Data Protection guidance for community-led supplementary schools

The Data Protection Act 1998, and the European General Data Protection Regulation 2016/679 (GDPR), are the key legislative and regulatory provisions governing the security of person-identifiable information. The purpose of these provisions is to safeguard the public from abuse in the collection, storage, usage and distribution of personal information.

1. Data protection principles

These are the main principles in GDPR which form the basis of your responsibilities as a data controller.

You must:

1. Process data lawfully, fairly and transparently.
Processing 'lawfully' means you must have a legal basis for processing data – see part 2 below for more information.

2. Collect data for specified purposes
Tell people what you are collecting personal data for and only use it for these purposes.

3. Only collect the data you need
Do not collect data which is not necessary to fulfil your purposes. Do you need to collect someone's date of birth, or gender, for example? Think about why you need data before you collect. If it is not really necessary, do not ask for it. Delete anything you do not need or cannot justify holding.

4. Make sure your data is accurate
Keep the data you hold up to date – make it easy for people to contact you to update their details.

5. Hold data only for as long as it is needed
Only hold data for as long as is necessary to fulfil the purpose for which you collected it. Decide what is a reasonable length period is and then tell people what this is, and why, in your privacy statement. At the end of the period, you need to delete the data securely – paper and electronic copies. Some information may be necessary for a longer period for tax or legal purposes – seven years, for example.

6. Keep data secure
You need to keep personal data secure. This means thinking about a range of measures, from locking away paper documents containing personal data to protecting all your computers and mobile devices with passwords and thinking about encryption, depending on what you do with data.

7. Be accountable
As we note above, GDPR is underpinned by a requirement that we are all accountable for demonstrating how we put the principles above into practice. Our privacy statement template and simple data map will help you.

2. Lawful basis for processing data

To process personal data, you must have a **lawful basis**, of which there are six to choose from in GDPR:

1. Consent
2. Contract
3. A legal obligation
4. Vital interest
5. Public task
6. Legitimate interest

According to the ICO's Guide to GDPR: *"There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual."*

Don't:

- worry too much about the complexities of the Act and the GDPR– the data protection principles are simple;
- reveal personal data to third parties without the data subjects' permission or justification;
- disclose any personal data over the telephone or via email;
- hold sensitive data about a person without explicit consent;
- collect more data than you actually need for the purposes of collection;
- put personal data about an individual on the internet without his/her permission, unless it is a condition of his/her employment;
- send personal data outside the European Economic Area (EEA) without taking advice from the Information Commissioner's Office;
- leave personal data insecure in any way, whether it is in physical files or information held electronically;
- take personal data home without particular care for security;
- use email for sending confidential communications or unencrypted data, as it is relatively insecure;
- when sending e-newsletters or marketing campaigns via email you must not conceal your identity;
- use personal data held for one purpose for a different purpose without permission from the data subject;
- aside from routine amendments, erase or alter any personal data after the Data Protection Officer has received a request to inspect and/or disclose that personal data.

If you don't have a data protection policy or you would like legal advice on yours you can go online to Bates, Wells & Braithwaite law firm who specialise in working with charities. They will produce a data protection policy for you when you fill in an online form. https://getlegal.bwbllp.com/products/gdpr-friendly-data-protection-policy

Visit the website for the Information Commissioner's Office for further guidance, to report a breach of your data or a concern
https://ico.org.uk/