Private Data Policy

The Data Protection Act is mandatory. It is essential therefore that we fully comply with it, not just to avoid prosecution and bad publicity, but also to demonstrate to our partners and volunteers that we operate with due diligence and responsibility.

Cics is committed to complying with data protection law and data subjects' rights under it, in relation to their personal information, whilst it is under our control. The data subject is the person that the personal information identifies or relates to.

This means that we will comply with the eight principles of data protection, subject to exemptions and rights available under the law. The principles provide that personal information must be:

1. Processed fairly and lawfully.
2. Processed for clearly defined purposes, which the data subject is aware of, and which are lawful.
3. Adequate, relevant and not excessive for the purposes.
4. Accurate.
5. Not kept longer than necessary for the purposes.
6. Processed in line with data subjects' rights.
7. Kept private and secure.
8. Not transferred to people or organisations situated in countries without adequate protection.

Our commitment applies to our handling of the personal information throughout its time under our control. It applies to our obtaining, collection, storage, processing and destruction of personal information, and when we transmit it or make it available to third parties.

General principles:

- Consent is freely given and can be withdrawn at any time.
- People are clear about the nature of the consent they are giving and the purpose for which their data is held.
- People are fully informed and able to ask questions and change data preferences at any time. Anyone has the right to know what

information is held about them at any time (This is called a Subject Access Request)

Security of physical files and electronically stored information

	What we keep and why	How data is stored	
Staff	Staff personal details on application forms kept for contact details, pay, pensions and to fulfil legal requirements.	locked Filing cabinet. (RW +TP) Annual review forms will be kept electronically and password protected. The reviewee will have a printed copy to keep at home and only Trustees will have access to the electronic copy.	To be destroyed 7 years after termination of employment.
Staff emergency contacts	Contact details of a family member for emergencies.	Filing cabinet and in each staff member's private possession.	
Past Staff	Personal information and contact details.	Locked cupboard	These are destroyed after 7 years.
Job applications	Personal information and contact details.	Locked cupboard	Destroyed after 6 months.
Trustees	Personal information and contact details. Used to apply for grants and the	Locked cupboard	Destroyed 6 months after they cease to be a trustee.

	Charity Commission also requires them. DBS details are also kept.	name, email and phone details on all computers,securely inside password. locked filing cupboard	
Volunteers	We keep the names, home addresses, email addresses, mobile and home phone telephone numbers for all volunteers for the purposes of contacting them to ask them to volunteer for us in schools.DBS Checks that we have carried out are kept in a locked filing cabinet.	Volunteers fill in application forms which include form showing they have agreed to data storage under GDPR regulations. These are kept in a locked office. Personal data is stored on the computer which is in an Excel password protected file. DBS data stored on the password protected computer and hard copy in locked filing cabinet.	All volunteers are requested to provide us with permission to keep their data under GDPR rules. If they don't, we will destroy it.
Mailing Contacts	We keep names and email addresses of our supporters who have requested to be kept in touch with what we do.	We use Mail Chimp to send out newsletters and updates. This is Password protected.	Users can unsubscribe from this.
Churches and schools	Names of supporting Churches and	Most of the information we hold for Churches and	Deleted when the information

	Ministers, Head Teachers, RE Coordinators of the schools we work in	Schools is in the public domain and therefore does not require special permission to be held. If any personal details are given by individuals it has been done willingly and by consent.	becomes kept unnecessarily.

Service Users	When mentoring… Workers will always follow the policy and wishes of the school. (see mentoring policy) event s- chn - parent's contact number...	It may be necessary to keep some information which would normally be(hard copy?) in the school office. Any information kept on a device will be under a password and without identifying the individual, if possible.	Delete after years

Secure locations:

??

Releasing information to detect or prevent a crime

From time to time CICS staff or trustees may receive requests from the police or other organisations (such as local safeguarding authority) for the disclosure of information relating to a child we have worked with that is required in

connection with the prevention or detection of a crime, the apprehension or prosecution of offenders. This is commonly known as a section 29 request as it refers to section 29 of the Data Protection Act; this section allows for information to be shared without the consent of the data subject. Whilst in most cases it is likely to be in the public interest to assist such bodies by providing the required information, Cics is committed to ensuring that all such disclosures are fair and lawful, and in particular, that they are compliant with the Data Protection Act. We would expect, in most cases, that the request will come in writing and will be received by the Administrator or Safeguarding trustee.

With thanks to Hand to Mouth for Permission to use and adapt.

Approved March 2021