CRS Data Protection Policy

1. Background

1.1. The new EU General Data Protection Regulation (GDPR) came into force on 25th May 2018

1.2. CRS wishes to assert its compliance with the GDPR and, as a consequence, must implement an overall data protection policy (this policy)

2. Overall Committee responsibilities

2.1. All members of the CRS Committee are responsible for complying with this policy

2.2. All members of the CRS Committee shall be required to sign a GDPR compliance statement

3. Data Compliance Officers

3.1. CRS shall appoint one or more Data Compliance Officers (DCO) from amongst the Committee, who shall ensure compliance with the GDPR

3.2. DCOs shall be appointed for an initial term of two years after which they may be re-appointed for another two-year period if it is their wish and that of the Committee

3.3. One of the DCOs shall be designated Lead DCO, who shall be responsible for registering CRS with the Information Commissioners Office (ICO) and for investigating and reporting on any data breaches

3.4. DCOs shall liaise with those members of the Committee with responsibilities for managing the CRS website, membership database and all forms of communication with members and other stakeholders with whom members' personal data may be shared

4. Rights of Data Subjects (CRS Members)

4.1. Rights of data subjects as described in the GDPR shall be preserved in all processes operated by CRS

4.2. Rights of data subjects shall be incorporated into a CRS Data Privacy Statement that shall be posted on the CRS website and made available in written form

5. Communication with Members, potential members and other stakeholders

5.1. All CRS communications shall contain a link or reference to the CRS Data Privacy Statement

6. Data management processes

6.1. Acquisition of membership personal data and consent for its use

6.1.1. All means by which individuals provide their personal data to CRS shall offer the opportunity to review the Data Privacy Statement and give consent to its use

6.2. Data processing

6.2.1. All means by which Members' personal data are entered into databases and used for communication with members and external organisations (where appropriate) shall preserve data privacy according to the consent given by individuals

6.3. Data storage

6.3.1. Personal data stored in electronic form shall be maintained on password-protected files on computer drives under the supervision of designated Committee members

6.3.2. Copies of electronic datafiles shall be kept to an absolute minimum and avoided where possible

6.3.3. Personal data stored in paper form shall be maintained in locked filing cabinets or drawers under the supervision of designated Committee members

6.4. Data security & backup

6.4.1. All computers and drives shall be protected by established commercial data security software which shall be regularly updated

6.4.2. Data files shall be backed up onto secure external drives at regular intervals using appropriate operating system software & applications.

6.4.3. External drives shall be kept secure and under lock and key where possible

6.4.4. Memory sticks used for data sharing between Committee members shall be encrypted and subject to control by the Membership Secretary and DCO

6.4.5. Transfer of files containing personal data by email shall be avoided

6.5. Data retention & disposal

6.5.1. Personal data shall be retained for as long as it is required for communication with the individual and within the consent provided by the individual

6.5.2. Personal data shall be deleted from electronic and paper databases on request of the individual or the individual's family if deceased

6.6. Data sharing within the CRS Committee

6.6.1. Data files containing personal data which are required to be shared within the CRS Committee shall be made available in password protected form on an encrypted memory stick

6.6.2. Passwords for such files shall be changed regularly and when Committee members leave the Committee

6.7. Data sharing with other stakeholders and external bodies

6.7.1. The decision to share personal data and what data is shared, shall be the responsibility of the Chair (or Deputy) and DCO (or deputy)

6.7.2. When data sharing is necessary in order to meet CRS objectives (eg to support a local Neighbourhood Watch group or Residents' Association), explicit consent from the individuals whose data is shared may not always be required. However, where external commercial interests are involved, this shall require discussion and agreement by the whole Committee and explicit consent from individuals obtained

6.7.3. In all cases, the external organisation involved shall be required to preserve the data privacy rights of the individuals whose data is shared

6.8. Data breaches

6.8.1. When a data breach or potential data breach is identified, the lead DCO shall immediately investigate and report their findings to the Committee who shall decide on the appropriate course of action under the GDPR