CAMBRIDGESHIRE ACRE
DATA PROTECTION POLICY

1. Introduction

1.1. This Policy sets out the obligations of Cambridgeshire ACRE regarding data protection and the rights of its employees, customers, members, partners and other contacts (its 'data subjects') in respect of their personal data under the UK General Data Protection Regulation ('the UK GDPR').

1.2. The UK GDPR defines 'personal data' as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

1.3. This Policy sets out the procedures that are to be followed when processing personal data. Processing is anything done with/to personal data (obtaining, recording, adapting or holding/storing).

1.4. Cambridgeshire ACRE is both the Data Controller ('the Controller'), i.e. the organisation who determines the how and what of data processing and the Data Processor ('the Processor'), i.e. the organisation that processes the data on behalf of the Controller, of its own data. There are instances where Cambridgeshire ACRE acts as the Processor for another Data Controller's data and instances where Cambridgeshire ACRE asks a third party to process data on its behalf.

1.5. The principles and procedures set out in this policy must be followed at all times by Cambridgeshire ACRE's employees, volunteers, trustees or other parties working on its behalf (e.g. contractors).

1.6. Cambridgeshire ACRE is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. Data Protection Officer

2.1. Cambridgeshire ACRE has designated its Head of Business Services as its Data Protection Officer and accountability for data protection matters is included in the job description for this role.

2.2. The current Data Protection Officer is Alison Brown, Head of Business Services, email: alison.brown@cambsacre.org.uk.

3. The Data Protection Principles

3.1. This Policy aims to ensure compliance with the UK GDPR. The UK GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

3.1.1. processed lawfully, fairly and in a transparent manner in relation to individuals;

3.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3.1.3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

3.1.4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

3.1.5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

3.1.6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and

3.1.7. the Controller shall be responsible for, and be able to demonstrate, compliance with the principles. Paragraph 4 sets out how Cambridgeshire ACRE will demonstrate compliance.

4. Cambridgeshire ACRE's compliance with the Data Protection Principles

4.1. In order to demonstrate compliance, the Data Protection Officer keeps an up-to-date written record (an 'information audit') of all personal data collected, held, and processed, which incorporates the following information:

4.1.1. The purposes for which Cambridgeshire ACRE processes the personal data;

4.1.2. Details of the personal data collected, held, and processed by Cambridgeshire ACRE; and the data subject to which that personal data relates;

4.1.3. The lawful basis which Cambridgeshire ACRE is relying on in order to process the personal data (see Appendix 1 for details of the lawful bases under which personal data may be processed);

4.1.4. Details of the privacy notices used to inform data subjects about the purposes for which their data has been collected and their rights under the UK GDPR.

4.1.5. Details of any third parties that will receive personal data from Cambridgeshire ACRE;

4.1.6. Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

4.1.7. Details of how long personal data will be retained by Cambridgeshire ACRE;

4.1.8. Details of how Cambridgeshire ACRE will ensure that personal data is kept accurate and up-to-date; and

4.1.9. Detailed descriptions of all technical and organisational measures taken by Cambridgeshire ACRE to keep personal data secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

5. Data Protection by Design and Data Protection Impact Assessments

5.1. When establishing a new area of work (e.g. a project, service, consultancy agreement, contract or event), staff will be assisted by the Data Protection Officer to integrate data protection into new processing activities. Cambridgeshire ACRE's data protection template contains a requirement for staff to consider the types of personal data that will be collected and processed throughout the life of the project/service, consultancy agreement, contract or event so that this can be added to the organisation's Information Audit spreadsheet. The Data Protection Officer will provide advice on any data protection measures (privacy notices, consents, etc) that will need to be factored into work delivery.

5.2. Cambridgeshire ACRE will also assess any new work area to determine whether a Data Protection Impact Assessment (DPIA) is required under the UK GDPR. A DPIA is a type of audit used to help assess privacy risks and is required in situations where data processing is likely to result in high risk to individuals.

5.3. A DPIA Assessment Checklist (see Appendix 2) will be used to determine whether a DPIA might be required.

5.4. If a DPIA is deemed necessary, it shall be overseen by the Data Protection Officer and shall address the following areas:

5.4.1. The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;

5.4.2. Details of the legitimate interests being pursued;

5.4.3. An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

5.4.4. An assessment of the risks posed to individual data subjects; and

5.4.5. Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the UK GDPR.

