**National Association of City and Town Sheriff of England and Wales (NACTSEW)**

**Data Protection Policy**

**Context and overview**

Key details

\* Policy prepared by: Andrew Swinburne – acting Data Protection Officer

\* Approved by committee: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\* This version of the Policy became operational on: 10.04. 2018

\* Next review date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Introduction

NACTSEW needs to gather and use certain information about individuals the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company’s data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures NACTSEW:

- Complies with data protection law and follows good practice

- Protects the rights of members and any individual or organisation we collect and store data about

- Is open about how it stores and processes individuals’ data

- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 describes how organisations must collect, handle and store personal information. Since the new General Data Protection Regulation (in force from 25 May 2018) includes all organisations, NGO’s, charities etc. NACTSEW must now also comply.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully

2. Be obtained only for specific, lawful purposes

3. Be adequate, relevant and not excessive

4. Be accurate and kept up to date

5. Not be held for any longer than necessary

6. Processed in accordance with the rights of data subjects

7. Be protected in appropriate ways

8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:

* All members
* All speakers

It applies to all data that NACTSEW holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals

- Postal addresses

- Email addresses

- Telephone numbers

- …plus any other information relating to individuals

Data protection risks

This policy helps to protect NACTSEW from some very real data security risks, including:

- Breaches of confidentiality; For instance, - information being given out inappropriately.

- Reputational damage. For instance, the organisation could suffer if hackers successfully gained access to sensitive data.

Responsibilities

All serving committee members of NACTSEW have equal shared responsibility for:

- ensuring data is collected, stored and handled appropriately.

- ensuring that NACTSEW meets its legal obligations.

- evaluating and agreeing upon any third-party services the organisation uses to store or process data. For instance, cloud computing services

- approving any data protection statements, (whether or not) attached to communications such as emails and letters

- ensuring marketing initiatives abide by data protection principles, where necessary

- ensuring all systems, services and equipment used for storing data meet acceptable security standards

The acting Data Protection Officer is responsible for:

* Keeping the committee updated about data protection responsibilities, risks and issues.
* Reviewing all data protection procedures and related policies, in line with an agreed schedule.
* Handling data protection questions from anyone covered by this policy.
* Dealing with requests from individuals to see the data Chester Astronomical Society holds about them (also called ‘subject access requests’).
* Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
* Performing regular checks and scans to ensure security hardware and software is functioning properly.
* Addressing any data protection queries from journalists or media outlets like newspapers.

General committee guidelines

- The only people able to access data covered by this policy should be committee members who need it to carry out their committee role.

- Data should not be shared informally with unauthorised people. When access to confidential information is reasonably requested by anyone outside the committee, committee members must gain the consent of the person(s) concerned before sharing it (except in cases of disclosure to law enforcement agencies as stated later below).

- All matters pertaining to this policy will be discussed in committee meetings periodically to an agreed schedule or when any detail is perceived to be unclear, in order to help committee members understand their responsibilities when handling data.

- Committee members should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, strong passwords must be used and they should never be shared.

- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of. Chester Astronomical Society will delete/ dispose of any individual’s data three years after the last date the individual has any formal connections to the organisation

- Committee members should request help from the acting DPO if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to any committee member.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- Committee members should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.

- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared with unauthorised individuals.

- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.

- Data should only be stored on designated drives and servers, and should only be uploaded to an agreed cloud computing services.

- Data should never be saved directly to PCs, laptops or other mobile devices like tablets or smart phones.

Data use

Personal data is of no value to NACTSEW unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, committee members should ensure the screens of the devices they are viewing the data on are always locked when left unattended.

- Personal data should not be shared informally without the prior consent of the individual concerned on a case by case basis except in certain circumstances where the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. In particular, it should never be sent by email, as this form of communication is not secure.

- Personal data should never be transferred outside of the European Economic Area.

- Committee members should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

* The law requires NACTSEW to take reasonable steps to ensure data is kept accurate and up to date.
* The more important it is that the personal data is accurate, the greater the effort NACTSEW should put into ensuring its accuracy.
* It is the equally shared responsibility of all committee members to take reasonable steps to ensure it is kept as accurate and up to date as possible.
* Data will be held in as few places as necessary. Committee members should not create any unnecessary additional data sets.
* NACTSEW will make it easy for data subjects to update the information NACTSEW holds about them. This will be stated in the GDPR Statement
* Data should be updated as inaccuracies are discovered. For instance, if an individual can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by NACTSEW are entitled to:

- Ask what information the company holds about them and why.

- Ask how to gain access to it.

- Be informed how to keep it up to date on the consent form.

- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a ‘subject access request’.

Subject access requests from individuals should be made by email, addressed to the committee Secretary at cassecretary2@hotmail.com The acting data controller can supply a standard subject request form, although individuals do not have to use this.

Individuals will be charged no fee for a subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, NACTSEW will disclose requested data. However, the DPO will ensure the request is legitimate, seeking assistance from the committee and from the organisation’s legal advisers where necessary.

Providing information

NACTSEW aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used

- How to exercise their rights

To these ends, the NACTSEW has a Data Protection statement, setting out how data relating to individuals is used by the company.

[This is available on request. A version of this statement is also available on the Association’s website.]