Data Security Policy

(As we are continuing to achieve DSP Toolkit certification a name change to this policy is proposed as June 2022 From GDPR and Data Governance Policy to Data Security Policy)
Age UK Surrey (AUKS) manage and process data in accordance with the Data Protection Act 2018 and the UK General Data Protection Regulations (UK GDPR). AUKS handles data/information from a variety of individuals such as contractors, staff (current and past), volunteers and clients both personal and special category data. This document details the data protection principles that must be complied with. Staff must ensure high standards of data quality, data protection, integrity, confidentiality and records management are met in compliance with the relevant legislation and AUKS policies and procedures, To manage the confidential information legally, securely, efficiently and effectively and to deliver the best possible service to our clients. Data is a vital asset, both in terms of the management of staff and clients and in the efficient management of services, resources and performance.

This Policy should be read in conjunction with other relevant policies and procedures the ICT Communications and Monitoring Policy, the Confidentiality Policy and the Control of Documents and Records Procedures. In the documents 'staff' refers to paid staff and volunteers.

This policy has been developed following work carried out in relation to the Caldicott Review, the Data Protection Act 2018, the Freedom of Information Act 2000, data quality, information security, records management and in conjunction with advice and materials provided by the Data Security & Protection Toolkit.

Glossary of terms

Data/Information Governance Management of Data

SIRO:	Senior Information Risk Officer – this post is currently held by the Chief Executive
DPO	Data Protection Officer – this post is currently held by the Finance Manager
Caldicott Guardian:	Guardian of client-identifiable information – title is held by the CEO

1. Principles of Data Governance

AUKS has a need to share information with third parties eg. health organisations and other agencies in a controlled manner consistent with the interests of the client and in some circumstances, the public interest and the need to ensure high standards of data protection and confidentiality to safeguard personal and

commercially sensitive information. There is integral need for electronic and paper information to be accurate, relevant, and available to those who need it.

2. Main Themes

Information Governance is a balance of Openness, Legal Compliance, Information Security and Quality Assurance.

2.1 Openness

- Non-confidential information on Age UK Surrey and its services will be made available to the public through a variety of media
- Employees, volunteers and clients have the right to access information relating to their own records using the procedures laid out in the Data Protection Policy and the Client Information Handling leaflet “What do we use your information for?”

2.2 Legal Compliance

- All identifiable personal information relating to employees, volunteers and clients is confidential. However, confidentiality is not absolute and may be broken in certain circumstances, e.g. to prevent serious crime, danger to a person’s life, danger to others, danger to the community, danger to the health of a person.
- Age UK Surrey will establish and maintain agreements for the controlled and appropriate sharing of client information with other agencies, taking account of relevant legislation. No information is passed to a third party without the service user’s informed consent verbally, or in writing as appropriate.
- Tese policies are maintained to ensure compliance with the Data Protection Act and common law confidentiality. Policies are reviewed and approved by the Board every three years.
- We carry out annual assessments of compliance with legal requirements.

2.3 Information Security

- We have established and maintain policies for the effective and secure management of information assets and resources.
- We undertake annual assessments of information and security arrangements.
- We promote effective confidentiality and data security practice to employees through policies and training.

2.4 We have established and maintain incident reporting procedures and monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

2.5 Information Quality Assurance

- We have established and maintain policies and procedures for information quality assurance and the effective management of records.

- We undertake regular assessments of information quality and records management arrangements.
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services.

3. Implementation

The Board level lead for Information Governance is the Senior Information Risk Officer. Reports on work programmes and action plans will be submitted to the Board on a bi-monthly basis.

AUKS SIRO, Caldicott Guardian and Compliance Team have responsibility for the formulation of Data Governance policies and approve central returns required by the Data Security & Protection Toolkit to the Health and Social Care Information Centre.

The Data Security & Protection Toolkit (DSP Toolkit) will be used by Age UK Surrey to conduct baseline audits and construct action plans to ensure compliance. Service managers have responsibility for dealing with data governance requirements and action plans in individual service areas will be drawn up adhering to DSP Toolkit standards.

Information Governance/Data Security training is provided at the induction training for new staff as a face to face session. Further in depth Data security training will be carried out at the start of employment for office based staff and annually thereafter. This is mandatory.

4. Risk

AUKS will ensure that it operates within a robust Information Governance framework to reduce the risk of threats such as potential litigation, breach of the Data Protection Act and any compromise to client care. Risk assessments will be carried out in the individual component areas as required by the DSP Toolkit with additional Data Governance risk assessments performed as required.

