HAUGHLEY PARISH COUNCIL

Security Incident Response Policy

Adopted 16th March 2021

This Council understands that planning for a security incident is essential to ensure that it has a process in place to deal with a security incident at short notice should it occur.

1. **The Security Incident Response Plan below sets out the key issues, which the Council has considered in preparing for a data breach.**

    a) The Clerk should be notified immediately of a suspected data breach and in the absence of the Clerk, the Chairman should be notified.
    b) The Clerk in consultation with the Chairman will take responsibility with delegated authority to manage the data breach. An extraordinary meeting of the Council may be called if required.
    c) The Clerk will consult other data controllers or contractors as a matter of urgency for any external assistance as necessary and this is covered in the Council's Privacy Policy and Subject Access Policy.
    d) The Clerk may, depending upon the nature of the data breach, need to contact others to identify any actual data breach and activate a data breach response team if the extent of the data breach requires.
    e) The Council will review its response plan each year, testing the process with others if required.

2. **Legal issues**

    a) The Council will maintain legal privilege and confidentiality where required.
    b) Should a pause of document destruction processes be required, the Clerk will instruct as necessary.
    c) The Clerk will lead on gathering appropriate evidence and information about the data breach.
    d) The Council if required will contact its external lawyers to manage the investigation and give legal advice.
    e) The Clerk will ensure that steps to manage the investigation are recorded.
    f) Contractual rights and obligations with third parties are set out in the Council's Privacy Policy.
    g) The Council may need to notify third parties as set out in the Council's Data Management Policy and Audit Log.
    h) The Council sets out its contractual rights within its policies and contracts with others.
    i) The Council will contact the Information Commissioners Office ("ICO") and its local law enforcement officer where necessary.
    j) The Council may take advice from its legal advisers on the legal options available to gather evidence from third parties.
    k) The Clerk will consult with its legal advisers and/or insurers on potential liabilities to third parties.

3. **IT**

    a) The Clerk will consult with its IT consultant where required in managing potential risk and responding to a data breach.
    b) The Council's asset register will identify devices where a potential data breach may occur.
    c) The flow of data is set out in the Council's Communications Statement.

d) The Clerk will consult with its IT consultant to quickly secure and isolate potentially compromised devices and data, without destroying evidence should this be necessary.
e) The Clerk will ensure the quick physical security of premises should this be necessary.

4. Cyber breach insurance

a) The Council takes advice from its insurers on cyber breach insurance and actions on notifying and obtaining consents should a breach occur.
b) The Clerk holds emergency contact details.

5. Data

a) Data held by the Council is set out in the Data Management Policy and Audit Log, which includes its classification, destruction time and risk assessments, which includes protections for any sensitive data.
b) The Clerk liaises with its IT consultant, should encryption be necessary.
c) The Clerk will ensure that data is held no longer than required.

6. Data subjects

a) The Council has in place Subject Access Request and Privacy Policies with appropriate notices which are published on its websites: These include notifying data subjects and contractual and legal rights of data subjects.
b) The Council will provide appropriately worded notifications to data subjects.
c) The Council has in place its policies and notices in compliance with GDPR, recognising the potential harm to data subjects should loss of data held by the Council occur.
d) The Council is committed to arranging appropriate training for councillors and staff with includes action in the event of a breach.

7. Public Relations

a) The Council will consult its legal advisers in dealing with data breaches particularly with pro-active and re-active press statements.
b) The Council will put in place arrangements to monitor media reaction as required after any breach.

Changes to this policy
The Council will keep this Security Incident Response Policy under regular review and it will place any updates on its website www.haughleypc.co.uk

Contact Details
Please contact the Parish Council if there are any questions about this Policy or the personal data we hold or to exercise all relevant rights, queries or complaints at:

The Data Controller, Haughley Parish Council, 2 Broomspath Road, Stowupland, Stowmarket, Suffolk, IP14 4DB | Email: clerk@haughleypc.co.uk