Provider Portal

Acceptable Use Policy

Care Provider Staff Users

Version history

Author	Jen Weedon, Commissioning Manager Integrated Brokerage
Document Version	1

Revision Date	Summary of changes	Version	Edited by

1.0 Introduction and scope

1.1 This Acceptable Use Policy defines what you may and may not do when using the ContrOCC Provider Portal (hereafter known as the Provider Portal).

1.2 Gloucestershire County Council may require external care providers to use the Provider Portal for under the terms of their contract or prevailing operational instructions referred to in their contract.

1.3 This policy applies to all third party users of the module; usually employees of external care Providers in roles where there is a need to read, query or respond to the information accessed via the Provider Portal.

1.4 All Provider Portal users are expected to comply with this policy at all times when using the Provider Portal, regardless of the device through which it is accessed, for example a desktop computer, laptop, tablet or mobile.

1.5 Gloucestershire County Council has purchased the Provider Portal module and is the controller - as defined by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 - for the information in it.

2.0 Provider Portal functions

2.1 The Provider Portal enables providers to:

- Contact the Council and maintain an up to date record of key staff contacts and roles within their organisation;
- View live purchase order information for the care packages they are currently providing;
- Review and sign contracts for packages of care electronically;
- Send queries relating to individuals receiving care or payments due/received;
- View scheduled payments and remittance (where this applies in the prevailing business rules of the contract).

3.0 Risk Management

3.1 The Provider Portal supports the aims and objectives of the Council and it is essential that your use of it complies with current legislation and does not create unnecessary business and information risks for the Council.

3.2 Users need to be aware of the risks associated with the use of the Provider Portal. Protecting personal and or sensitive information from unauthorised access, modification, disclosure or misuse is essential to mitigate the following risks:

- Harm to individuals
- Service disruption
- Potential legal action and /fines against the Council or individual(s)
- Damage to the Council's reputation
- Loss of credibility
- Theft, fraud or misuse of facilities

Please note that this list is not exhaustive.

4.0 Using the Provider Portal – equipment and logging in

4.1 The following equipment is required to use the Provider Portal and its key functions:

- A desktop or laptop computer
- Internet connection and browser
- csv file editing software (Excel for example)
- A PDF viewer (Adobe Reader for example)
- A secure (named) email address
- A printer and scanner

4.2 The login procedure for authorised users of the Provider Portal involves a two-step user verification process requiring entry of a password and random digits from a 6-digit security number, set up when the user account is created. User account creation is covered separately in the Provider Portal User Access Policy.

5.0 Using the Provider Portal

5.1 Things You Must Do

a) Take the time to read and understand this policy before using the Provider Portal and adhere to this policy while using it.
b) Use the Provider Portal in accordance with the Provider Portal User Handbook/ training guides.
c) Understand and comply with your personal responsibilities when accessing personal and sensitive data according to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, as well as responsibilities in relation to Care Plans as set out by the Care Quality Commission (CQC).
d) Only access personal or sensitive information relating to individuals receiving care on a 'need to know' basis. System users working for care providers will be assigned a Provider Portal security role by the Integrated Brokerage team as part of setting up their user access accounts. This role will give users either 'read' or 'edit' access to certain types of information shared via the Provider Portal.
e) Keep your personal user account login details (password and 6-digit code) stored securely and do not share them with anyone else.
f) Communicate about personal and sensitive information held on the Provider Portal only in relation to the functions of the module outlined in section 2 of this policy.
g) Any personal or sensitive information that has been exported or printed for the purpose of providing care or contract management must be stored and managed confidentially.
h) Report suspected breaches of information security and/or this Acceptable Use policy without delay by (1) following your own internal reporting mechanism for breaches of policy and/or information security and also (2) reporting in writing to Gloucestershire Integrated Brokerage via email: brokeragesystems@gloucestershire.gov.uk.

5.2 Things You Must Not Do

a) Share user log in details or allow anyone else to log in to the Provider Portal using your login details.

b) Leave your user accounts logged in at an unattended and unlocked computer/other device.

c) Use anyone else's user account login details to access the Provider Portal.

d) Exceed the limits of your authorisation/security role or specific business need to interrogate the system or data within the Provider Portal.

e) Use comments, notes or messages on the Provider Portal which could be regarded as unprofessional or considered inappropriate or litigious language. As with other forms of communication, the content on the Provider Portal forms part of the official record.

f) Export, copy or forward information obtained via the Portal in any way that is unrelated to the key functions of the Portal, without the written instructions of GCC as the controller. Examples that are related to the key functions of the system would include printing a contract or contract signature page for an individual or their appointed representative to sign, or exporting summary Care Package Line Item data in a spreadsheet to assist with contract/financial administration.

g) Try to gain unauthorised access to information, or share information without proper authority.

h) Allow third parties, contractors or suppliers to remotely access/take over your PC or laptop via the Internet, as this could compromise the security of the Council's data network.

6.0 The role of Organisational Managers/Lead Correspondents within Provider Portal

6.1 Anyone within an organisation that has implemented Provider Portal and is assigned the security role of Lead Correspondent has a specific responsibility to operate within the boundaries of this policy, ensuring that all Provider Portal

users within their organisation understand the standards of behaviour expected of them to work according to this Acceptable Use policy, and to take action when behaviour falls below or is in breach of its requirements.

6.2 Organisation Managers / Lead Correspondents within Provider Portal should also be prepared to assist where information rights requests are made by an individual or their representative.

6.3 Organisation Managers / Lead Correspondents within Provider Portal are also assumed to hold responsibility for requesting user account creation, amendment or suspension as outlined in the User Access Policy in a timely manner.

7.0 Recording and Monitoring

7.1 All activity within the Provider Portal is traceable to the individual user account holder. The information recorded includes but is not limited to the user's name, date and time and activity undertaken.

8.0 Security breaches

8.1 Any possible breaches of this Acceptable Use policy will be investigated. We will determine, at our discretion, whether there has been a breach of this Acceptable Use policy through your use of the Provider Portal system. Where investigations reveal a breach of information security or of this policy, appropriate action will be taken in respect of data protection legislation and Council contract management and review processes, with reports made to the Information Commissioner's Office (ICO) as necessary.

9.0 Policy Review

9.1 We may review this Acceptable Use policy at any time. This policy will be reviewed as it is deemed appropriate, but no less frequently than every twelve months.