

<b>Data protection policy</b>	
<b>Author</b>	Ann Donkin, Chief Executive (Interim)
<b>Division</b>	Senior Management Team
<b>For use by</b>	Staff, Volunteers and Trustees
<b>Purpose</b>	To set out the data protection policy of the Charity
<b>Key related documents</b>	Other policies relating to <i>General Data Protection Regulation (GDPR)</i>
<b>Version date</b>	20 <sup>th</sup> July 2023
<b>Approval date</b>	Governance Sub Committee 20 <sup>th</sup> July 2023
<b>Review date</b>	Q2 2024 / 25 or sooner if any new legislation is introduced

DOCUMENT CONTROL			
DATE	EDITS	EDITOR / REVIEWER	CHANGE CONTROLLER / DOCUMENT OWNER
29 <sup>th</sup> March 2023	Working draft received from external adviser / named DPO	Ann Donkin, Chief Executive (Interim)	Ann Donkin, Chief Executive (Interim)
15 <sup>th</sup> May 2023	First draft for SMT discussion.  <i>Editor</i> check of grammar & spelling.	Ann Donkin, Chief Executive (Interim)	Ann Donkin, Chief Executive (Interim)
20 <sup>th</sup> June 2023	Amended point 5 last bullet point from '12 months' to attend or complete data protection awareness training sessions at intervals 'as appropriate to their role and responsibilities'.  Renumbered incorrect numbering from point 5 onwards.	Ann Donkin, Chief Executive (Interim)	Ann Donkin, Chief Executive (Interim)
20 <sup>th</sup> July 2023	To Governance Sub Committee for approval.	Ann Donkin, Chief Executive (Interim)	Ann Donkin, Chief Executive (Interim)

## **Data protection policy**

### **Age UK Norfolk's Commitment**

The Trustees and staff of Age UK Norfolk (AUKN) are fully committed to follow all UK data protection legislation laws. This includes, but not limited to, the UK *General Data Protection Regulation (GDPR)* and the *Data Protection Act 2018*, in respect of processing personal data and respecting the 'rights and freedoms' of the people whose personal data comes into the possession of AUKN.

#### **1 Policy purpose**

- 1.1 This policy sets out the expectations of AUKN's Trustees and Chief Executive as to how the processing of personal data will be carried out. This policy document refers to other documents (processes and / or procedures) and the latter are to have owners and are subject to change control and review dates.

#### **2 Risks**

- 2.1 The processing of personal data, even in limited quantities, carry risks that cannot be eliminated in their entirety. To monitor and mitigate the impact of risk, a corporate risk register will be maintained noting any risks of potential data protection breaches as appropriate.

#### **3 What are the key risks?**

- 3.1 The key risks are:
- personal data breaches resulting from human error, lack of awareness training and lack of understanding of responsibilities between AUKN and other agencies
  - data protection infringements resulting from inadequate policies, procedures and processes
  - loss of personal data or inability to process it resulting from IT system failures caused by external actors or inadequate defence measures.

## **Data protection policy**

### **4 Policy applicability**

- 4.1 This policy applies to all AUKN staff, volunteers, Trustees and contractors, including those that are part-time, as well as permanent. All parties have a collective responsibility for the proper processing of the personal data for which AUKN is responsible.

### **5 Wider data protection responsibilities**

All personnel covered by this policy have a responsibility:

- to process personal data in accordance with the principles of data protection (see below), any specific requirements set out in this policy and all relevant supporting procedure documents, and to respect the disclosing or sharing of information when it is of a confidential nature
- to report any incidents of unlawful use of personal data, whether intentionally or not, to the designated Privacy Manager (see below). All incidents are treated in confidence in the first instance until such a time that the appropriate action (if required) is established to mitigate the impact of the incident
- to attend or complete data protection awareness training sessions at intervals as appropriate to their role and responsibilities.

### **6 Data protection principles**

- 6.1 AUKN will ensure that the processing of all personal data will be conducted in accordance with the six data protection principles shown below, in so much that personal data will be:

- processed lawfully, fairly and transparently
- collected for a specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary (and no more)
- accurate and, where necessary kept up to date
- kept for no longer than is necessary
- processed in a manner that ensures appropriate security

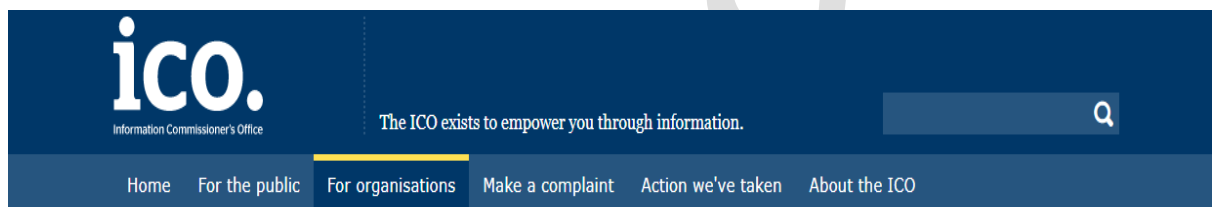
- 6.2 In summary, this means AUKN will be fully accountable for the way it manages and processes personal data, regardless of its source.

