EVOLVE Top Tips for ensuring GDPR compliance

- ✓ Change your password regularly and keep this safe.
- ✓ Never reveal or share your password with anyone. We will never ask you for your password when supporting you.
- ✓ Do not share user accounts with colleagues. Request a unique login from your EVC when planning your trips.
- ✓ Ensure staff accounts are deactivated as soon as they finish employment. (EVOLVE+ automates this process and ensures all staff accounts are created and disabled automatically – one less thing to worry about!)
- ✓ Always keep your email address up to date in your profile for notifications (EVOLVE+ ensures this is checked daily and kept up to date)
- ✓ Make use of EVOLVE's Access Controls to ensure all users have appropriate levels of access for Payments, Bookings, Communications, Consent purposes (System Administrators only).
- ✓ As a data subject can make a Subject Access Request at any time, minimise inclusion of sensitive data in attachments where an alternative solution is available e.g. by using EVOLVE's integrated register module. This will allow you to more quickly search for that subject should you need to.
- ✓ Avoid inclusion of sensitive data for *multiple* individuals in single attachments e.g. risk assessments. Best practice would be to produce separate risk assessments to upload to EVOLVE and name these accordingly, to ensure that should you need to delete a reference to an individual in future or quickly identify the attachment that refers to the individual, this can be carried out without affecting other data.
- ✓ Review EVOLVE Data Security Dashboard regularly (System Administrators only).
- ✓ Consider using Event Specific Notes module for data usually stored in separate Risk Assessments. This will allow you to search the Visit Form for sensitive data including names.