

**Policy & Procedure for
CESSA Housing Staff/Tenants using the communal computers**

H 14 – USING THE COMMUNAL COMPUTERS PROVIDED BY CESSA HA/GHSH

Author: DoH
Approved: CEO

Dated: July 2024
Review: July 2027

Preamble: About 2014, CESSA HA & GHSH (the Organisation) noted that many of its tenants were of a generation that had not routinely been taught how to use personal computers and the internet. Accordingly, they were missing the many positive aspects of the computer age, particularly for those less able to get about. Indeed, since the internet has become the primary method of administrative exchange with government & business, without computer-skills and access, some tenants might find it increasingly difficult to remain independent. Therefore, the Organisation has provided the facilities described in this document, under the conditions set out. More recently, their use has declined as residents have gained access to other information technology, e.g. mobile smart phones, and/or computers in their flats. Indeed, this has been encouraged through initiatives such as Project Semaphore at Greenwich Place that provided iPads and taught those interested in how to use them. However, the communal computers continue to be used at CH, DC, GL, SG, TC, GC, GP and TQ.

Policy

The Organisations provide, as a free service to tenants, a special age/beginner appropriate computer in each scheme's communal lounge, together with internet access. The Scheme Manager is the Administrator for the computer in that scheme and is qualified to train tenants in its use and to create an individual 'user account' for each tenant who requests one. Scheme Managers and tenants must operate the computers in accordance with this document and the related manuals/guides, noting their responsibilities set out below.

Procedure

Any tenant wishing to learn how to use the communal computer should ask the Scheme Manager. They will create an individual user account for that tenant (in accordance with the Administrative Guide) and show them how to use the computer (in accordance with the manual provided). Both documents mentioned are also accessible at the links below.
<http://www.simplyunite.com/GuidesAndDownloads/SimplyUnite Manual v3 5.pdf>
<http://www.simplyunite.com/GuidesAndDownloads/Admin Guide v3 5.pdf>
Tenants will need to sign a copy of the enclosed user agreement (and Privacy Statement) before being granted access (see below).

Responsibilities

In order to protect the security of tenants, and meet the Organisation's commitments in its licence agreement with the provider of the purchased software used on the machines, all tenant users and Scheme Managers must abide by the following conditions.

Tenants: Must be responsible for the security of their own passwords. Like with most service arrangements, there are a number of things users must agree NOT to do. These are set out in the Enclosure, a copy of which each user should sign and give to the Scheme Manager before being given access to the computer. While the list is long, please note many are most unlikely to be an issue for the Organisation's tenants, especially if new to computers.

Scheme Managers: Must protect the privacy of the tenant users and maintain the confidentiality of their password as Administrator, the latter only being used in accordance with the guides provided and stored securely. Note other relevant policies in this regard. They must also:

- Immediately notify SimplyUnite¹ (and T&SM who will inform DoH) of any unauthorised use of, or access to, the Service, administrator privileges, password or of any other breach or attempted breach of which they become aware, including, without limitation, any security breach.
- To the extent permitted by law, alert SimplyUnite (and T&SM who will inform DoH) if any service user or administrator, receive a subpoena or other legal information request that requires information from the Service and/or user accounts.
- At SimplyUnite's request, promptly suspend or terminate any SimplyUnite Account in response to a violation of any applicable terms of use or policy by a Service User.
- When a Scheme Manager deletes a tenant account on the SimplyUnite service because it is no longer required by the tenant and they request that their data be deleted then the Scheme Manager should send an email to: support@simplyunite.com to ask for the data to be deleted. This email will need to come from one of the registered emails SimplyUnite have on record.

Any Related Documents: B04 – Data Protection. H12 – Use of Communal Lounges, B20 – Acceptable Use Of CESSAC/CESSA HA WiFi.

Distribution: DoH, T&SM, Scheme Managers, Tenant Policy Folder + File

Enclosure: Certificate (and Privacy Statement) to be signed by Tenant users.

