Branston Parish Council

Information Security Policy

1.1 Information Security

The availability of complete and accurate information is key to providing excellent services to members of the public, employees, service partners, suppliers and its own operation.

Branston Parish Council have a number of responsibilities to protect their reputation as well as safeguarding individuals from the possibility of information and systems misuse or infringement of personal privacy. Therefore the **confidentiality**, **integrity**, **availability** and **accountability** of this information need to be protected from harm in a way that is proportionate to the risks to the information.

This Information Security Policy provides the overall framework to help everyone play his or her part.

1.2 Scope

The Information Security Policy applies to everyone.

Please note that throughout this document, the words “employee” and “user” are used to cover all the groups of people.

The Information Security Policy applies to **all forms of information**, including, but not restricted to, text, pictures, photographs, maps, diagrams, video, audio, CCTV, which is owned by, administered or controlled by Branston parish council, including information, which is:

- □ Spoken face to face, communicated by fixed line, by mobile telephone
- □ Written on paper or printed out from a computer system. This may include working both on- site or remotely (e.g. at home)
- □ Stored in structured manual filing systems
- □ Transmitted by electronic mail, fax, over the Internet and via wireless technology
- □ Stored and processed via computers, computer networks
- □ Devices, including, but not restricted to, PCs, mobile phones, laptops, tablet PCs, electronic organisers
- □ Stored on **any** type of removable computer media including, but not restricted to CDs, DVDs, USB memory sticks, external hard disks, and memory stores in devices including, but not restricted to, digital cameras, MP3 and MP4 players.

1.3 Purpose

The purpose of the Information Security Policy is:

- To protect the Parish Councils Information and subsequently to protect the Parish Councils reputation
- □ To enable secure information sharing to deliver services
- □ To protect the Parish Council from legal liability and inappropriate use
- □ To encourage consistent and professional use of information and systems

- To ensure everyone is clear about their roles in using and protecting information
- To maintain awareness of information security
- To protect the parish councils employees

1.4 Breaches of the Information Security Policy

Actions or neglect leading to a breach of this policy will be investigated, which could result in disciplinary action; this could include dismissal without notice even for a first offence if sufficiently serious.

In certain circumstances the matter will be referred to the police to consider whether criminal proceedings should be instigated.

Breaches of the Data Protection Act 2018 could result in a hefty fine

1.5 Legal Framework for Information Security

Line managers and individuals have responsibilities regarding the legal use of information. There are many laws and legal rules governing how information is handled. The list below demonstrates the importance of using information correctly.

- Health and Safety at Work Act 1974
- Theft Act 1978
- Indecent display (Control) Act 1981
- Obscene Publications Act 1984
- Copyright, Designs and Patents Act 1988
- Data Protection Act 2018
- Human Rights Act 1998
- Protection of Children Act 1999
- Freedom of Information Act 2000
- Computer Misuse Act 1990

This list is not exhaustive and will change over time.

2. Information Security Roles and Responsibilities

2.1 All information users including all employees, contractors, consultants, volunteers, partners and suppliers must:

1. **Comply with** this Information Security Policy, processes, procedures and guidelines at all times.
2. Comply with legal, statutory, regulatory and contractual obligations related to information at all times.
3. Be familiar with the operation and security requirements of the information and computer systems, to minimise the possibility of harm to **confidentiality**, **integrity** and **availability**.
4. Observe the utmost care when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the parish council without proper authorisation.
5. Report immediately all suspected violations of this and all other security policies, system intrusions, and any other security incidents or weaknesses in security, which might jeopardise the parish council information or information systems, following agreed incident management

policies and processes.

6. Play an active role in protecting information in day-to-day work.

2.2 Parish councillors

1. Approve this highlevel Information Security Policy.
2. Actively promote effective and appropriate information security by the use of structured risk management in all future developments and by appropriate retrospective risk assessment of current processes and systems.
3. Implement and promote Information Security to all staff
4. Ensure that employees understand and abide by the Information Security Policy
5. Provide effective means by which all staff can report security incidents and weaknesses, and act on all such reports according to agreed incident management policies and processes.
6. Apply security controls relating to Human Resources and ensure that job descriptions address all relevant security responsibilities.
7. Provide written authorisation for access to information where appropriate
8. Ensure that communications regarding information security are cascaded effectively to all staff.
9. Ensure that information security is an integral part of all processes.

2.3 Information owners

Data sets may have different owners and where several potential information owners exist, responsibility should be assigned to the group who makes the greatest use of the data

1. Use structured risk assessment to select security controls to protect their information.
2. Monitor to ensure security controls continue to be effective and that information is being handled correctly.
3. Report and act on security incidents and weaknesses
4. Manage the residual risks to their information.

