ICT ACCEPTABLE USE POLICY

Prepared By:	David Adcock	Date Adopted:	New Policy
Job Title:	IT Lead	Status:	Non-contractual
Authorised By:	Kate Grant	Last Reviewed:	June 2021
Job Title:	CEO	Ratified:	January 2021
Reviewed by:	David Adcock	Next Review date:	December 2021
Job Title:	IT Lead	Version:	2.2

TABLE OF CONTENTS

1. Purpose

1.1 This policy ensures that users understand their responsibility for the appropriate use of Trust's information technology resources. Understanding this will help users to protect themselves and Trust's equipment, information and reputation.

2. Definitions

2.1 "The Trust" means Jigsaw CABAS® School, Jigsaw Plus and Jigsaw Trading 2013 Limited (Café on the Park).

2.2 "ICT facilities" means all IT devices, facilities, systems and services including, but not limited to, network infrastructure, intranet, internet, desktop computers, laptops, iPads and tablets, phones, personal organisers, music players, software, websites, web applications or services and any device, system or service which may become available in the future which is provided as part of the ICT service.

2.3 "Users" are defined as anyone who has access to the Trusts ICT facilities, IT and communication systems either internally or externally.

2.4 "Personal use" means any use or activity not directly related to the users' employment, study or purpose.

2.5 "Authorised Personnel" means employee(s) authorised by the Trust to perform systems administration and/or monitoring of the ICT facilities.

2.6 "Materials" means files and data created using the ICT facilities including but not limited to documents, photographs, audio, video, printed output, web pages, social networking sites, bulletin boards, newsgroups forums and blogs.

3. Scope

3.1 This policy applies to all users, this includes but is not limited to all staff trustees, governors, contractors, volunteers, work experience, consultants, agency workers, visitors. and those using and/or accessing any element of the Trusts IT infrastructure, systems and services, from on or off site

4. The Policy

4.1 This policy should be read in conjunction with associated policies in section 13

4.2 All users are responsible for the success of this policy and should ensure that they take the time to read and understand it and the associated policies. Any unacceptable use should be reported to a manager for further action. Questions regarding the content or application of this policy should be directed to a member of the HR team.

4.3 Users must abide by all applicable laws and Trust policies to protect the copyrights and intellectual property rights of others. It is the responsibility of the user to assume that materials found upon the internet are copyrighted unless the materials contain an express disclaimer to the contrary.

5. Monitoring

5.1 Jigsaw respects the privacy of its users but retains the right to monitor or intercept messages, emails and internet access under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 for the

following reasons:

- To monitor the performance and operation of the ICT facilities
- To investigate or detect the unauthorised use of the systems, e.g., that this policy is being observed, that no discriminatory or offensive content appears in emails, etc
- To maintain an adequate level of security for Jigsaw's computer systems
- To detect any computer viruses
- To check mailboxes of absent employees
- 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 Trust

5.2 To exercise these rights under the Regulations, Jigsaw must have made all reasonable efforts to inform every person who may use the system that interception may take place. The communication of this policy to all employees is intended to meet this requirement.

6. Email

6.1 See Email Policy

7. Passwords

7.1 See Password Policy

8. Acceptable Uses

8.1 As a general principle, network access is provided to users to support work related activities. The list below is not intended to be a definitive list, but sets out broad areas of use that Jigsaw considers to be acceptable use:

- To store work related resources
- To communicate within the Trust
- To communicate with other organisations for educational and operational purposes
- To access resources and training
- Any other use that directly supports work related functions

9. Unacceptable use

9.1 Unacceptable use constitutes (but is not limited to) the following points:

- Attempting to discover another person's username and password, by any means
- Sharing your password with other users
- Attempting to monitor or tamper with another user's electronic communication or data, or reading, copying, modifying or deleting another user's data without the explicit agreement of that user, or their Manager. (Except in the case of electronic mail messages where messages sent and received can be copied and/or monitored)

- Attempting to circumvent by any means the computer or network security
- Using the computer systems (such as electronic mail) to act abusively towards others (including individuals, groups, companies or any other organisation) whether internally or externally
- Using the computer systems to access obscene, racist, hateful, violent, weapons, terrorism, militant, offensive, defamatory, fanatical or harassing material
- Knowingly running and installing on any computer or network, or giving to another user, a program or macro intended to disrupt or damage in any way the computer systems and/or network operations, it's files, programs, data, or any related peripheral or device
- Downloading any copyright materials belonging to third parties, hacking into unauthorised areas, personal financial transactions, deliberate activities that waste networked resources or deliberate or negligent introduction of a virus
- Violating terms and conditions of software copyrights and agreements, including making illicit copies of software
- Installing any software by whatever medium (e.g. data sticks, CD-ROM or data transfer) not provided, virus checked and approved by Jigsaw's IT Department
- The transfer of any data files from data sticks, CD-ROM or data transfer to any of Jigsaw's computers without being fully virus checked. Jigsaw has an anti-virus software system to scan and alert the IT department if further monitoring is required.
- Performing any act that will interfere with the use of the computer, network or equipment (such as printers) or will affect other users' ability to make use of that equipment, such as downloading unnecessary large documents
- Using the computer systems for any activity not related to your work for Jigsaw or for personal financial gain (exemptions to this include collecting personal emails, e-banking or searching other appropriate websites during a recognised break with the prior permission of your manager).
- Relocating or re-allocating computer equipment without the permission and guidance of Jigsaw's IT Department
- Deliberately wasting computer resources such as game playing or sending "junk" or "chain" emails (either electronic or printed) during working hours
- You should not subscribe to any on-line subscription-based internet sites unless they pertain to work duties
- Users may not use the Trust'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.
- If you are allocated a laptop computer, you are responsible for ensuring the safe keeping of this equipment whilst out of the office. Under no circumstances should this equipment be left un-attended in a public place, or in public view. Further you must ensure that all security systems and precautions have been activated to safeguard the laptop