5. Data

Appendix A of this document shows the data Age UK Surrey hold and how it is protected.

- AUKS will obtain, keep and use personal information (also referred to as data) about service users, current and former employees, temporary and agency workers, volunteers, contractors and job applicants for a number of specific and lawful purposes, as set out in the charity's data protection privacy notices.

- AUKS will comply with its data protection obligations and seek to protect personal information relating to its workforce, its clients, and contractors. AUKS will also ensure that staff understand and comply with the rules

governing the collection, use and deletion of personal information to which they may have access.

- AUKS is committed to complying with its data protection obligations and to being concise, clear and transparent about how the charity obtains and uses personal information and how (and when) it deletes that information once it is no longer required.
  The Compliance Team will inform and advise staff on data protection obligations and will monitor compliance with those obligations.

6. Data Protection Principles

AUKS will only process personal data in accordance with the principles of the GDPR. Data will be:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or un-authorised processing, access, loss, destruction or damage

7. Basis for processing personal information

Before processing starts and then regularly while it continues AUKS will:

- review the purposes of the processing activity and select the most appropriate lawful basis (or bases) for that processing, ie:
  - that the data subject has consented to the processing
  - that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
  - that the processing is necessary for compliance with a legal obligation to which AUKS is subject
  - that the processing is necessary for the protection of the vital interests of the data subject or another natural person
  - that the processing is necessary for the purposes of legitimate interests of AUKS or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject
- except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (ie that there is no other reasonable way to achieve that purpose)
  document AUKS's decision as to which lawful basis applies, to help demonstrate the charity's compliance with the data protection principles

include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s)
where special category data is processed, also identify a lawful special condition for processing that information and document it
where criminal offence information is processed, also identify a lawful condition for processing that information and document it.

When determining whether AUKS's legitimate interests are the most appropriate basis for lawful processing, we will:

- conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify any decision

- if the LIA identifies a significant privacy impact, consider whether AUKS also needs to conduct a data protection impact assessment (DPIA)

- keep the LIA under review and repeat it if circumstances change

- include information about AUKS's legitimate interests in the charity's relevant privacy notice(s).

8. Special Category Data

Where AUKS need to process special category data we will only process it if:

- there is a lawful basis for doing so as set out above, eg it is necessary for the performance of the contract, to comply with AUKS's legal obligations or for the purposes of AUKS's legitimate interests

- one of the special conditions for processing special category data applies, eg:

  - the data subject has given explicit consent verbal or written
  - the processing is necessary for the purposes of exercising the employment law rights or obligations of AUKS or the data subject
  - the processing is necessary to protect the data subject's vital interests and the data subject is physically incapable of giving consent
  - processing relates to personal data which are manifestly made public by the data subject
  - the processing is necessary for the establishment, exercise or defence of legal claims
  - the processing is necessary for reasons of substantial public interest.

Before processing any special category data, staff must notify the Compliance Team of the proposed processing, so an assessment can be made whether the processing complies with the criteria noted above. Processing will not take place until:

- the assessment is complete.

- the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

AUKS's data protection privacy notice sets out the types of personal information that AUKS processes, what it is used for and the lawful basis for the processing.

During the recruitment process HR will ensure that (except where the law permits otherwise):

- during the short-listing, interview and decision-making stages, no questions are asked relating to special category data or any data related to protected characteristics such as, age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation.. Any completed equal opportunities monitoring form must be kept separate from the individual's application form and not seen by the person short-listing, interviewing or making the recruitment decision
- if special category data is received, eg the applicant provides it without being asked for it within their CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted

  Identity and 'right to work' checks are carried out at interview stage
  AUKS will only ask health questions once an offer of employment has been made.

During employment HR will process:

- health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance, and facilitating employment-related health and sickness benefits

- special category data for the purposes of equal opportunities monitoring.
- employment data eg staff appraisal, discipline etc

9. Criminal records information

Criminal records information will be processed in accordance with Recruitment of Ex-Offenders and the Recruitment Policy.

10. Data protection impact assessments (DPIAs)

Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where AUKS is planning to use a new form of technology), the charity will carry out a DPIA prior to commencing any processing.

This is to establish:

- whether the processing is necessary and proportionate in relation to its purpose
  the risks to individuals
  what measures can be put in place to address those risks and protect personal information.
  Before any new form of technology is introduced, the manager responsible must arrange with the Compliance Team for a DPIA to be carried out.