2.4 ICT Services

1. Be the custodian of electronic information in its care by implementing and administering technical security controls
2. Assist Information Owners in identifying technical information security risks and appropriate technical security controls.
3. Provide contingency arrangements for information systems
4. Provide appropriate protection from malicious software.
5. Monitor and report breaches of this policy including unauthorised attempts to access information or systems.
6. Monitor and investigate technical security breaches.
7. Provide technical support to enable compliance with this policy.

3. Information Security Policy

3.1 The Parish council **operates within the law at all times. All users might be held personally responsible for any breach of the law.**

1. All personal information processed electronically or held in a structured manual filing system shall be processed in accordance with the **Data Protection Act 2018**. Utmost care shall be taken when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the parish council without proper authorisation.
2. Advice shall be sought from Data Protection Officer about what information is covered by the Data Protection Act and for detailed guidance about how to handle such information.
3. Personal, confidential or sensitive information **shall be protected** appropriately at all times and in particular when removed from office premises either physically on paper or electronic storage devices, or when transmitted electronically.
4. Personal, confidential or sensitive information shall not be included in the text of e-mails to be sent outside the parish council, unless these are securely encrypted or sent by secure network links. Please be confident that the link is secure before this is used.
5. Any request for information under the **Freedom of Information Act 2000** (FOIA) shall be handled in accordance with the law and processed within 20 working days. Anyone handling FOIA requests shall have completed the appropriate level of training.
6. Information **shall not be used** in any way that might be seen as defamatory, libellous, insulting or offensive by others, Electronic and non- electronic communications shall not contain material that is profane, obscene, indecent, pornographic, defamatory, inflammatory, threatening, discriminatory, harassing (racially, sexually or otherwise offensive), subversive or violent, racist or of an extreme political nature, or which incites violence, hatred or any illegal activity.
7. The parish council shall only use **licensed software** on its computers, and other computing devices.

3.2 Access to information shall be controlled

1 The requirements for **confidentiality**, **integrity**, **availability** and **accountability** shall be determined for all information, from creation to deletion.

2 Structured **information security risk assessment** shall be used to determine the appropriate security controls required to protect information, which are proportionate to the risks to the information and information systems. This risk assessment shall be done as part of system and process development. The effort expended on risk assessment and the amount of formal documentation required shall be proportionate to the perceived risks to the information and the impact of a breach of its security.

3 Access to information shall be **authorised** by management, including sharing information with partners and other organisations. Briefings and formal acceptance of security policies are required **before** access is granted to certain information systems and facilities.

4 Information users shall not attempt to access information to which they do not have **authority**.

5 Information users shall keep personal **passwords** confidential at all times.

6 **Agreements and contracts** with external partners and suppliers shall include the requirement to adhere to this policy, where there is relevance to do so.
All information about the **security arrangements** for parish council and systems and structured manual filing systems is confidential to the parish council and shall not be released to people who are not authorised to receive that information.

3.3 The availability of information shall be protected

1. Business continuity plans shall include all aspects of the parish councils **infrastructure**, which are required to maintain the continuity of all critical business processes and support services. This shall include, but not be limited to, manual filing systems, information systems, information on mobile devices and storage, communications including telephone services, staffing requirements, transport facilities, electricity supply, office accommodation and maps.

3.4 The integrity of information shall be maintained

1. A named individual should have operational responsibility for the ICT systems and procedures
2. The accuracy and completeness of information, including structured manual filing systems, processing methods and computer software shall be **protected** from unauthorised modifications. Users shall not attempt unauthorised modifications.
3. Users shall use only the **officially provided or approved facilities and systems** to access School information.
4. Users shall not interfere with the **configuration** of any computing device without approval
5. Update regularly all devices, which are subject to the threat of **malicious software**, with malicious software scanning software.
6. Update regularly all devices, which are subject to the threat of **security vulnerabilities** with appropriate security patches.

4. Monitoring of the Information Security Policy

The use of electronic and non-electronic information and the use of information systems shall be monitored for the following reasons:

- To ensure that this policy is adhered to and to detect and investigate unauthorised use of information
- To maintain the effectiveness, integrity and security of the computer network
- To ensure that the law is not being contravened

All monitoring shall be:

- Fair and proportionate to the risks of harm to the Council's information and reputation

- Undertaken so as to intrude on users' privacy only as much as is necessary
- Carried out similarly regardless of whether the user is office based or working remotely
- Carried out subject to the requirements of legislation, e.g. Regulation of Investigatory Powers Act 2000. Access to any records of usage shall be stringently controlled.

