

# Data Protection Youth Club Information Sheet

To prepare for the changes in the data protection law, there are a few changes you need to make to the way you handle data. The main changes that impact on youth clubs are listed below.

Definitions used in this document

- Parental consent: includes the consent of a guardian.
  - Data Subject: an individual who is the subject of the personal data.
1. Pre-ticked and opt-out boxes will no longer be sufficient for proving “consent” – data subjects must actively opt-in to receive different forms of communication. This can take the form of tick boxes written/electronic/oral statements, and consent clearly indicates acceptance "for the reason stated and nothing more". Our new consent forms clearly show this.
  2. Requests for opt-in consent must be clear and unambiguous, using easily accessible plain language catered to the person being communicated with.
  3. It is no longer acceptable to withhold goods/services from individuals who do not give consent for something completely unrelated (e.g. free WiFi for subscribing to email updates). However, you can of course withhold goods / services if those goods / services require consent (for example, coming to club or going on a trip).
  4. The definition for what is considered “personal data” has been expanded to include online identifiers (such as IP addresses and location information).
  5. While some data can be collected if it is claimed as “legitimate interest”, adequate reasons must be given for what legal basis there is for collecting this data. The organisation must balance its rights to collect data with the rights of the person. Privacy statements on consent forms will cover this; see our sample.
  6. It is good practice that our policies and information show what exactly what data will be used for and how long it will be held (SYCS Data Protection Recording Documentation’ sample covers this).
  7. All data collection forms must be kept proving consent was granted or a legitimate reason for processing. Again, our Data Protection Recording Documentation’ sample covers this.
  8. Individuals have the right to revoke data consent at any time and they must be made aware of this right. The process of unsubscribing must be just as easy as subscribing.
  9. You are legally required to report all data breaches (no matter how small) ‘without undue delay’ – and within 72 hours – to the Information Commissioner’s Office (<https://ico.org.uk>). The ICO will maintain a public register of the types of breaches notified. You are legally required to inform the individuals ‘without undue delay’ where the breach could result in ID theft or fraud; physical harm; significant humiliation and/or damage to reputation.

10. You must also do the following:

- a. (1) Risk Analysis – you need to assess whether or not data processing activities present specific risks and put in place control measures. This should be reviewed on an annual basis or at the time of significant change.
- b. (2) Privacy Impact Assessments – if you start using or processing personal data differently, you must check to see if there are any privacy issues as a result.
- c. (3) Privacy by Design and Privacy by Default – systems and procedures should be designed to comply with Data Protection principles by default – so, you should not collect, retain or share personal data beyond the minimum necessary.

11. You must have appropriate organisational and technical control. The easiest way to do this is to have a data protection policy - adopting the sample 'Data Protection Policy' will cover this for you. It is good practice to keep records of the appropriate procedures to demonstrate compliance with the Regulation. Completing the sample 'Data Protection Recording Documentation' will provide this for you. You must review them at least every two years, but it is best done annually.

12. Your club is not required to register with the ICO and does not need a statutory Data Protection Officer, just a nominated person to act as a Data Protection Controller to ensure policies are followed.

So, what do you actually need to do?

- a) Adopt a Data Protection Policy – our sample is good. Make sure you can do all things it says.
- b) Complete the Data Protection Recording Document sample with the relevant information. Use this as a living document to record your data processes and any changes.
- c) If you want to contact young people via phone, text or email, make sure your consent forms have the correct 'opt-in' tick boxes and the privacy notice (our 'Annual Consent form' sample has all of these)
- d) If you don't want to contact young people via phone, text or email, you still need the new privacy notice
- e) If you have a website, ensure that there is a privacy notice and that consent has been gained from a parent or guardian for you to contact young people via it.
- f) Keep updating the 'Data Protection Recording Documentation' as you go along and review all policy and procedure documentation annually.

**If you want to talk this through, please contact one of the Youth and Community Officers, either:**

- Kirstie Brown - telephone 01823 357553 / 07899 700170 or email [kbrown@somerset.gov.uk](mailto:kbrown@somerset.gov.uk) or
- Zara Scott-Davies - telephone 01823 357554 / 07919 540738 or at [zscottdavies@somerset.gov.uk](mailto:zscottdavies@somerset.gov.uk)