Gloucestershire Community Help Hub
Advice for Residents

Social Distancing & Protective Measures

- To protect both you and the volunteer, please adhere to the Public Health England social distancing guidance by:
  - Not inviting volunteers into your home
  - Asking volunteers to leave items on your doorstep and ensuring they move two metres away (about three steps) before you open your door
- Once you have taken your items inside, please follow the Public Health England advice of washing your hands with warm water and soap for at least 20 seconds as some surfaces can retain the virus
- If a volunteer or other visitor is claiming to be an official, such as a Police Officer, Council Worker, Public Health Representative or Utilities Worker, please ask them to provide identification and review this, ensuring you stay two metres (about three steps) away from them at all times
- If a volunteer claims to be a Police Officer or Community Support Officer, please ask them to wait whilst you call 101 to verify their identity – any genuine member of staff will respect this and allow you to verify who they are
- Be aware of fraudsters – across the UK there have been reports of individuals visiting homes offering doorstep COVID-19 Coronavirus tests or ‘cures’; these are not genuine

Payment

- Do not send payment for any items until you have received them
- Where possible, avoid the use of cash. Instead use alternative methods such as BACS bank transfers, cheques or PayPal (but please ensure your account is secure – advice below)
- Do not give a volunteer your debit or credit card for them to use

Securing PayPal

- Use three random words to make a long and strong password that you don’t use anywhere else and isn’t easy to guess (avoiding family names, pets’ names, places,
the word ‘Password’, sports teams, etc.)

- Turn on two-factor authentication if possible – you will need a mobile phone or an Authenticator app on a phone or tablet for this. This means even if someone manages to get hold of your password, your account should still be secure as they will not have access to the code sent to or generated by your phone. Step by step guidance on turning on two-factor authentication for PayPal can be found here: https://www.telesign.com/turnon2fa/tutorials/how-to-turn-on-2fa-for-paypal/

- Be wary of emails that appear as though they have come from PayPal – PayPal users are a common target for fraudsters and cyber criminals. If in any doubt that an email may be genuine, do not click on any links or attachments and instead log in to PayPal’s website by typing the web address into your search bar; www.paypal.com and logging in directly.