Stewards Academy

Parnall Road

Harlow

Essex

CM18 7NQ

POLICY NAME	Acceptable Use of IT Policy - Pupils			**POLICY NO.**	
EFFECTIVE DATE	17/5/23	**DATE OF LAST REVISION**	17/5/23	**VERSION NO.**	3
REVIEW FREQUENCY	Annual				
ADMINISTRATOR RESPONSIBLE	Network Manager		**CONTACT INFORMATION**		
APPLIES TO apply group names to define applicable areas of staff					
GROUP 1		GROUP 2		GROUP 3	
GROUP 4		GROUP 5		GROUP 6	

VERSION HISTORY				
VERSION	**APPROVED BY**	**REVISION DATE**	**DESCRIPTION OF CHANGE**	**AUTHOR**
1	Headteacher	December 2020	Created	
2	Headteacher	January 2021	Reviewed	Optimus
3	Headteacher	March 2023	Review – minimal updates	Optimus
4	Trust Board	17th May 2023	Approved	

Stewards Academy

Acceptable use of ICT policy

Adopted: March 2023 Review date: March 2024

1.1 This policy outlines what are acceptable and unacceptable uses of Information Communications Technology (ICT) facilities within Stewards Academy. It is relevant to pupils, staff, governors and visitors. Whilst we aim to support the full use of the vast educational potential of new technologies we also have a responsibility to provide safeguards against risk, unacceptable material and activities. These guidelines are designed to protect pupils, staff and visitors from e-safety incidents and promote a safe e-learning environment for pupils.

1.2 At Stewards Academy we believe that pupils should be trusted to use digital technologies in a principled and productive way. The general spirit of this policy is about giving everyone the opportunity to make productive decisions in the ways they decide to use digital technologies; we should all be fully engaged in the on-going debate about what responsible digital citizenship means and how we can nurture it within our school.

Acceptable use

2.1 The Academy's ICT facilities should only be used to support learning, teaching, research, administration and approved business activities of the Academy. These services may not be used for personal commercial, political, charitable, and other such activities unless expressly authorised by the Academy.

2.2 Should authorisation be provided permitting other personal, personal commercial, political, or charitable, any such use must not hinder or interfere with an individual's duties and must not prevent the legitimate use of these facilities by others. Users may not use the Academy's ICT facilities to store personal non-work related information or materials on the ICT facilities (e.g. eBooks, music, home videos, photography), and use of the ICT facilities is provided with no expectation of privacy.

2.3 Users should therefore engage in safe computing practices by establishing appropriate access restrictions for their accounts by setting a password for their user account, safeguarding their passwords, backing up files, and promptly reporting any misuse or violations of this policy.

2.4 Users' accounts and passwords must not be shared with anyone. Users are responsible for the security of their passwords, accounts and setting account and file permissions. Disclosure of account or password information may result is disciplinary action.

Monitoring of users

3.1 The Academy may monitor the usage of any or all IT facilities and has access to reports on any internet sites that have been visited. This is irrespective of whether it is for Academy or personal use, and users should have no expectation of privacy when accessing or using IT systems or services.

3.2 Monitoring of ICT facilities is performed:

- To monitor the performance and operation of the ICT facilities;
- To secure, fix, enhance or as an inherent part of effective and responsible systems development or operation;
- To collect evidence pertaining to compliance with this policy, and other related policies, regarding the acceptable use of ICT facilities within the School;
- To investigate or detect unauthorised use of the computing and network facilities of the Academy;
- In the interests of national security, as required by law; and
- To prevent or detect crime, as by required by law.

3.3 The Academy reserves the right to inspect any items of computer equipment connected to the network. Any ICT device connected to the Academy's network will be removed if it is deemed to be breaching Academy policy or otherwise interfering with the operation of the ICT facilities.

3.4 The Academy will designate Authorised Personnel, usually IT services or support staff, to be permitted to engage in monitoring and it will be considered a disciplinary offence for anyone to engage in monitoring activities without proper authorisation or monitor areas outside their areas of responsibility. On the occasions monitoring, especially covert monitoring is required there will be a clear purpose, for example, but not limited to Health and Safety, behaviour/disciplinary, security. Each incident will be assessed via a risk assessment/DPIA prior to the monitoring taking place. The monitoring will conducted under a specific lawful basis (1 of 6) and, if sensitive data is to be captured, a second special category condition (1 of 10). Collecting the data through monitoring will be limited to achieving the purpose that has been specified.