6. The Rights of Data Subjects

6.1. The UK GDPR sets out the following rights applicable to data subjects:

6.1.1. The right to be informed;

6.1.2. The right of access;

6.1.3. The right to rectification;

6.1.4. The right to erasure (also known as the 'right to be forgotten');

6.1.5. The right to restrict processing;

6.1.6. The right to data portability;

6.1.7. The right to object;

6.1.8. Rights with respect to automated decision-making and profiling.

6.2. Paragraphs 7 – 15 below set out, in turn, how Cambridgeshire ACRE will ensure data subjects can exercise these rights, where they apply.

7. Cambridgeshire ACRE's compliance with the 'right to be informed'

7.1. Cambridgeshire ACRE provides UK GDPR-compliant Privacy Notices to every data subject when personal data is collected. These Notices include:

7.1.1. Details of Cambridgeshire ACRE including, but not limited to, the identity of its Data Protection Officer;

7.1.2. The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;

7.1.3. Where applicable, the legitimate interests upon which Cambridgeshire ACRE is justifying its collection and processing of the personal data;

7.1.4. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

7.1.5. Where the personal data is to be transferred to one or more third parties, details of those parties;

7.1.6. Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the EEA), details of that transfer, including but not limited to the safeguards in place (see paragraph 19 of this Policy for further details concerning third country data transfers);

7.1.7. Details of the length of time the personal data will be held by Cambridgeshire ACRE (or, where there is no predetermined period, details of how that length of time will be determined);

7.1.8. Details of the data subject's rights under the UK GDPR;

7.1.9. Details of the data subject's right to withdraw their consent to Cambridgeshire ACRE's processing of their personal data at any time;

7.1.10. Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the UK GDPR);

7.1.11. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;

7.1.12. Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

7.2. The information set out above in paragraph 7.1 shall be provided to the data subject at the following applicable time:

7.2.1. Where the personal data is obtained from the data subject directly, at the time of collection;

7.2.2. Where the personal data is not obtained from the data subject directly (i.e. from another party):

7.2.2.1. If the personal data is used to communicate with the data subject, at the time of the first communication; or

7.2.2.2. If the personal data is to be disclosed to another party, before the personal data is disclosed; or

7.2.2.3. In any event, not more than one month after the time at which Cambridgeshire ACRE obtains the personal data.

8. Cambridgeshire ACRE's compliance with the 'right of access'

8.1. A data subject may make a subject access request ('SAR') at any time to find out more about the personal data which Cambridgeshire ACRE holds about them.

8.2. Cambridgeshire ACRE will respond to SARs within one month of receipt.

8.3. All subject access requests received must be forwarded to the Data Protection Officer who will handle them in accordance with Cambridgeshire ACRE's *Policy and Procedure for Handling Subject Access Requests (SARs)* (Appendix 3).

8.4. Cambridgeshire ACRE does not charge a fee for the handling of normal SARs. Cambridgeshire ACRE reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

9. Cambridgeshire ACRE's compliance with the 'right to rectification'

9.1. If a data subject informs Cambridgeshire ACRE that personal data held by the organisation is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt of the data subject's notice.

9.2. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

10. Cambridgeshire ACRE's compliance with the 'right to erase'

10.1. Data subjects may request that Cambridgeshire ACRE erases the personal data it holds about them in the following circumstances:

10.1.1. Where it is no longer necessary for Cambridgeshire ACRE to hold that personal data with respect to the purpose for which it was originally collected or processed;

10.1.2. Where the data subject wishes to withdraw their consent to Cambridgeshire ACRE holding and processing their personal data;

10.1.3. Where the data subject objects to Cambridgeshire ACRE holding and processing their personal data (and there is no overriding legitimate interest to allow Cambridgeshire ACRE to continue doing so) (see paragraph 13 of this Policy for further details concerning data subjects' right to object);

10.1.4. Where the personal data has been processed unlawfully;

10.1.5. Where the personal data needs to be erased in order for Cambridgeshire ACRE to comply with a particular legal obligation.

10.2. Unless Cambridgeshire ACRE has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request.

10.3. In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure.

11. Cambridgeshire ACRE's compliance with the 'right to restrict processing'

11.1. Data subjects may request that Cambridgeshire ACRE ceases processing the personal data it holds about them. If a data subject makes such a request, Cambridgeshire ACRE shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

11.2. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it.

