ISO27001:2022 Clause 5.1 Leadership and commitment ISO27001:2022 Clause 5.2 Policy ISO27001:2022 Clause 6.2 Information security objectives and planning to achieve them ISO27001:2022 Clause 7.3 Awareness	ISO27002:2022 Clause 5 Organisational Controls ISO27002:2022 Clause 5.1 Policies for information security ISO27002:2022 Clause 5.36 Compliance with policies, rules, and standards for information security ISO27002:2022 Clause 5.4 Management Responsibilities ISO27002:2022 Clause 6 People Controls ISO27002:2022 Clause 6.3 Information security awareness, education, and training ISO27002:2022 Clause 6.4 Disciplinary process	ISO27001:2013/2017 Clause 5 Leadership ISO27001:2013/2017 Clause 5.1 Leadership and commitment ISO27001:2013/2017 Clause 5.2 Policy ISO27001:2013/2017 Clause 6.2 Information security objectives and planning to achieve them ISO27001:2013/2017 Clause 7.3 Awareness	ISO27002:2013/2017 Clause 5 Information security policies ISO27002:2013/2017 Clause 5.1 Management direction for information security ISO27002:2013/2017 Clause 5.1.1 Policies for information security ISO27002:2013/2017 Clause 5.1.2 Review of the policies for information security ISO27002:2013/2017 Clause 7 Human resource security ISO27002:2013/2017 Clause 7.2.1 Management Responsibilities ISO27002:2013/2017 Clause 7.2.2 Information security awareness, education, and training

	ISO27002:2022 Clause 5.10 Acceptable use of information and other associated assets ISO27002:2022 Clause 5.14 Information Transfer ISO27002:2022 Clause 8 Technological Controls ISO27002:2022 Clause 8.1 User endpoint devices		ISO27002:2013/2017 Clause 7.2.3 Disciplinary process ISO27002:2013/2017 Clause 8 Asset Management ISO27002:2013/2017 Clause 8.1 Responsibility for Assets ISO27002:2013/2017 Clause 8.1.3 Acceptable Use of Assets ISO27002:2013/2017 Clause 8.2.3 Handling of Assets ISO27002:2013/2017 Clause 13 Communications Security ISO27002:2013/2017 Clause 13.1 Network Security Management ISO27002:2013/2017 Clause 13.2.1 Information transfer policies and procedures ISO27002:2013/2017 Clause 13.2.2 Agreements on information transfer