Marks Tey Parish Council eCRB Security Policy

Handling of Disclosure and Barring Certificate Information

Secure Storage, Handling, Use, Retention & Disposal of Disclosure and Barring Service (DBS) Certificates and Certificate information

General principles :- As an organisation using the Disclosure and Barring (DBS) service to help assess the suitability of applicants for positions of trust, **Marks Tey Parish Council** complies fully with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of Certificates and Certificate information; this applies to paper applications and via the ebulk service. It also complies fully with its obligations under the Data Protection Act 1998 and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of Certificate information and has a written policy on these matters, which is available to those who wish to see it on request.

Storage and access:- Certificate information should be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

Electronic (ebulk) - All data stored in encrypted form and access is only by password authenticated users. The online systems used to store information are located in a secure facility which undergoes regular security penetration testing and security audits to meet DBS security requirements. Information management processes are compliant for ISO 27001. User accounts have access only to the information needed for processing purposes for their specific role.

Handling:- In accordance with section 124 of the Police Act 1997, Certificate information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom Certificates or Certificate information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.

Ebulk - Atlantic Data access to the system is limited to specific named system administrators and controlled by password authentication. Access by Atlantic Data is only for the purposes of system support in response to incidents raised by Essex County Council and not for processing. All access is logged in audit trails. Audit trails are available to DBS by written request.

Usage:- Certificate information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Retention:- Once a recruitment (or other relevant) decision has been made eCRB Services must be notified to allow us to adhere to the DBS code of practice, we do not keep Certificate information for any longer than is necessary. This is generally for a period of

up to six months, to allow for the consideration and resolution of any disputes or complaints. If, in very exceptional circumstances, it is considered necessary to keep Certificate information for longer than six months, we will consult the DBS about this and will give full consideration to the Data Protection and Human Rights of the individual before doing so. Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.

Disposal of electronic information will be by secure data destruction to security levels equivalent to HMG Infosec No. 5.

Disposal:- Once the retention period has elapsed, we will ensure that any Certificate information is immediately destroyed by secure means, i.e. by shredding, pulping or burning. While awaiting destruction, Certificate information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack). We will not keep any photocopy or other image of the Certificate or any copy or representation of the contents of a Certificate. However, notwithstanding the above, we may keep a record of the date of issue of a Certificate, the name of the subject, the type of Certificate requested, the position for which the Certificate was requested, the unique reference number of the Certificate and the details of the recruitment decision taken.

Disposal of electronic information will be by secure data destruction to security levels equivalent to HMG Infosec No. 5.