- Providing an opinion that can be attributed to Jigsaw, a member of staff or a client/pupil on a platform (such as social media) that could be viewed by third parties or that may bring Jigsaw into disrepute

9.2 The Trusts network may not be used directly or indirectly by a user for the download, creation, manipulation, transmission or storage of:

- any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
- unlawful material or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others
- unsolicited "nuisance" emails
- material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the Trust or a third party
- material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation
- material with the intent to defraud or which is likely to deceive a third party
- material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation
- material which advocates or promotes any unlawful act
- material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or material that brings the Trust into disrepute

10. Data Protection Officer

10.1 The Data Protection Officer is responsible for overseeing data protection within the school so if you do have any questions in this regard, please do contact them on the information below: -

Data Protection Officer: Judicium Consulting Limited

Address: 72 Cannon Street, London, EC4N 6AE

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0203 326 9174

Lead Contact: Craig Stilwell

11. Policy Review

11.1 This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

11.2 This policy was last reviewed in December 2020.

12. Version History

No.	Date	Amendment
2.1	Dec 2020	Policy completely reworked
2.2	June 2021	Removal of contents of section 6 and section 7, referring to separate policies. Addition of section 10 re DPO

13. Related Legislation & Guidance

Document	Location
Data Protection Act, 2018	http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf
General Data Protection Regulation (GDPR), 2018	https://gdpr-info.eu
The Telecommunications (Lawful Businss Practice) (Interception of Communications) Regulations 2000	The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (legislation.gov.uk)
Computer Misuse Act, 1990	https://www.legislation.gov.uk/ukpga/1990/18/contents

14. Related Internal Documentation

Document	Electronic Copy Location
Data Protection Policy	Common / MyJigsaw / Policies / Trust / GDPR
Data Breach Policy	Common / MyJigsaw / Policies / Trust / GDPR
Mobile Devices Policy	Common / MyJigsaw / Policies / Trust / GDPR
ICT Security Policy	Common / MyJigsaw / Policies / Trust / GDPR
Password Policy (to follow)	Common / MyJigsaw / Policies / Trust / GDPR
Social Media Policy (to follow)	Common / MyJigsaw / Policies / Trust / GDPR
	Common / MyJigsaw / Policies / Trust / GDPR

APPENDIX 1 – ICT Acceptable Use Agreement

This agreement is intended to ensure you have read understood and agree to the IT Acceptable use Policy and associated policies

1. All internet activity must be appropriate to staffs professional activity and / or the pupils' education
2. I will not disclose my username or password to anyone else.
3. I will not use another person's username and password.
4. I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of, to the appropriate person.
5. I understand the Trust can monitor and has full access rights to all my digital information and may use such externally if there is a legitimate requirement.
6. I will only use social networking sites in school in accordance with the school's social networking policy.
7. I will not engage in any on-line of activity that may compromise my professional responsibilities.
8. I will not try to upload, download or access any materials which are illegal or inappropriate.
9. When I use my mobile devices in school, I will follow the rules set out in mobile device policy.
10. I will not use my personal equipment to record images, unless I have permission to do so.
11. I will not cause physical or electronic damage to the Trusts equipment or network.
12. I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities.
13. I understand pupils must be supervised by a member of staff at all times when accessing the internet.
14. Internet Access should only be made via the Trusts filtered network.
15. Activity that threatens the integrity of the central ICT systems, or activity that attacks or corrupts other systems is forbidden.
16. I will not open any hyperlinks in emails or any attachments, unless the source is known and trusted
17. I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner
18. I understand that the data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential.
19. I understand Confidential and sensitive information should be encrypted if sent via email
20. Email use may be monitored if there is any suspicion that the facility is being abused and personal confidential mail should not be sent or received via the company system
21. I will exercise extreme caution when sending emails to any destination to ensure the correct recipient and should confidential information be emailed to the wrong recipient; I will report it immediately.
22. I understand that Jigsaw may be held legally responsible for any email that breaches copyright, if defamatory, racially or sexually abusive or obscene; posting anonymous messages and forwarding chain letters is forbidden
23. Copyright of materials must be respected

I understand that if I fail to comply with this acceptable use policy and associated policies, I could be subject to disciplinary action.

I have read, understood and agree to abide by the ICT Acceptable Use policy

Full name: _____

Signed: _____

Date: _____

APPENDIX 2 - Acceptable Use Policy / ICT Code of Conduct for Visitors

- I understand that it is a criminal offence to use Jigsaw's ICT system for a purpose not permitted by its owner.
- I will only use the Jigsaw's email / internet / intranet and any related technologies for the purpose for which I have been given access.
- I will comply with the ICT system security and not disclose any passwords provided to me by Jigsaw or other related authorities.
- I will not install any hardware or software without the permission of Senior Management or Jigsaw's ICT Support Engineer.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory whilst using Jigsaw's ICT systems.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to the Senior Management Team or my employer.
- I will respect copyright, data protection and intellectual property rights.
- I understand that if I disregard any of the above then it will be reported to senior management and serious infringements may be referred to the police.
- I agree to follow this code of conduct and to support the safe use of ICT throughout Jigsaw and will sign the Visitor's AUP Record Log.

APPENDIX 3 - Acceptable Use Policy / ICT Code of Conduct for Visitors Record Log

Jigsaw Trust

Name	Organisation	Date	Time