### **7 AUKN data protection responsibilities**

- 7.1 The Chief Executive is responsible for the proper management of personal data being processed by AUKN and those covered by this policy.

## Data protection policy

- 7.2 The Chief Executive will appoint a permanent member of staff to serve as the (in-house) Privacy Manager (PM). The appointment will form part of the individual's employment contract. The designated PM, the Head of Corporate Services, will also maintain an incident reporting register.
- 7.3 The Chief Executive may appoint, if it decides to do so, a Data Protection Officer (DPO) whose principal tasks are to provide advice and guidance on the proper management of personal data relating to AUKN's privacy framework. The Chief Executive (Interim) completed the *Information Commissioner's Office (ICO)* questionnaire 'Do I need a Data Protection Officer (DPO)?' on 15<sup>th</sup> April 2023. The results are shown below. It is not intended to appoint a DPO at this time.



[For organisations](#) / Does my organisation need a data protection officer (DPO)?

### Do I need a Data Protection Officer (DPO)?

[Start again](#)

1. Are you a public authority or body?

No

[Change this answer](#)

2. Do your organisation's core activities require regular and systematic monitoring of individuals on a large scale?

No

[Change this answer](#)

3. Do your organisation's core activities involve processing on a large scale 'special categories' of personal data, or 'criminal convictions or offences data'?

No

[Change this answer](#)

Your organisation does not need a data protection officer.

## Data protection policy

### 8 Data protection documentation

8.1 AUKN will provide documentation to cover all data protection related matters including:

- External documentation: this is made available to the general public in accordance with AUKN's legal obligations. The minimum set of documentation used for this includes:
  - a website privacy statement
  - a website cookie policy
  - privacy notices prepared for specific categories of recipients such as, *inter alia*, service users, employees and volunteers, job candidates, suppliers, contractors; and
- Internal documentation: this is for internal use only, that is to say it is not made available to the general public. Such documentation provides the necessary privacy framework by which AUKN can execute the proper and responsible management of personal data processing and provide demonstrable evidence of due diligence/ accountability required by UK legislation. The minimum set of documentation used for this purpose includes:
  - Data protection policy
  - Serious Incident response / breach reporting process
  - Incident Notification Form
  - Staff awareness training and record keeping
  - Security policies covering both IT and physical aspects
  - Data subject access request and other 'rights' procedures
  - Personal data retention schedule
  - Data Protection Impact Assessment Procedure
  - Data processing agreements with third-party data processors
  - Data sharing agreements with organisations considered to be joint controllers
  - Consent Procedures
  - Internal audit policy.

## **Data protection policy**

### **9 Lawful conditions for processing**

9.1 AUKN collects personal data for a variety of reasons and the lawful condition for doing so will vary accordingly. In all instances, it will process personal data using one of the following lawful conditions:

- using consent given prior to processing, subject to the criteria set out in the UK *GDPR*
- to meet contractual obligations
- to comply with all legal/statutory obligations
- when acting in the vital interests of an individual
- when processing is necessary for tasks in the public interest
- for the purposes of our legitimate interests, where it is assessed that such actions do not override the rights and freedoms of the affected individual.

### **10 Where the personal data is processed and stored**

10.1 The routine processing and storage of personal data will be restricted to the UK wherever possible.

### **11 Requesting consent**

11.1 AUKN understands consent to mean any freely given, specific, informed and unambiguous indication of an individual's wishes, by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. In all cases, consent must be valid according to the definition above.

### **12 Change of purpose of processing**

12.1 From the outset, AUKN will state the purpose for which personal data is collected. If this purpose is changed, the affected individuals are to be contacted with the relevant information and further appropriate action will be taken if required. In the case of consent being the original lawful basis, processing of the same personal data against the new purpose is not to commence until either permission has been received or the affected people have been informed. In all other cases, the processing of personal data is not to commence unless justified in writing and the result of due analysis. The exception being where the processing is necessary in the vital interests of an individual, even then a justification will be recorded after the event, in a timely manner, by the PM.