5. Review of the Information Security Policy

This policy shall be reviewed on a regular basis and at least annually. This policy and its associated policies, processes, procedures and guidelines shall be updated according to:

- Internally generated changes e.g. changes in service strategy, organisation, locations and technology
- Externally generated changes e.g. changes in legislation, security threats, security incidents, recommended best practice and audit reports
- All changes shall be approved by the Parish Council and be made available to everyone to whom it applies.

6– Reporting Information Security Breaches

You must report security incidents and weaknesses to the following people:
Clerk and Chairman. You can make your report by phone, face to face, by email l - whichever you prefer.

Examples of incidents:

Breach of security

- Loss of computer equipment due to crime or an individual's carelessness
- Loss of computer media e.g. memory sticks
- Accessing any part of a database using someone else's authorisation either fraudulently or by accident
- Finding the doors and/or windows have been broken and forced entry gained to a secure room/building that contains service user records

Breach of confidentiality/security

- Finding a computer print out with a header and a person's information on it at a location outside of parish council premises
- Finding any paper records about a service user/member of staff or business of the organisation in any location outside of the parish council premises
- Being able to view service user records in the back (or front) of an employees car
- Discussing service user or staff personal information with someone else in an open area where the conversation can be overheard

7 – Passwords for Staff

1. Never reveal your password to anyone else or ask others for their password.

2. When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you, such as your name or address. Generally, longer passwords are better than short passwords. It is advisable to use a 'strong' password. A strong password is one which contains a combination of upper and lower-case letters, numbers and other punctuation characters. You can substitute numbers and letters for other characters that look similar, such as '3' for 'E', '1' for 'I' or '@' for 'O', '!' for '1' etc. This will help to make your password much more difficult to guess. Remember that passwords are case-sensitive.

3. There is a useful tool that will help identify how strong a password you are using – check your password out at http://www.microsoft.com/protect/yourself/password/checker.mspx

4. Users with administrative level access should ensure that they utilise a complex password – 6 random character/numbers in mixed case.

5. If you forget your password, please request that it be reset from the System Administrator

6. If you believe that someone may have discovered your password, then change it ***immediately***

7. Never use the feature 'Remember password'

8. Change passwords regularly

9. Never leave your computer unattended while using any personal data – if called away you should lock the workstation – this will normally require a password to reopen

10. Never allow another person to login to any system with your login ID and password. Auditing measures in place could result in you being responsible for the actions of another person.

11. Never write your password down and leave it out for others to find.

8 – USB Memory Stick Policy / Removable Hardware

Despite their small size, USB memory sticks have a very large capacity and therefore pose a considerable security risk if they are lost, stolen or abused.

Importance of encryption, protection of equipment e.g. do not leave in a car or unattended.

9– Use of personal devices i.e. Phone, iPads, laptops

All devices must be PIN / Password protected

10- Email security

Unacceptable email activities, sending confidential information securely by email e.g. encryption.

11- Remote access security.

Accessing parish council data from outside the office best practice e.g. being careful about who can see the screen, making sure that all systems are logged out from before leaving the PC etc.

12- Working from home security.

Protection of paper records: e.g. lock them away when not in use. Do not allow family or friends see data. Family and friends should not use parish councils ICT equipment.

13- Backups.

What should be backed up, frequency of backups, security of backup tapes and where they should be held etc.

14 - Printing/scanning/copier security.

Making sure that users make sure that confidential information is not left in devices.

15 - Social Networking.

Detail what is classed as unacceptable behaviour, responsibility of staff to maintain confidentiality.

16 - Asset registers including data assets, hardware assets and software assets.

What should be recorded, who is responsible for recording etc.

17 - Personal Network Storage/Cloud storage.

What the position is in allowing access to PNS sites. What if anything can be stored there. The use of cloud storage for data etc.

18 - Clear desk policy.

Not leaving confidential papers lying on desks, using lockable filing cabinets etc.

19 - Process for allowing third parties access to IT systems.

E.g. Remote support, etc. Detail what assurances should be sought, what level of access should be given, what auditing should be in place etc.

20 - Physical security.

Make sure security badges are checked, visitors credentials checked, windows and doors to secure areas kept locked. Access to keys process etc.

Declaration

The parish council accepts that it must abide by the conditions of use defined in this Information Security Policy.

The understand that misuse of electronic and other communications may lead to consequences, which could be harmful to individuals, the Council, or other organisations. I understand that for certain types of misuse, they may be open to criminal prosecution under the Obscene Publications Act, the Computer Misuse Act or the Data Protection Act.

They understand that in order to ensure that the Information Security Policy is properly followed, and to maintain the effectiveness, integrity and security of the network, the use of electronic communications will be monitored.