12. Cambridgeshire ACRE's compliance with the 'right to data portability'

12.1. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes. It only applies to personal data an individual has provided to a controller; where the processing is based on the individual's consent or for the performance of a contract and where the processing is carried out by automated means.

12.2. As Cambridgeshire ACRE does not carry out any processing by automated means (see para 14 below), data subjects will not be able to exercise this right.

13. Cambridgeshire ACRE's compliance with the 'right to object'

13.1. Data subjects have the right to object to Cambridgeshire ACRE processing their personal data based on its legitimate interests, processing for direct marketing purposes or processing for scientific and/or historical research and statistics purposes.

13.2. Where a data subject objects to Cambridgeshire ACRE processing their personal data based on its legitimate interests, Cambridgeshire ACRE shall cease such processing forthwith, unless it can be demonstrated that Cambridgeshire ACRE's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

14. Cambridgeshire ACRE's compliance with 'rights in relation to automated decision-making'

14.1. Cambridgeshire ACRE does not use personal data for the purposes of automated decision-making (where decisions are made by automated means without any human involvement).

15. Cambridgeshire ACRE's compliance with 'rights in relation to profiling'

15.1. Cambridgeshire ACRE does not use personal data for profiling purposes (automated processing of personal data to evaluate certain things about an individual).

16. Cambridgeshire ACRE acting as a Data Processor for another Data Controller

16.1. Cambridgeshire ACRE sometimes acts as the Data Processor for another Data Controller's data, for example where we provide a service to a third party.

16.2. The UK GDPR requires that a written contract should exist between the two parties, the Controller and the Processor, so that both parties understand their responsibilities and liabilities.

16.3. The UK GDPR sets out the compulsory details and terms that must be included in any such contracts.

16.4. Cambridgeshire ACRE issues UK GDPR-compliant contracts to any third party Data Controller on whose behalf it processes personal data.

17. Data Protection Measures

17.1. Cambridgeshire ACRE will endeavour to ensure that all employees, volunteers, trustees or other parties working on its behalf (e.g. contractors) comply with the following when processing personal data:

17.1.1. Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hard copies should be shredded and electronic copies should be deleted from the system;

17.1.2. Personal data is transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

17.1.3. Where personal data is to be transferred in hard copy form it should be passed directly to the recipient or sent using Royal Mail recorded delivery;

17.1.4. No personal data may be shared informally and if an employee, volunteer, trustee, or other party working on behalf of Cambridgeshire ACRE requires access to any personal data that they do not already have access to, such access should be formally requested from Cambridgeshire ACRE's Data Protection Officer;

17.1.5. All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked cabinet or similar;

17.1.6. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, volunteers, trustees or other parties at any time. Particular care must be taken when employees are working from home or in a public, shared space;

17.1.7. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it. Particular care must be taken when employees are working from home or in a public, shared space;

17.1.8. All electronic copies of personal data should be stored on Office 365, access to which is secured by password;

17.1.9. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords should be a minimum of 8 characters and should contain a combination of uppercase and lowercase letters, numbers, and symbols. Two factor authentication should be used where offered;

17.1.10. Staff should store their passwords securely.

17.1.11. Through its contract with Chess ICT, Cambridgeshire ACRE's Office 365 applications are backed up through Datto Saas Protection which provides reliable, automatic cloud backups;

17.1.12. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to Cambridgeshire ACRE or otherwise without the formal written approval of Cambridgeshire ACRE's Data Protection Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and

17.1.13. When an employee leaves Cambridgeshire ACRE's employment, their access to Office 365 will be revoked on the day their contract ends.

17.2. Cambridgeshire ACRE holds the Cyber Essentials Certificate. Cyber Essentials is a Government-backed scheme that helps organisations protect themselves against a range of the most common cyber-attacks.

