Information Audit – Data Flow

1. Initial Acquisition

Direct Enquiry:
- Walk-In (person arrives at facility and discloses new personal information in verbal format)
- Phone Call (person calls or texts business number and discloses new personal information in verbal format)
- Email (person sends email to business address and discloses new personal information)
- Online (person submits form via business website or social media page and discloses new information)

Indirect Enquiry:
- Out-Of-Hours (person discloses new personal information to member of staff outside of working hours)
- Referral (business receives new personal information about a person, given by a third party with explicit or unambiguous consent from the person)
- Indiscreet Disclosure (business receives new personal information about a person, given by a third party without explicit or unambiguous consent from the person)

2. Data Capture

Walk-In:
- Written (information is collected by writing down on paper)
- Locally Stored (information is collected in Word document on business laptop or desktop)
- Online (information is input into customer profile on online management software 'https://goteamup.com/en-gb')

Phone Call:
- Written (information is collected by writing down on paper)
- Locally Stored (information is collected in Word document on business laptop or desktop)
- Online (information is input into customer profile on online management software 'https://goteamup.com/en-gb')

Email:
- Direct Enquiry to Inbox (information is acquired from contents of email, but not transferred into other format at point of capture)
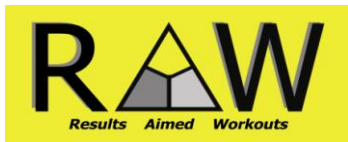
- Referral to Inbox (information is acquired from contents of email, but not transferred into other format at point of capture)

Online:
- Customer Registration (information is collected on form and delivered to business email inbox)
- Mailing List (information is collected on form and delivered to mailing system 'https://mailchimp.com/' and business email inbox)
- Enquiry Form (information is collected on form on customer profile on online management software 'https://goteamup.com/en-gb' and business email inbox)

Out-Of-Hours:
- Written (information is collected by writing down on paper)

3. Data Storage

Written:
- Client basic and contact details are stored on-site in lockable safe

Locally Stored:
- All stored data is stored on computer hard drives and USBs, kept on business premises

Online:
- Client basic, contact, health record, membership and payment details are stored on our online booking software (goteamup.com)
- Client basic, contact, health record, exercise regime and membership details are stored on our online programming website (resultsaimedworkouts.co.uk)

Email Inbox:
- Client email address and any information shared directly in emails is stored in our mailbox (outitgoes.com)
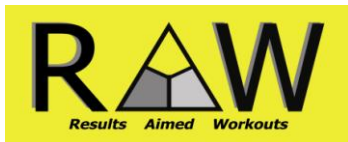
Mobile Phone Inbox:
- Client phone number and any information shared directly in text messages is stored in our business mobile's internal messages folder

Landline Phone Inbox:
- All information given in a recorded message to our landline answer machine will be stored on the machine for a maximum period of 1 month.

4. Data Processing

Booking Software:

- All information that is stored on our booking software (see above 'online' for details) will be taken from any other streams and added to the booking software, where it will be protected by the software provider (goteamup.com)

Programming website:

- All information that is stored on our programming website (see above 'online' for details) will be taken from any other streams and added to the website, where it will be protected by the web provider (wix.com).

Offline data:

- No offline data will be shared or processed by anyone other than our staff who are contracted to adhere to the strictest confidentiality.
- For safety and ease purposes, any offline data that is not stored on the booking software or programming website will be saved onto each business computer, which is protected by our anti-virus software (avg.com), and each universal storage bus (USB), which is password encrypted.
- Any offline data that has been captured on paper (excluding medical information) will be transferred onto a business computer and the paper copy will be shredded beyond recognition and discarded at the earliest convenience.
- Any medical information stored on paper will be locked away in lockable safe.

Points and Statements of Consent:

- Each person whose personal information is obtained and stored by the business will be requested permission in order to do so.
- Unless directly requested in writing by the person, we will not disclose any of their information to anyone outside of the staff team.
- Business Written – permission is verbally requested in order to capture information on paper, which will then be stored in an on-site lockable storage cabinet until it can be transferred onto business computers and USBs and discarded, but never disclosed outside of staff team.
- Person Written – person is asked to write information on paper, which will then be stored in an on-site lockable storage cabinet until it can be transferred onto business computers and USBs and discarded, but never disclosed outside of staff team
- Local Storage – permission is verbally requested in order to capture information in a Word document on a business computer, which will be saved onto the computer hard drive, universal storage bus (USB),
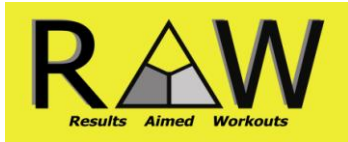
transferred onto the other business computers and saved to their hard drives, and updated on each at any point where more information is acquired.

- Online – person is asked to fill out required information on online form for use by the business.