Yorkhill Housing Association Limited **Agenda Item 5.1**

Report to: Management Committee - 29 May 2019

Prepared by: Stewart Pattison: Compliance Manager

Subject: **Payment Card Industry Compliance**

---

1. Introduction

1.1 On 4 February 2019 the Association received correspondence regarding payment card industry compliance from Allpay, the provider of the system used to obtain payment for services we provide. For example, for rent, factoring and other service charges.

1.2 Every tenant is issued with an Allpay card but it is their decision whether or not they use it. Uptake however is high and majority of the Association's rental income is received in this way. The Allpay facility is also used to process debit card and direct debit payments for rent and factoring charges so the use of this facility is significant and integral to our cash-flow.

1.3 Along with the correspondence we received a self-assessment application that we are required to complete. The self-assessment exercise requires to be completed to confirm that the Association is Payment Card Industry (PCI) compliant. Without being compliant we would not be able to continue with the Allpay service. Because the vast majority of the Association's income is obtained through this mechanism it is imperative that we fulfil all the necessary criteria stipulated.

2. Self-assessment approach

2.1 In order to meet the necessary criteria the Association is required to demonstrate that we have all the necessary processes and security measures in place to meet the quite stringent criteria. Our approach was to look at our operations, consult our information technology support provider and submit the application. The reasoning behind this approach was that our service provider Allpay was clear that they would not be providing any advice on the self-assessment process.

2.2 Having taking this approach seems to have been useful in that Allpay replied to us highlighting a number of areas requiring consideration.

This has helped us to focus on particular issues including the need for a policy to address the issues pertaining to card payment transactions. A policy has been developed and is appended to this report for consideration for approval.

3. PCI Compliance - networking activity

3.1. By networking with other associations' through the Glasgow and West of Scotland Forum it is apparent that other associations' are finding the PCI Compliance self-assessment process challenging. Some have investigated costs for consultancy services in this regard. The outcome of the networking exercise for the Association was; considering the feedback we received from other associations, revisiting our I.T. systems with our support provider in view of the Allpay comments received, and producing a Card Payment Transaction Policy.

3.2 Given the action taken it is felt that we are now in a position to resubmit our application. We believe we should now be compliant, if the appended policy is approved.

4. Recommendation

4.1 It is recommended that Committee note the content of this report and action taken to date; and

4.2 Approve the appended 'Card Payment Transaction Policy' to support our self-assessment application.

Appendix 1

Yorkhill Housing Association Limited

Card Payment Transactions Policy

1. Introduction

1.1 Yorkhill Housing Association take card payments and process Allpay transactions for services provided by the Association.

1.2 In undertaking this activity it is necessary to ensure that data protection principles and Payment Card Industry (PCI) compliance requirements are met.

1.3 This card payment transaction policy ensures the Association's compliance with data protection principles and PCI requirements by stipulating the procedure to be undertaken during data processing activity.

2. The Association's Procedure for Processing Card Payments

2.1 As necessary to process payments, Association staff are exposed to customers' 'Primary Account Numbers' (PANs). The 'Primary Account Numbers' for the purposes of this activity are numbers unique to customers and Allpay. To meet compliance requirement for our purposes, we need to protect the security of these numbers and ensure that they are not stored by us. Although we did store the numbers previously it is now acknowledged through reviewing our processes that we do not need to. This practice has now ceased.

2.2 In processing payments, to ensure security and achieve data protection and PCI compliance requirements:

- Staff will input data directly through the Allpay System'.
- Staff will not write down or in any way record PANs;
- Staff will not communicate PANs to each other or any third party;
- Staff will not share PANs through email or any other messaging facility;

  and

- The Association will not store any PAN information.

3. Visual Display Units (VDUs)

3.1 Staff will ensure that their computers are locked and no information is displayed when they are not at their work stations.