Unacceptable use

4.1 The Academy reserves the right to block, disconnect or otherwise prevent what it considers to be unacceptable use of its ICT facilities. Unacceptable use includes, but is not limited to:

- All actions or activities that are illegal or in conflict with the Academy's policies, procedures and processes;

- Using the ICT facilities for access, creation, modification, storage, download, hosting or transmission of material that could be considered pornographic, offensive, obscene, or otherwise inappropriate, or for placing direct or indirect links to websites which publish or host pornographic, offensive or inappropriate material;

- Publishing materials or making statements which the Academy may deem to be advocating illegal activity, or threatening, or harassing, or defamatory, or bullying or disparaging of others, or abusive, or libellous, or slanderous, or indecent, or obscene, or offensive or promotes unlawful discrimination, breaches copyright or otherwise causing annoyance, or inconvenience;

- Unauthorised production, distribution, copying, selling, hiring, performing of copyrighted material including, but not limited to, digitisation and distribution of computer software, television, radio, streaming services, websites, photographs, magazines, books, music or any copyrighted sources and installation of any copyrighted software for which the Academy does not have an active licence or explicit permission of the copyright owner, is strictly prohibited;

- Authoring or sending any form of electronic communications or messages, including, but not limited to, messages and emails that were unsolicited and may be considered junk mail, "chain letters", "Ponzi", hoax warnings or advertising, and that do not correctly identify you as the sender, or messages which appear to originate from another person;

- Unauthorised transmission, distribution, discussion or disclosure of information gained through a user's presence within the Academy or through the use of ICT facilities;

- Connecting any non-approved ICT device, system or service (including wireless access points) to Academy networks or setting up any network services, without the explicit or delegated permission from Authorised Personnel;

- Unauthorised access (or attempted unauthorised access) to any ICT facilities provided by the Academy;

- Allowing, inciting, encouraging or enabling others to gain or attempt to gain unauthorised access to the ICT facilities;

- Causing any damage to ICT facilities, including through the consumption of food or drink, or moving or removing such facilities without authorisation. The Academy reserves the right to charge for any damage caused;

- Attempting to modify, alter or in any way interfere with ICT facility security controls, hardware or software, configurations, settings, equipment, data files or websites without the written authorisation or delegated permission from Authorised Personnel;

- Introduction of unauthorised and/or malicious software or programs into the ICT facilities, including, but not limited to: unlicensed software, viruses, worms, Trojan horses or logic bombs; by downloading, creating or using any program, tool or item of software designed to monitor damage, disrupt or interfere with the functioning of ICT facilities, user accounts or data;

- Effecting security breaches or disruptions of network communication, including, but not limited to, accessing or modifying data (or data headers) of which the user is not an intended recipient or logging into an ICT system or service, or account, that the user is not expressly authorised to access. Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information;

- Executing any form of network monitoring including any data capture, port scanning or security scanning without written authorisation or delegated permission from Authorised Personnel;

- Registering for any system or service, including, but not limited to, social media accounts, web applications, domain names, which includes the name of the Academy or any similar name, or abbreviation that may mislead the public into believing that the domain name refers to the Academy; and

- Acting in any way that directly or indirectly causes disruption to others' use of Academy ICT facilities, or using ICT facilities to disrupt or deny the use of ICT facilities of third parties at any time.

Remote Access

5.1 Remote access to the Academy network is possible where this has been granted by the ICT Department.

5.2 Remote connections are considered direct connections to the Academy network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy.

Social Media

6.1 As an Academy we recognise that social media and networking are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and blogs for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks. Staff should apply the guidance given in Social Media policies with regard to social networking.

6.2 Social media (specifically Twitter and Instagram) is used for information sharing; marketing and promotion of the school; and celebrating achievement. Learning will be supported through other platforms such as Microsoft Teams and ClassCharts.

Appendix 1 - Acceptable Use Policy Agreement (Secondary Pupils)

I understand that I must use Academy systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

When using the Academy's ICT facilities:

- I understand that the Academy systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have prior permission;
- I understand that the School may monitor my use of the devices, systems, services and communications at any time;
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it;
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc);
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line;
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes);
- I will respect others' work and property and will not access, copy, remove or otherwise use or alter any other user's files, without the owner's knowledge and permission, and I will ensure that any use is in accordance with Academy policies;
- I understand there are risks when using the systems and services, and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials;
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions;
- I will respect copyright of materials and intellectual property rights and not take or distribute text, images or other materials without permission;
- I will not use or modify any of the Academy devices, systems and services in any way that will disrupt their use for others in any way;
- I will not install or attempt to install or store programmes of any type on any Academy device, nor will I try to alter computer settings;
- I understand that I am not permitted to attempt to connect any devices or systems (e.g. laptops, mobile phones, USB devices, etc) to any Academy devices, systems or services without prior permission from an Authorised Person within the Academy. I understand that, if I am permitted to use my own devices in school I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

I understand that I am responsible for my actions, both inside and outside of the School:

- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the Academy and where they involve my membership of the Academy community (for example, cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Academy ICT systems and services, disciplinary action as set out in the codes of conduct and in the event of illegal activities involvement of the police.

I agree to follow these guidelines at all times when:

- using or connected to the Academy's devices, systems and services;
- using my own equipment inside or outside of the Academy in a way that is related to me being a member of this School (for example, communicating with other members of the School, accessing Academy email, websites and services, etc).

I have read and understand that use of the Academy IT systems and devices is governed by the full Acceptable Use Policy, the Safeguarding Policy, the Online Safety policy, the Behaviour Policy and the Data Protection Policy.

Print Name (Pupil)

Signed (Pupil)

Print Name (parent):

Signed (parent):

Date (parent):