GDPR: Technology Compliance **Hannington Parish Council**

Objective:

> "*To implement the necessary technologies to comply with the GDPR requirements thereby protecting the privacy of people, and their right to be removed from the record, when communicating with parish council members via email.* "

Method:

To provide secure online communication for the Hannington Parish website and for council member emails, and the automated recording of internal emails and those emails received or sent externally by Cllrs and Clerk:-

1. The domain name 'hannington-hants-pc.gov.uk' has been implemented for both the website and council member emails.
2. Website access is via HTTPS (Secure) encrypted online connection. See guidance at https://www.ncsc.gov.uk/guidance/tls-external-facing-services . Hugo Fox have implemented the necessary SSL/TLS Certificate for the Hannington Parish Council website. See https://www.digicert.com/help/ for certificate verification.
3. To comply with the policy of only using 'hannington-hants-pc.gov.uk' email addresses for conducting council business, all parish Cllrs and Clerk are issued with email addresses. These are of the form Cllr.*firstname.surname*@hannington.hants.pc.gov.uk and where the Parish Clerk has a generic form of Clerk@hannington.hants.pc.gov.uk. The management of email addresses and their issuance is performed by the Parish Clerk.
4. The 'hannington-hants-pc.gov.uk' emails have been secured according to the 'Securing government email – Guidance' See https://www.gov.uk/guidance/securing-government-email . Specifically, Domain-based Message Authentication, Reporting and Conformance (DMARC), Sender Policy Framework (SPF) and Domain-Keys Identified Mail (DKIM) have been implemented. The Microsoft Exchange email system uses the Transport Layer Security (TLS) version 1.2 encryption protocol by default to protect data in transit.
5. Automated '*Forwarding*' of Hannington Parish Council emails is prevented by a Microsoft Policy implementation.
6. The Cryoserver, for recording all email correspondence between internal 'hannington-hants-pc.gov.uk' and external email users is in operation. The Cryoserver has been implemented with the Clerk 'Admin' and 'Priv' accounts to allow access by the Parish Clerk (an 'Officer' of the parish council) to recorded email correspondence. Whenever the Cryoserver is accessed, for whatever reason, an automated email is issued to one or more 'Guardians'. The Clerk in this case can interrogate and trace all emails, e.g. where an individual has exercised the right to be 'removed', and then delete the associated email records on the Cryoserver. Subsequently, request the individual Cllrs to delete the associated 'traced' email held on their computing device. The Cryoserver maintains an audit trail of the deletions compliant with the GDPR requirement.

   Note: That the Cryoserver provides the means to the Clerk to fulfil '*Freedom of Information*' requests with regard to email correspondence when the occasion arises.

Control & Monitoring (Auditing):

1. **Microsoft Email Account Administration Security:** Microsoft recommends to the Office 365 'Administrator' to implement security controls – 20 actions in the queue – these are in the process of implementation over time. These actions cover the basics, and include some defence in depth options. Microsoft notifies if email breaches are detected.
2. **Email Security:** Message Authentication, Reporting and Conformance (DMARC) – a rolling 7 days of email correspondence can be monitored by the Parish Clerk on a regular basis. The Dmarcian application is at https://dmarcian-eu.com/domain-overview and has been implemented. The major email provider's data, e.g. Google, Yahoo, Proximus.be, may send their data relating to the emails emanating from the 'hannington-hants-pc.gov.uk' domain to the reporting application where issues are highlighted.
3. **Website Security:** Automated Notifications from the '*Web Check Service*' provided by the National Cyber Security Centre (part of GCHQ) monitors changes to the security of the 'hannington-hants-pc.gov.uk' website. It clearly highlights the status of security of the website by categorising the findings as 'Urgent', 'Advisory', 'Informational' and 'Positive'**.** The Hannington Parish Council website conforms to the NCSC recommendations.

Hannington Parish Council Email Distribution List:

To comply with GDPR the creation of an email distribution list, specifically under the control of the Clerk to the Hannington Parish Council, is required. To this end, the GDPR compliant integration of MailChimp with the Hannington Parish website is to be explored.

Author: Jan Hertz, 8th March 2019