18. Organisational Measures

18.1. Cambridgeshire ACRE shall ensure that the following measures are taken with respect to the processing of personal data:

18.1.1. All employees, volunteers, trustees or other parties working on behalf of Cambridgeshire ACRE shall be made fully aware of both their individual responsibilities and Cambridgeshire ACRE's responsibilities under the UK GDPR and under this Policy, and shall be provided with a copy of this Policy;

18.1.2. Only employees, volunteers, trustees or other parties working on behalf of Cambridgeshire ACRE that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by Cambridgeshire ACRE;

18.1.3. All employees, volunteers, trustees or other parties working on behalf of Cambridgeshire ACRE handling personal data will be appropriately trained to do so;

18.1.4. All employees, volunteers, trustees or other parties working on behalf of Cambridgeshire ACRE handling personal data will be appropriately supervised;

18.1.5. Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

18.1.6. The performance of those employees, volunteers, trustees or other parties working on behalf of Cambridgeshire ACRE handling personal data shall be regularly evaluated and reviewed;

18.1.7. All third parties working on behalf of Cambridgeshire ACRE handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as the relevant employees, volunteers and trustees of Cambridgeshire ACRE arising out of this Policy and the UK GDPR; and

18.1.8. Where any third party working on behalf of Cambridgeshire ACRE handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Cambridgeshire ACRE against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

19. Transferring Personal Data to a Country Outside the EEA

19.1. Cambridgeshire ACRE will not transfer ('transfer' includes making available remotely) personal data to a country outside the EEA.

20. Data Breach Notification

20.1. All personal data breaches must be reported immediately to Cambridgeshire ACRE's Data Protection Officer.

20.2. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer will ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

20.3. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under paragraph 20.2) to the rights and freedoms of data subjects, the Data Protection Officer will ensure that all affected data subjects are informed of the breach directly and without undue delay.

20.4. Data breach notifications shall include the following information:

20.4.1. The approximate number of data subjects concerned;

20.4.2. The categories and approximate number of personal data records concerned;

20.4.3. The name and contact details of the Data Protection Officer (or other contact point where more information can be obtained);

20.4.4. The likely consequences of the breach; and

20.4.5. Details of the measures taken, or proposed to be taken, by Cambridgeshire ACRE to address the breach including, where appropriate, measures to mitigate possible adverse effects.

20.5. The Data Protection Officer will also be responsible for reporting any significant personal data breach as a 'Serious Incident' to the Charity Commission in line with their requirements.

Version in use: Updated to reflect UK GDPR on 10-May-2021

Appendix 1

LAWFUL BASES FOR DATA PROCESSING

The UK GDPR states that processing of personal data shall be lawful if at least one of the following applies:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes **[consent of data subject]**;

2. processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract **[contract with data subject]**;

3. processing is necessary for compliance with a legal obligation to which the Controller is subject **[legal obligation]**;

4. processing is necessary to protect the vital interests of the data subject or of another natural person **[vital interests of data subject]**;

5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller **[public interest]**; or

6. processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child **[legitimate interests]**.

Appendix 2

DATA PROTECTION IMPACT ASSESSMENT (DPIA) ASSESSMENT CHECKLIST

Under the UK GDPR, data protection impact assessments (DPIAs) are mandatory where the processing poses a high risk to the rights and freedoms of individuals. Cambridgeshire ACRE needs to be able to evaluate if a DPIA is required.

This checklist will be used to help the Data Protection Officer make that assessment and sets out some of the issues that may need to be considered in more detail if there is a need to carry out a DPIA.

1. Do you need to carry out a DPIA?

    1.1. What is the objective/intended outcome of the project?

    1.2. Is it a significant piece of work affecting how services/operations are currently provided?

    1.3. Who is the audience or who will be affected by the project?

    1.4. Will the project involve the collection of new personal data about people? e.g. new identifiers or behavioural information relating to individuals

    1.5. Will the project involve combining anonymised data sources in a way that may give rise to a risk that individuals could be identified?

    1.6. Will the project involve combining datasets originating from different processing operations or data controllers in a way which would exceed the reasonable expectations of the individuals?

    1.7. Is data being processed on a large scale?

    1.8. Will the project compel individuals to provide personal data about themselves?

    1.9. Will personal data about individuals be disclosed to organisations or people who have not previously had routine access to the personal data?

    1.10. Will personal data be transferred outside the EEA?

    1.11. Is personal data about individuals to be used for a purpose it is not currently used for, or in a way it is not currently used?