11. Documentation and records

AUKS will keep written records of processing activities which are high risk, ie which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information, including:

the name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and DPO) the purposes of the processing a description of the categories of individuals and categories of personal data categories of recipients of personal data where possible, retention schedules where possible, a description of technical and organisational security measures. As part of the charity's record of processing activities AUKS will document, or link to documentation, on:

- information required for privacy notices
  records of consent
  controller-processor contracts
  the location of personal information
  DIPAs
  records of data breaches.
  If AUKS processes special category data or criminal records information, the charity will keep written records of:

the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose
the lawful basis for the charity's processing
whether AUKS retain and erase the personal information in accordance with its policy and, if not, the reasons for not following the charity's policy.

AUKS will conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- carrying out information audits to find out what personal information the charity holds
  distributing questionnaires and talking to staff to get a more complete picture of AUKS's processing activities
- reviewing AUKS's policies, procedures, contracts and agreement to address areas such as retention, security and data sharing AUKS documents its processing activities in electronic form so it can add, remove and amend information easily.

12. Privacy Notice

AUKS will issue privacy notices to inform individuals about the personal information the charity collects and holds relating to the individual, how the latter can expect personal information to be used and for what purposes. These notices will be: a concise, transparent, intelligible and easily accessible form, using clear and plain language.

13. Individual rights

The individual (in common with other data subjects) has the following rights in relation to personal information:

- to be informed about how, why and on what basis that information is processed – please see AUKS's Privacy Policy Notice
  to obtain confirmation that the individual's information is being processed and to obtain access to it and certain other information, by making a subject access request – please see AUKS's subject access request procedure
  to have the data corrected if it is inaccurate or incomplete
  to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten'
  to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but the individual does not want the data to be erased), or where the employer no longer needs the personal information but the individual requires the data to establish, exercise or defend a legal claim
- to restrict the processing of personal information temporarily where the individual does not think it is accurate (and AUKS is verifying whether it is accurate), or where the individual has objected to the processing (and AUKS is considering whether the organisation's legitimate grounds override the individual's interests).

14. Individual obligations - employees

Staff must let HR know if the information provided to AUKS changes, for example a change of address or a change details of the bank or building society account to which an individual's salary is paid.

You may have access to the personal information of other members of staff, suppliers and clients of AUKS in the course of your employment or engagement. If so, AUKS expects you to help meet its data protection and confidentiality obligations to those individuals.

If an individual has access to personal information, the individual must:

- only access the personal information that the individual has authority to access and only for authorised purposes
  only allow other AUKS staff to access personal information if they have the appropriate authorisation

- only allow individuals who are not AUKS staff to access personal information if they have specific authority to do so from the CEO
  keep personal information secure (eg by complying with rules on computer access, password protection and secure file storage and destruction and other precautions set out in AUKS's IT Communications and Monitoring Policy and Control of Records Procedure)
- not remove personal information or devices containing personal information (or which can be used to access it) from AUKS premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes.

Individuals should contact their manager or the Compliance Team if there is any concern or suspicion that one of the following has taken place:

- processing of personal data without a lawful basis for its processing or, in the case of special category data, without one of the conditions set out in paragraph 7/8 being met.
- any data breach as set out in paragraph 16
- access to personal information without the proper authorisation
- personal information not kept or deleted securely
- removal of personal information, or devices containing personal information (or which can be used to access it), from AUKS premises without appropriate security measures being in place
- any other breach of this policy or of any of the data protection principles set out in paragraph 6.

15. Information security

AUKS will use appropriate technical and organisational measures to keep personal information secure by protecting against unauthorised or unlawful processing, accidental loss, destruction or damage of data. These measures may include:

- where possible, personal information is pseudonymised or encrypted ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner
- a process for regularly testing, assessing and evaluating the effectiveness of measures in place for ensuring the security of the processing.

Where AUKS uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard personal information. Contracts with external organisations must provide that:

- the organisation may act only on the written instruction of AUKS
  those processing the data are subject to a duty of confidence
  appropriate measures are taken to ensure the security of processing
  sub-contractors are only engaged with the prior consent of AUKS and under a written contract
- the organisation will assist AUKS in providing subject access and allowing individuals to exercise their rights under the GDPR
  the organisation will assist AUKS in meeting its GDPR obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments
  the organisation will delete or return all personal information to AUKS as requested at the end of the contract

- the organisation will submit to audits and inspections, provide AUKS with whatever information it needs to ensure that they are both meeting their data protection obligations and tell AUKS immediately if it is asked to do something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the CEO.

16. Storage and Retention of Personal Information

Personal information (and special category data) will be kept securely in accordance with AUKS's IT Policy and Control of Records Procedure.

