KENWYN PARISH COUNCIL

Check list questions – Technical and Organisational Safeguards & Measures

☐ Keep the formats the Council use for capturing and collating data to a minimum (e.g. if you capture information using a hard copy and then transfer all the information to electronic storage is it necessary to keep the original hard copy?)

☐ Ensure the Council only captures the information you need to carry out the process (minimisation) – once the process is complete do you need to keep the information (retention)

☐ Restrict access to the information to only those who need it

☐ Ensure you follow the Councils retention and disposal procedures in regards to the information you hold – if you haven't got one, document one

☐ Secure personal information, in particular special categories of information by encryption (if possible) or at least password protect sensitive spreadsheets and word documents. Keep sensitive hard copy in lockable storage when not in use

☐ Ensure information is backed up to minimise the risk of corruption and unavailability – consider the risk to your business processes if hard copy information suddenly became unavailable

☐ Contracts and Data Sharing Agreements – make sure third parties (internal and external if necessary) are aware of their responsibilities in regards to data privacy and the possible consequences if they are not. The Council cannot abdicate responsibility.

☐ Carryout Data Protection Impact Assessment (Data Protection by Design) and IT security assessment

☐ Conduct regular reviews of the personal data we process and update our documentation accordingly

☐ We have identified staff in our service / teams who are the first point of contact for data protection