    1.12. Will personal data about children under 13 or other vulnerable persons be collected or otherwise processed?

1.13. Will new technology be used which might be seen as privacy intrusive? (e.g. tracking, surveillance, observation or monitoring software, capture of image, video or audio or location)

1.14. Is monitoring or tracking or profiling of individuals taking place?

1.15. Is data being used for automated decision making with legal or similar significant effect?

1.16. Is data being used for evaluation or scoring? (e.g. performance at work, economic situation, health, interests or behaviour)

1.17. Is sensitive data being collected including:
- 1.17.1. Race
- 1.17.2. Ethnic origin
- 1.17.3. Political opinions
- 1.17.4. Religious or philosophical beliefs
- 1.17.5. Trade union membership
- 1.17.6. Genetic data
- 1.17.7. Biometric data (e.g. facial recognition, finger print data)
- 1.17.8. Health data
- 1.17.9. Data about sex life or sexual orientation?

1.18. Will the processing itself prevent data subjects from exercising a right or using a service or contract?

1.19. Is the personal data about individuals of a kind likely to raise privacy concerns or is it personal data people would consider to be particularly private or confidential?

1.20. Will the project require contact to be made with individuals in ways they may find intrusive?

2. Other issues to consider when carrying out a DPIA

2.1. In addition to considering the above issues in greater detail, when conducting a DPIA, you will also need to look at issues including:
- 2.1.1. The lawful grounds for processing and the capture of consent where appropriate
- 2.1.2. The purposes the data will be used for, how this will be communicated to the data subjects and the lawful grounds for processing
- 2.1.3. Who the data will be disclosed to
- 2.1.4. Where the data will be hosted and its geographical journey (including how data subjects will be kept informed about this)
- 2.1.5. The internal process for risk assessment
- 2.1.6. Who needs to be consulted (data subjects, the Information Commissioners Office (ICO))
- 2.1.7. Data minimisation (including whether data can be anonymised)
- 2.1.8. How accuracy of data will be maintained

2.1.9. How long the data will be retained and what the processes are for deletion of data
2.1.10. Data storage measures
2.1.11. Data security measures including what is appropriate relative to risk and whether measures such as encryption or pseudonymisation can be used to reduce risk
2.1.12. Opportunities for data subject to exercise their rights
2.1.13. What staff (including trustee and/or volunteer) training is being undertaken to help minimise risk
2.1.14. The technical and organisational measures used to reduce risk (including allowing different levels of access to data and red flagging unusual behaviour or incidents)

3. The UK GDPR requires that Cambridgeshire ACRE carry out a DPIA when processing is likely to result in a high risk to the rights and freedoms of data subjects.

4. If two or more of the following apply, it is likely that Cambridgeshire ACRE will be required to carry out a DPIA.

1.	Profiling is in use.	☐
2.	Automated-decision making.	☐
3.	CCTV surveillance of public areas or processing used to observe, monitor or control data subjects.	☐
4.	Sensitive personal data as well as personal data relating to criminal convictions or offences.	☐
5.	Large scale data processing. There is no definition of 'large scale'. However consider: the number of data subjects concerned, the volume of data and/or the range of different data items being processed.	☐
6.	Linked databases - in other words, data aggregation. Example: two datasets merged together, which could "exceed the reasonable expectations of the user" e.g. if Cambridgeshire ACRE merged its mailing list with another rural community council.	☐
7.	Data concerning vulnerable data subjects, especially when power imbalances arise, e.g. staff-employer, where consent may be vague, data of children, mentally ill, asylum seekers, elderly, patients.	☐
8.	New technologies are in use.	☐
9.	Data transfers outside of the EEA.	☐
10.	Unavoidable and unexpected processing.	☐

Appendix 3

CAMBRIDGESHIRE ACRE
POLICY AND PROCEDURE FOR HANDLING SUBJECT ACCESS REQUESTS (SARs)

Policy Statement

1. All subject access requests must be sent, or forwarded immediately, to the Data Protection Officer (Alison Brown, Head of Business Services).

2. The Data Protection Officer will identify whether a request has been made correctly under UK GDPR legislation.

3. Any member of staff who receives a request from the Data Protection Officer to locate and supply personal data relating to a SAR must make a full exhaustive search of the records to which they have access.

4. All the personal data that has been requested will be provided unless an exemption can be applied.

5. Cambridgeshire ACRE must respond within one calendar month after accepting the request as valid.

6. Subject Access Requests will be undertaken free of charge to the requestor unless the legislation permits reasonable fees to be charged.