Personal information should not be retained for any longer than necessary. The length of time over which data should be retained will depend on the circumstances, including the reasons why the personal information was obtained. Relevant retention periods are set out in the Control of Records Procedure.

Personal information (and special category data) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

17. Data breach

Examples of a data breach might be:

- loss or theft of data or equipment on which personal information is stored.
- unauthorised access to or use of personal information either by a member of staff or third party
- loss of data resulting from an equipment or systems (including hardware and software) failure.
- human error, such as accidental deletion or alteration of data orsending emails to the wrong address in the contact address book.
- unforeseen circumstances such as fire or flood.
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams.
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

AUKS will:

- make the required report of a data breach to the Information Commissioner's office without undue delay and, within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals. See here https://ico.org.uk/for-organisations/report-a-breach/
- Report major incidents to the Charity Commission as required
- Report to Age UK National as required
- notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

It is imperative that any staff or volunteer identifying a date breach or suspecting a data breach make their Line Manager and Qlic IT support or a member of the compliance team aware as soon as they are able so checks can be made.

18. Consent

If the lawful basis for storing data is consent then it must be freely given, specific, granular, clear, prominent, opt-in, informed and unambiguous, properly documented and easily withdrawn. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must be verifiable and stored with the client data on Charity Log where appropriate.

19. International transfers

AUKS will not transfer personal information outside the European Economic Area (EEA) comprising the countries in the European Union and Iceland, Liechtenstein and Norway.

20. Training

AUKS will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

21. Consequences of failing to comply

Failure to comply with this policy is very serious. It might:

- put at risk the individuals whose personal information is being processed
- carry the risk of significant civil and criminal sanctions for the individual and AUKS
- may, in some circumstances, amount to a criminal offence by the individual and may incur a fine.

An employee's failure to comply with any requirement of this policy may lead to disciplinary action under the charity's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

Review

This policy will be reviewed every three years

Issue	Date agreed by Board of Age UK Surrey	Reviewed
1	Amalgamated Oct 2019 26th November 2019	
2	Name Change	June 2022
3	Name,Minor updates for references and Appendix	

APPENDIX A - AUKS DATA

Asset name/description	Asset Responsibility	Cyber Security	Access Controls	Location	Backup Location	Sent to/Received from
Charity Log	Charity Log & Charity Log Administrators	ISO 27000 ISO9001 Cyber essentials Plus	Two stage password login, restricted access to client information	Rackspace UK datacentre Cloud		Used solely in house, only anonymised data sent to 3rd parties. Extract of Address set out for marketing. Some data agreements for specific projects
Sage 200	Finance Manager, Finance staff, HR & Business Coordinator		Stored on private server, password protected and monitored	Cloud/Stored in house		Used solely in house
Sage Payroll 50	Finance Manager & Finance staff		Stored on private server, password protected and monitored	Cloud/Stored in house		Used solely in house
Paper Records / Client, staff, 3rd parties	All staff, volunteers, 3rd parties		securely locked in cabinets / desk drawers, clean desk at end of day or away for lunch or period of time	Stored in house / regional offices	Server/Kellys	Clients, volunteers, staff, 3rd parties
Emails	All staff, volunteers, 3rd parties	Sophos	Encrypted where sensitive, firewall protected, spam filter and virus protector. MFA	Cloud		Clients, volunteers, staff, 3rd parties
Laptops	Various staff	Sophos Win10 defender	Password protected, controlled via network security policy Spohos or W10 defender	Various	N/A	Clients, volunteers, staff, 3rd parties
Mobile Phones	Various staff		Password protected	Various	N/A	Staff only

APPENDIX A - AUKS DATA

Asset name/description	Asset Responsibility	Cyber Security	Access Controls	Location	Backup Location	Sent to/Received from
NaS Drive?	ICT		Password protected, firewalled, Sophos cloud protection	Clockhouse		Staff only
Sharepoint	Qlic	Cyber Essentials	Password protected, firewalled, panda cloud protection	Cloud	Cloud	Staff only
Salesforce	Salesforce		Password Protected/MFA	Cloud	Another Cloud	Clients, volunteers, staff, Ageuk National
BrightHR BrightBase	BrightHR	Cyber Essentials Plus	Password Protected MFA	Cloud	On personnel drive	Staff only
DBS Checks	Staff member	Regulated website	Staff	Doc Library evidence	Evidence HR BrightHR	Staff/Volunteers
iHASCO	iHASCO	Cyber Essentials	Password Protected MFA	Cloud	On personnel drive	Staff only