## **Data protection policy**

### **13 Security of all information**

- 13.1 The safeguarding of all information, including personal data, being processed by AUKN is essential to maintain trust with service users, employees, volunteers, contractors and suppliers/ professional support agencies alike.
- 13.2 AUKN operates a 'need to know' principle but will always try to get the right balance between ensuring the privacy of the individual and being able to offer an effective and efficient service to its customers.
- 13.3 Whilst the overall responsibility for the implementation of data protection policies and procedures lies with the PM, all staff and permanent contractors are to be responsible for the personal data they process. This includes, but is not limited to, safeguarding information when not in use and keeping documentation out of sight of those that have no reason to view it.

### **14 IT Security**

- 14.1 A third-party IT support company is primarily responsible for maintaining the confidentiality, availability and integrity of the personal data processed by AUKN. A separate policy document entitled AUKN IT Security Policy will be published to ensure the proper and consistent use of all IT systems including privately owned devices that process AUKN related information. The support company will be subject to a data processing agreement, as set out in A.28 (UK GDPR) either embedded in the contractual agreement for services or as a separate document.

### **15 Physical security**

- 15.1 The application of appropriate physical measures in an organisation is intricate to the responsible processing of information, particularly personal data. AUKN is to adopt a layered approach to physical security such that there is no single point of failure.
- 15.2 An on-site Security Manager (SM) will be appointed who will be responsible for implementing physical security arrangements. The designated SM will be the Head of Corporate Services.



## **Data protection policy**

### **16 Disclosure of data**

- 16.1 Over and above the disclosure of personal data to external bodies identified in the website privacy statement or separate privacy notices, personal data are not to be disclosed to third parties, unless there is a lawful reason to do so, and its disclosure has been authorised by the relevant staff member against a stated lawful basis. In some instances, non-AUKN staff are to sign a confidentiality agreement or Non-Disclosure Agreement (NDA) before AUKN information is made available.
- 16.2 If, subsequently, it is discovered that the disclosure of personal data was deemed to be inappropriate, then this will be reported to the PM and recorded in an incident report. The PM will then decide on further action as required.

### **17 Retention of personal data after the lawful condition for processing it has ended**

- 17.1 AUKN will maintain a data retention policy that provides details as to how long particular categories of personal data can be retained. This information will be reflected in the website privacy statement or relevant privacy notices. Regardless of the source of personal data held by AUKN, once it is no longer needed or there is no lawful condition to process it, it will be reduced, deleted or destroyed in accordance with the retention policy, within 3 months of its scheduled retention date.

### **18 Website use of cookies**

- 18.1 AUKN maintains a website for publicity purposes and as a source of information to potential and actual service users. The website uses cookies to enhance user experience and to collect analytical data of the web browsers used to view the website, but this is only to happen with the users' prior, valid consent.
- 18.2 To facilitate valid consent to the use of non-essential cookies (and similar technologies), the website will use a cookie consent management platform (CMP). This allows users to enable (opt-in) and later disable (opt-out) the use of non-essential cookies. In addition, a cookie policy will be made available on the homepage of each website. This will include a list of the non-essential cookies that could be enabled if the user chooses to do so.
- 18.3 No attempt must be made to identify the individuals, via technical means or otherwise, that visit the website, unless there is a legal requirement to do so.

## Data protection policy

### 19 Individuals' (*data subjects*) rights

19.1 The UK *GDPR* puts great emphasis on transparency of processing and accountability by all parties involved in handling of personal data. It also extends the rights of individuals (referred to as *data subjects*) in respect of their personal data. It should be noted that these are limited and do not apply in all situations. These are shown below:

- right to be informed
- right to access
- right to rectification
- right to erasure ('right to be forgotten')
- right to restrict processing
- right to data portability
- right to object to processing
- rights related to automated decision making and profiling.

19.2 AUKN will ensure that individuals may exercise these rights including the handling of *Data Subject Access Requests (DSAR)* and complaints relating to the processing of an individual's personal data.

### 20 Data transfers

20.1 For those instances where data transfers are needed (meaning international transfers to and from the UK) account must be made of the applicable legislation to effect it lawfully.

### 21 Data deletion when staff leave the Charity

21.1 The PM will ask managers to confirm that, when staff leave the organisation, any personal data is **PERMANENTLY DELETED** by leavers from Charity owned devices. Managers must record that this has been done on the relevant employee's leaver record log on the HR system (currently *PeopleHR*).