7. Where a requestor is not satisfied with a response to a SAR, Cambridgeshire ACRE must manage this as a complaint, following Cambridgeshire ACRE's agreed Complaints Procedure.

Procedure

1. The Data Protection Officer will ensure the request has been received in writing and that the data subject is asking for sufficiently well-defined personal data held by Cambridgeshire ACRE relating to the data subject. The Data Protection Officer will clarify with the requestor what personal data they need and will ask him/her to supply their address and valid evidence to prove their identity. Cambridgeshire ACRE accepts the following forms of identification[1]:
    a. Current UK/EEA Passport
    b. UK Photocard Driving Licence (Full or Provisional)
    c. Firearms Licence / Shotgun Certificate
    d. EEA National Identity Card
    e. Full UK Paper Driving Licence
    f. State Benefits Entitlement Document*

[1] * These documents must be dated in the past 12 months, +These documents must be dated in the past 3 months

g. State Pension Entitlement Document*
h. HMRC Tax Credit Document*
i. Local Authority Benefit Document*
j. State/Local Authority Educational Grant Document*
k. HMRC Tax Notification Document
l. Disabled Driver's Pass
m. Financial Statement issued by bank, building society or credit card company+
n. Judiciary Document such as a Notice of Hearing, Summons or Court Order
o. Utility bill for supply of gas, electric, water or telephone landline+
p. Most recent Mortgage Statement
q. Most recent Council Tax Bill/Demand or Statement
r. Tenancy Agreement
s. Building Society Passbook which shows a transaction in the last 3 months and requestor's address

2. The Data Protection Officer will arrange to search emails (including archived emails and those that have been deleted but are still recoverable), documents, spreadsheets, databases, systems, removable media (for example, memory sticks, portable hard-drives), audio recordings, paper records in relevant filing systems etc. for relevant personal data.

3. Personal data will not be withheld if a staff member believes it will be misunderstood; instead, an explanation will be provided with the personal data. Personal data will be provided in an 'intelligible form', which includes giving an explanation of any codes, acronyms and complex terms. The personal data must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort. The Data Protection Officer may be able to agree with the requestor that they will view the personal data on screen if this is deemed appropriate. The Data Protection Officer will redact any exempt personal data from the released documents and explain why that personal data is being withheld.

4. When responding to a SARs request, template letters will be used to ensure correct wording; these can be found in the Appendices to this Policy and Procedure.

5. The Data Protection Officer will maintain a record of SARs received, how they have been dealt with and compliance against the statutory timescale and will report on this annually to the Board of Cambridgeshire ACRE.

6. When responding to a SARs complaint, Cambridgeshire ACRE must advise the requestor that they may complain to the Information Commissioners Office (ICO) if they remain unhappy with the outcome.

Appendices – Template letters for responding to SARs

All letters must include the following information:
(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data;
(d) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with the Information Commissioners Office (ICO);
(g) if the data has not been collected from the data subject: the source of such data;
(h) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Letter 1: Replying to a subject access request providing the requested personal data

[Name]
[Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of [date] making a data subject access request for [subject]. We are pleased to enclose the personal data you requested.

Include (a) to (h) above.

Copyright in the personal data you have been given belongs to Cambridgeshire ACRE. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely

Letter 2: Release of part of the personal data, when the remainder is covered by an exemption

[Name]
[Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of [date] making a data subject access request for [subject]. To answer your request we asked the following areas to search their records for personal data relating to you:

- [List the areas]

I am pleased to enclose [some/most] of the personal data you requested. [If any personal data has been removed] We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you.

You will notice that [if there are gaps in the document] parts of the document(s) have been blacked out. [OR if there are fewer documents enclosed] I have not enclosed all of the personal data you requested. This is because [explain why it is exempt].

Include (a) to (h) above.

Copyright in the personal data you have been given belongs to Cambridgeshire ACRE. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely

Letter 3: Replying to a subject access request explaining why you cannot provide any of the requested personal data

[Name]
[Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of [date] making a data subject access request for [subject].
I regret that we cannot provide the personal data you requested. This is because [explanation where appropriate].

[Examples include where the personal data identifies another living individual or relates to negotiations with the data subject.]

Yours sincerely