



## Cyber Security Policy

### Version Control

| Version | Date Approved | Minute Reference | Website Updated | Next Review |
|---------|---------------|------------------|-----------------|-------------|
| Ver 1   | 19.01.2026    | 146/26a          | 22.01.2026      | March 2027  |
|         |               |                  |                 |             |

## 1. Introduction

The more we rely on information technology (IT) to collect, store and manage information, the more vulnerable we become to severe security breaches. Human error, hacker attacks and system malfunctions can not only cause great financial damage but jeopardise the reputation of Crondall Parish Council (CPC).

## 2. Purpose

- To ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring.
- To protect CPC from the risk of financial loss, loss of reputation or libel.
- To ensure that CPC's IT is not used so as to cause harm or damage to any person or organisation.

## 3. Scope

- This policy applies to CPC's Councillors and employees and anyone who has any access at any time to CPC's IT.

## 4. Confidential Information

- Confidential Information includes, but is not limited to:
  - **Personally Identifiable Information (PII)** - Information that can be used to distinguish or trace an individual's identity, whether alone or when combined with other information that is linked or linkable to a specific individual.
  - **Secret information** - Information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where disclosure could damage military capabilities, international relations or the investigation of serious organised crime.
  - **Commercial/operationally sensitive data** - Information whose loss, misuse, or unauthorised access or modification could adversely affect the commercial or operational security of CPC.
  - **Commercial-in-confidence data** - Commercially sensitive information which must be kept confidential between relevant parties for example a supplier's trade secrets that were shared in confidence with CPC.
  - **Special category personal data** - personal data that needs more protection because it is sensitive according to UK General Data Protection Regulation (GDPR) - this includes racial, religious, biometric and health data.
  - **Criminal offence data** - personal data relating to criminal convictions and offences or related security measures.
  - **Personal financial data** - a person's personal credit, charge or debit card information; bank account information; bank, credit or financial statements; account or PIN numbers and other information relating to personal finances.
  - **Payment card data** - information used to process credit or debit card transactions
  - **Other sensitive or critical data** - any other information whose loss, misuse, or unauthorised access or modification could adversely affect security.

- This Policy should be read in conjunction with CPC's *Councillor Email Guide and Social Media & Electronic Communications policy*.

## **5. Use of computer systems**

- Any Councillor or staff member using a computer, laptop, tablet or similar device for CPC business, whether or not the same is the property of CPC, must ensure that:
  - It is protected by (a) a log-on ID and (b) a secure password of at least eight characters, comprising at least one upper case letter, one lower case letter, one numeral and one symbol (e.g. !, #, £ etc.);
  - It is protected by reputable anti-virus software whenever in use and that any provider updates are promptly installed;
  - It is properly logged-off after use and not left to auto-log-off (or battery expiry);
  - A full back-up routine is carried out after each period of use, onto either the relevant cloud drive or a dedicated USB drive stored securely and itself protected by a secure password as above.

## **6. CPC Equipment**

- In addition to the obligations set out at section 5 above:
  - Other than software from a reputable supplier and which is deemed essential for the effective management of CPC's affairs (for example, Accounting and Payroll programs) no software may be installed onto any CPC Equipment unless this has been approved in advance by the Clerk.
  - Equipment must be kept secure at all times;
  - Faults, defects or malfunctions of any kind must promptly be reported to and/or resolved by the Clerk
  - Upon the request of the Clerk at any time, for any reason, including the termination of your employment, you will immediately return any Equipment and all software to the Clerk (or, in the case of the cessation of the Clerk's employment, to the Chairman).

## **7. Email (internal or external use)**

- Councillors should never communicate anything relating to CPC, its policies and finances, other Councillors, its staff and other CPC-related information (especially but not only Confidential Information) other than via their CPC email account (XXX@crondall-pc.gov.uk)
- Email is not a secure medium of communication: it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If sending Confidential Information by email any attachments must be securely password protected.
- Email messages must not be forwarded unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper memo given its content, then do not forward the email.
- Do not 'Reply All' unless it is appropriate to do so – it only disseminates information unnecessarily and wastes others' time

- As with many other records, email may be subject to discovery in litigation. Like all communications, so not say anything that might appear inappropriate or that might be misinterpreted by a reader.
- Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute unlawful harassment is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.
- Staff will be required to surrender their email account and all of its contents to the Clerk (or in the case of the Clerk, to the Chairman) upon leaving CPC.

## **8. Personal devices**

- When employees and Councillors use their digital devices to access CPC correspondence and other information, they introduce security risk to CPC. It is, however, acknowledged that the parish council does not provide Councillors with devices (laptop, tablet or phone) specifically for parish council use and the use of personal devices for CPC purposes is unavoidable. It is therefore advised that users of personal computers, laptops, tablets and mobile phones should:
  - Keep all devices password protected;;
  - Ensure that anti-virus software is installed and regularly updated;.
  - Ensure their device is not left exposed or unattended.
  - That personal accounts and systems are only logged-in through secure and private networks only.

## **9. General guidance**

Never leave any equipment or data (including but not limited to files, laptops and mobile phones) unattended on public transport or in an unattended vehicle.

## **10. Breach of the policy**

Compliance with this policy is mandatory and forms part of the terms and conditions of employment of staff and part of Councillors' duties. Breach of this policy by staff will be regarded as a disciplinary offence, dealt with under CPCs disciplinary process or a Councillor's breach of duty.

Anyone who considers that there has been a breach of this policy in relation to personal information about them held by CPC should raise the matter via CPCs formal grievance procedure.

## **11. Reporting and Complaints**

Any questions about or issues with the content of this Policy should, in the first instance, be raised in writing to the Parish Clerk ([clerk@crondall-pc.gov.uk](mailto:clerk@crondall-pc.gov.uk)).

## **12. Review and Amendments**

A regular review of this policy will be undertaken to ensure its continued effectiveness, relevance and alignment with legal requirements.