JustUs Data Security Policy

1. Aims and Objectives

1.1. In order to comply with the seventh principle of the Data Protection Act 1998 regarding information security, all JustUs personnel shall abide by this policy when processing client data. Processing of data includes any act that involves client-identifiable information.

1.2. The majority of data breaches do not occur as a result of hacked information; it is almost always human error (e.g. sending sensitive personal data to the wrong recipient, losing belongings containing sensitive personal information). This policy should minimise the risk of this happening.

1.3. JustUs members should remember that every client will trust JustUs personnel with personal information that may be highly sensitive. JustUs' handling of it must therefore reflect the significance that the information will have to each client. In order to do this, all client's personal data shall be treated as sensitive personal data under the definition of the Data Protection Act 1998.

2. Electronic Security

2.1. Any electronic document that holds information about a client shall be password-protected.

2.2. A list of passwords shall be held by each caseworker. This document shall always be encrypted by a separate password that shall never be reproduced or shared with anyone other than a trustee / caseworker. The Business Continuity Policy shall ensure that trustees can have access to this document should a caseworker become unavailable for a period that would leave client casework to be neglected.

2.3. Caseworkers must be sure that the recipient email address is correct and must ensure when sending emails to new recipients to ensure it is the correct person.

2.4. Once password-protected documents have been emailed, another, separate email can be sent with the corresponding password.

2.5. Emails that omit client-identifiable information can be sent un-encrypted, but caseworkers must be sure that the information contained cannot be 'pieced together' with publicly available information that would lead to identification of a person.

2.6. Documents for each client shall be stored in a folder labelled with the date and the client's initials.

2.7. Faxes are never to be used due to their inherently insecure nature. Documents can be scanned and sent in password-protected emails.

2.8. Caseworkers should be extremely careful when forwarding emails that client-identifiable information has not been included in the original email.

3. Physical Security

3.1. Paper files containing client data must be scanned into electronic password-protected files as soon as possible and the paper copy must then be shredded unless there is a specific need to keep it. In which case, documents will be kept in a locked cabinet in a lock room to make it impossible for a third party to obtain without breaking and entering.

3.2. Telephone conversations identifying client information must be conducted in private areas.

3.3. Incoming callers must have their identity verified before discussing client data.

3.4. Caseworkers must ensure recipient postal addresses are correct if client data must be sent my mail.

3.5. Mobile phones must not contain client-identifiable data in case of loss or theft. This includes text messages. If clients send client-identifiable texts they must be deleted once they have been responded to. Codes must be used when listing client phone numbers.

3.6. Client data must be transported in locked bags to prevent accidental loss / theft and must be kept to a bare minimum.

Adopted:	June 2015
Last Reviewed	January 2018
Next Review date:	January 2021