1 Down Barn Close
Winterbourne Gunner
Salisbury
SP4 6JP

www.greatbustard.org

Reg. Charity 1092515

The Queen's Award for Voluntary Service

Patron: HM King Charles III

Data Security Policy

Effective from: 2nd October 2025
Review date: 31st December 2026

1. Purpose

The purpose of this policy is to ensure that Great Bustard Group protects personal data and other sensitive information from loss, misuse, unauthorised access, disclosure, alteration, or destruction.

This policy supports compliance with UK data protection law and helps ensure that the information we hold about staff, volunteers, members, donors, partners, and beneficiaries is kept secure.

2. Scope

This policy applies to all staff, trustees, volunteers, contractors, and anyone who processes information on behalf of the Great Bustard Group. It covers all data held by the charity, whether stored electronically, on paper, or in other formats.

3. Principles

The Great Bustard Group will ensure that information is:

- Protected against unauthorised access or disclosure.
- Kept accurate and up to date where necessary.
- Stored securely using appropriate technical and organisational measures.
- Only accessed by individuals who need the information for legitimate organisational purposes.
- Retained only for as long as necessary and disposed of securely when no longer required.

4. Data Security Measures

Access Control

- Access to personal and sensitive data will be restricted to authorised individuals.
- Passwords must be strong, kept confidential, and changed regularly.
- Shared accounts should be avoided wherever possible.

Electronic Data Security

- Computers and devices should be protected with passwords and, where possible, encryption.
- Systems should be kept up to date with security updates and antivirus protection.
- Sensitive information should only be stored on approved organisational systems or secure cloud services.

Physical Security

- Paper records containing personal or sensitive data should be stored in locked cabinets or secure areas.
- Documents should not be left unattended in public or shared spaces.
- Sensitive paper records must be securely shredded when no longer needed.

Data Transmission

- Personal data should only be shared when necessary and through secure methods.
- Care should be taken when sending emails containing personal information.
- Sensitive files should be password protected or encrypted where appropriate.

Use of Personal Devices

- Personal devices used for charity work must have appropriate security measures such as passwords or device locks.
- Sensitive data should not be stored permanently on personal devices unless authorised.

5. Data Breaches

Any suspected or actual data breach must be reported immediately to the Executive Officer or a Trustee.

The charity will investigate breaches promptly and take appropriate action. Where required by law, breaches will be reported to the Information Commissioner's Office within the required timeframe.

6. Responsibilities

- The Board of Trustees has overall responsibility for ensuring appropriate data security arrangements are in place.

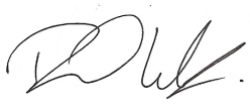
- A designated Data Protection Lead will oversee implementation of this policy.
- Staff and volunteers must follow this policy and handle data responsibly.

7. Training and Awareness

The Great Bustard Group will ensure that staff and volunteers who handle personal data are aware of their responsibilities and receive appropriate guidance or training where required.

8. Monitoring and Review

This policy will be reviewed regularly to ensure it remains effective and compliant with relevant legislation.

Approved by: 

David Waters
Executive Officer

Date: 2nd October 2025