¹ Contact: 0345 388 4453

Certificate (and Privacy Statement) to be signed by Tenant users

Communal computer users i.e. those tenants who have had an account created for them by the Scheme Manager must agree NOT to undertake the following prohibited actions:

- Promote or encourage illegal activity
- Interfere with other users' enjoyment of the Service
- Display any content on the Service (including, but not limited to the customisable login page) that contains any pornographic, hate-related or violent content or contain any other material, products or services that violate or encourage conduct that would violate any criminal laws, any other applicable laws, or any third party rights
- Send, upload, distribute or disseminate or offer to do the same with respect to any unlawful, defamatory, harassing, abusive, fraudulent, infringing, obscene, or otherwise objectionable content
- Transmit content that may be harmful to minors
- Not to generate or facilitate unsolicited commercial email ("spam"). Such activity includes, but is not limited to;
 - sending email in violation of the CAN-SPAM Act or any other applicable anti-spam law
 - imitating or impersonating another person or his, her or its email address, or creating false accounts for the purpose of sending spam
 - data mining any web property (including SimplyUnite) to find email addresses
 - sending unauthorised mail via open, third-party servers
 - sending emails to users who have requested to be removed from a mailing list
 - selling, exchanging or distributing to a third party the email addresses of any person without such person's knowing and continued consent to such disclosure
 - sending unsolicited emails to significant numbers of email addresses belonging to individuals and/or entities with whom you have no pre-existing relationship
- Intentionally distribute viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other items of a destructive or deceptive nature
- Conduct or forward pyramid schemes and the like
- Impersonate another person (via the use of an email address or otherwise) or otherwise misrepresent yourself or the source of any email
- Illegally transmit another's intellectual property or other proprietary information without such owner's or licensor's permission
- Use the Service to violate the legal rights (such as rights of privacy and publicity) of others
- Create multiple user accounts in connection with any violation of the Agreement or create user accounts under false or fraudulent pretences

- Sell, trade, resell or otherwise exploit for any unauthorised commercial purpose or transfer any account
- Modify, adapt, translate, or reverse engineer any portion of the Service
- Remove any copyright, trademark or other proprietary rights notices contained in or on the Service
- Reformat or frame any portion of the web pages that are part of the Service
- Modify the SimplyUnite logo or any other SimplyUnite Brand Features
- Use the Service in connection with illegal peer-to-peer file sharing

Security

You must take care of your password and promptly notify SimplyUnite (through the Scheme Manager) of any breach of security related to the Service, including but not limited to unauthorised use of your password or account. To help ensure the security of your password/account, **please sign out at the end of each session.**

Service User Terms

You acknowledge that as a Service User you will be bound by terms, which may be modified from time to time, relating to each component of the Service. These terms may include but are not limited to the terms set forth at the following URL:

http://www.simplyunite.com/SimplyUnite/SimplyUnite_Terms_and_Conditions.pdf

PRIVACY STATEMENT

This statement explains how CESSAC & CESSA Housing Association (CESSA HA) collect and use your personal information supplied to open a computer account with SimplyUnite.

Who We Are

CESSAC is the data controller for Greenwich Hospital Housing, whereas CESSA HA is the data controller for its Housing. The office is based at 1 Shakespeare Terrace, 126 High Street, Portsmouth, PO1 2RH, U.K. Tel +44 (0) 2392 829319.

What Information We Collect About You

Your personal details as listed:

- name
- email address
- your account login details, including your user name and password
- other personal data which you may disclose to us when you use our Services at any time
- Details you provide to set up contacts within your accounts: name, email address and skype name

How & Why We Use The Information Provided

We collect and store this information in order to open and maintain an account for you on this SimplyUnite computer, which constitutes a contract (although you are not charged for this). Your information will be stored securely in accordance with the General Data Protection Regulation (GDPR) that came into force on 25th May 2018 and the new Data Protection Act 2018.

How Long Do We Keep Your Information For

Your data will be stored until you instruct us to delete it. SimplyUnite also reserves the

right to, at their discretion, delete data from your account if the account is not used for over 12 months.

Your rights

You may ask the Scheme Manager at any time to:

- request that we provide you with a copy of the personal data which we hold about you which will be provided to you in the original format that we stored it for photos and emails, and as an XML structured format for all other data.
- request that we update any of your personal data which is inaccurate or incomplete;
- request that we delete any of your personal data which we are holding

Your request must include your name and email address and we may request proof of your identity. Please allow at least seven working days for us to process your request.

What We Will Not Do

We will not sell or pass on your personal data to unrelated third parties unless we are allowed or required to do so by law or we have your explicit permission to do that. We will not transfer or store your personal data outside of Europe (the European Economic Area) outside of the control of the UK / European regulations.

Your Right To Complain

You have the right to complain about how we use your personal data: in the first instance please contact our office. If you then wish to complain about our use of your personal data you may complain to the UK Information Commissioner's Office (ICO) at

<https://ico.org.uk/>

Signed by New User:

Name:

Date:

Signed by Administrator (Scheme Manager):

Name:

Date: