Data Protection Policy

Policy summary

CAA-UK (Computer Applications and Quantitative Methods in Archaeology UK Chapter) is a national chapter of the international organisation bringing together archaeologists, mathematicians and computer scientists. Its aims are to encourage communication between these disciplines, to provide a survey of present work in the field and to stimulate discussion and future progress.

To facilitate this, CAA-UK uses personal information to carry out the many functions connected to the running of our yearly conference and membership programme.

CAA-UK therefore collects a wide range of personal data and will endeavour to ensure that they use personal information in line with the expectations and interests of those with whom they come into contact, including their Executive steering boarded, Sub-committees, and members, for the benefit of CAA-UK and in compliance with data protection legislation.

This policy provides guidance on the processing of personal data (collection, use, storage, sharing and disposal) in accordance with data protection legislation. It applies to data that relates to identifiable living individuals stored and used either electronically or on paper. Compliant processing will support effective business operations and minimise the risk of harm to individuals.

Adherence to this policy is mandatory for all CAA-UK Members who use personal data held by CAA-UK.

Contents

Introduction

1. The protection of personal data is enshrined in UK law, but it is also a responsibility that CAA-UK takes seriously. Embedding data protection within the organisation benefits CAA-UK and its members, by enabling uniform and consistent decision making, building a culture of awareness and responsibility, making personal data management and infrastructure more resilient; and, through transparency and accountability, instilling trust and confidence in individuals when they provide us with their data, and ensuring their rights and freedoms are upheld.

2. CAA-UK will comply with applicable legislation, including:

    a. Data Protection Act 2018
    b. General Data Protection Regulation 2016
    c. Human Rights Act 1998, Article 8
    d. The Common Law Duty of Confidence
    e. Privacy and Electronic Communications Regulations 2003
    f. Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011
    g. and other regulatory requirements and applicable guidance.

Purpose

The purpose of this policy is to set out the relevant legislation and to describe the steps that CAA-UK are taking to comply. It is our policy to ensure that our compliance with the relevant legislation is clear and demonstrable at all times.

This policy is also intended to provide CAA-UK with measures for ensuring that risks to individuals through misuse of personal data are minimised, such as:

- personal data being used by unauthorised individuals through poor security or inappropriate disclosure;
- individuals being harmed by decisions made using inaccurate or insufficient data;
- individuals being uninformed by lack of transparency leading to unlawful practice;
- the invasion of privacy due to over-collection or over-retention of data.

Personal data is processed according to the following principles:

1. **Data is processed lawfully, fairly and in a transparent manner** in relation to the data subject through the provision of clear and transparent privacy notices and responses to individual rights requests.
2. **Data is collected for specified, explicit and legitimate reasons** and not further processed for different reasons incompatible with these purposes. CAA-UK will maintain an Information Asset Register and Register of Processing Activities for all Executive positions and committees that will be regularly and consistently reviewed and updated. Data that can be stored and used for archiving purposes in the public interest, scientific or historical research or statistical purposes will be managed by the CAA-UK Executive Steering Committee.
3. **Data is adequate, relevant and not more than is necessary** to complete the task for which it was collected and will be subject to ongoing review and analysis of business purposes, data collection processes and data needs.
4. **Data is accurate and up-to-date** and reasonable steps will be taken to ensure this through regular and consistent data quality checks.

5. **Data is not kept for longer than is necessary** to complete the task for which it was collected, by the implementation of a retention schedule and a regular data cleansing programme.
6. **Data is kept secure, with appropriate technical and organisational measures** to protect against unauthorised or illegal processing, or accidental loss by implementing robust policies and procedures that define the security processes of the organisation and clearly delineate the responsibilities for security within the organisation; regular and consistent training of the executive steering committee; the documentation and implementation of access controls; regular risk assessment of information assets; and the documentation of data access controls across all committees.
7. **Data that is transferred outside the European Union** will only take place with appropriate safeguards to protect the rights of individuals.
8. **Accountability**

   CAA-UK are responsible for, and will demonstrate, compliance with the principles by:

   - Implementing a privacy management framework to embed accountability measures and create a culture of privacy across the organisation;
   - Adopting and implementing data protection policies;
   - Adopting and implementing a Data Protection Impact Assessment process for uses of personal data that are likely to result in high risk to individuals' interests to ensure privacy by design and by default;
   - Put in place written contracts with 3rd Party Processors that process personal data on our behalf;
   - Maintaining a Register of Processing Activities (ROPA);
   - Adopting and implementing a data breach policy and procedure and records and, where necessary, report personal data breaches to the Information Commissioner's Office (ICO);
   - Having a Data Protection Officer for CAA-UK;
   - Implementing regular reviews and reports to the Executive Steering Committee and, where necessary, to update the measures we have put in place.

Scope

This policy applies to CAA-UK as listed, and to any separate entities that fall under its constitution.

CAA-UK

- Executive Steering Committee
- CAA International Ethics Committee
- Local Organisational Teams

CAA-UK require all those processing personal data on behalf of CAA-UK, including their suppliers, partners, contractors and agents, to act in accordance with this policy.

This policy is applicable to and must be followed by all CAA-UK members, including agency workers, consultants, contractors and volunteers. Failure to comply could result in disciplinary action, including the permanent removal of CAA-UK membership, and termination of contracts with contractors, consultants or agency staff.

Definitions

- **Personal Data** - Any information that relates to an identifiable living individual.
- **Special Categories of Personal Data** (also known as sensitive personal data) - Specific types of data that require additional care being taken when processing. The categories are: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.
- **Data processing** – Any activity relating to the collection, recording, organising, structuring, use, amendment, storage, access, retrieval, transfer, analysis, disclosure, dissemination, combination, restriction, erasure or disposal of personal data.
- **Data Protection Impact Assessment (DPIA)** - A process designed to help systematically analyse, identify and minimise the data protection risks of a project or activity.
- **Register of Processing Activities (ROPA)** – A register of all processing activities where personal data is used.
- **Data Subject** - The individual to whom the data being processed relates.
- **Data Controller** - A body or organisation that makes decisions on how personal data is being processed.
- **3rd Party Data Processors** - These are parties that process data on behalf of a Data Controller, they do not have the ability to make any decisions about how the data should be processed. They must always be designated through a Contract or a Data Processing Agreement.
- **Information Asset Register (IAR)** –registers listing all personal and non-personal information assets (bodies of information managed as a single unit), including information ownership, processing activities, information sharing and retention; which is risk assessed to ensure appropriate information assurance is established and maintained.
- **Information Risk Register** – a document containing risks to information security, protection and privacy affecting the organisation and/or individuals, rated for likelihood and impact.
- **Information Sharing Protocol (ISP)** - high-level agreement between Data Controllers describing the terms and conditions under which they will share personal data.
- **Information Sharing Agreement (ISA)** – An agreement that sets out in detail any information sharing arrangements between partners who have signed up to an Information Sharing Protocol.
- **Data Processing Agreement** - Part of a contract of works to be carried out on behalf of a Data Controller, this sets out the terms under which personal data can be shared and processed by the processor.

Policy

Policy Statement

Personal data that CAA-UK collects, uses, stores, transfers, shares and disposes of must be handled in line with the data protection principles listed above in the “purpose” section of this policy.

1. Data Protection Officer

CAA International, the parent organisation of CAA-UK have a Data Protection Officer (DPO), who may also be contacted by emailing gdpr@CAA-UK-international.org.

The DPO is responsible for assisting CAA to monitor internal compliance, to inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the DPA.

The DPO will monitor data sharing agreements, data breaches, information risk, individual rights requests and compliance with data protection policies and procedures. The DPO may require appropriate data protection actions and activities to be undertaken by the executive steering group where necessary.

The DPO reports to the CAA Executive Steering group

The contact details of the DPO should be included in all CAA-UK privacy notices.

2. Collecting personal data

Data protection legislation requires that the collection and use of personal data is fair and transparent. If you acquire any personal data related to an individual (including employees, officer holders, volunteers, suppliers, supporters or other external contacts), either directly from the data subject or from a third party, you must do so in line with the above principles.

If you acquire data in error i.e. that you should not have access to, by whatever means, you must inform a member of the Executive Steering Committee manager, who will assess whether the data should be retained and if so arrange for it to be given to the appropriate individual.

3. Information Asset Register and Register of Processing Activities

All processing of personal data, purposes for processing and lawful reasons must be recorded on the Information Asset Register (IAR), which also constitutes the Register of Processing Activities (ROPA).

4. Privacy Notice

Individuals have the right to be informed about the collection and use of their personal data and CAA-UK will be open and transparent about their use of personal data in line with CAA-UK Privacy Policy.

You must create and maintain privacy notices for all data processing activities relating to personal data and provide this to individuals at the time you collect or significantly amend their personal data.

If you obtain personal data from other sources, you must provide individuals with privacy notices within a reasonable period of obtaining the data and no later than one month. If a decision is made not to inform the data subject e.g. they are the subject of an investigation,

this must be fully documented and the DPO informed. The decision may be added to the Information Risk Register.

Privacy notices that don't comply with CAA-UK' Privacy Notice Policy must be amended and if necessary, reissued or republished.

Failure to issue a valid Privacy Notice where required will be considered an information risk and recorded on the Information Risk Register.

5. Lawful bases

Personal data must not be used unless you are sure that you have identified an appropriate lawful reason to use that data.

There are six available lawful bases for processing (Appendix 1). No single basis is 'better' or more important than the others, you must decide which basis is most appropriate depending on your purpose and relationship with the individual and must state this in your Privacy Notice.

If you are unable to find a suitable lawful basis, you must reconsider the necessity for processing the data, and if it is considered unnecessary you should not undertake it. You **must** have a lawful basis to process personal data.

Legitimate Interest Test

When using legitimate interest as a lawful basis, you should do a Legitimate Interest Assessment (LIA) and record this with your privacy notice. You must be able to produce the LIA if a data subject objects, to justify your continued use of the data. (Appendix 1)

6. Special categories of data

Processing of special category personal data is prohibited unless you have two lawful bases to use such data (Appendix 2) because special category data is more sensitive, and so needs more protection, (i.e. you must have one lawful basis from Article 6 and one lawful basis from Article 9 of the GDPR).

7. Additional conditions for special category data

In certain circumstances the GDPR Implementation Act 2018 imposes additional conditions when processing special category personal data. This includes when processing:

- is necessary for employment purposes or
- is in the substantial public interest

The additional conditions are explained in Appendix 3. You must ensure that you meet these conditions when relevant. If you are uncertain you should contact the Information Governance Officer.

8. Criminal offence data

This is personal data relating to criminal convictions and offences (includes criminal allegations), or related security measures.

To be lawful, the processing must meet the conditions specified by the Data Protection Act in order to be authorised under Dutch law. Further guidance on processing criminal offence data can be found in Appendix 3.

You must ensure that you meet these conditions when relevant. If you are uncertain you should contact the Information Governance Officer.

9. Individual rights

Data protection legislation gives individuals specific rights regarding their personal data:

1. The right to be informed
2. The right to access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object

These rights are defined and explained in the Individual Information Rights Policy.

CAA-UK will facilitate individual rights requests and ensure that action is taken within the legislated timescales.

10. Data Protection Impact Assessment

CAA-UK have adopted the principle of privacy by design. All new projects, updated processes or significantly changed systems that require the use of personal data and may pose a high risk to data subjects, will be subject to a Data Protection Impact Assessment (DPIA).

11. Information Sharing Framework

Information sharing across CAA-UK and between other organisations can play a crucial role in providing better, more efficient conferences to members of CAA-UK and local conference organisers, provided it is done in the right way and for the right reasons. To achieve these aims it is important that we share information across CAA-UK and with other organisations effectively and ethically.

Personal information may also be disclosed to, for instance, the Police, to prevent and detect crime, and prosecute offenders and assess taxes.

When sharing or disclosing personal data you should ensure that:

- You consider the benefits and risks, either to individuals or CAA-UK, of sharing the data, along with the potential results of not sharing the data;
- You are clear about with whom you can share the data. If you are unsure, check with the Information Governance Officer;
- You do not disclose personal data about an individual to an external organisation without first validating you have a legitimate reason to do so. See above - Paragraphs 5, 6 and 7;
- If you must transfer or share data, you do so using appropriate security measures;
- If you are sharing data outside of the Netherlands or the EU, you should take particular care to ensure that the destination country meets all the necessary requirements to protect the data.

If you are unsure whether or not you can share information, you must contact the Information Governance Officer.

Whilst we will support members in taking decisions about information sharing in accordance with their professional judgement, we may take disciplinary or legal action against those who wilfully or recklessly misuse personal data (see paragraph 16 below).

12. Information Sharing Protocol

CAA-UK's information sharing protocol sets out the principles under which information will be shared, whether internally across CAA-UK, or externally, with local conference organisers or with external organisations.

13. Information Sharing Agreements

The mechanism for sharing information under the Information Sharing Protocol is an information sharing agreement which is used to define a set of rules when sharing will take place on a regular basis or on a large scale with a third party.

We will work with our partners to develop agreements for sharing information across multi-organisational structures and will document pre-specified, regular or bulk sharing of information.

14. Third (3rd) Party Processors

CAA-UK uses 3rd party processors and they must comply with the 3rd Party Processor Policy, to ensure that such individuals or organisations are complying with relevant legislation, and to establish a 3rd Party Processing Agreement.

15. Storing and disposing of data

When storing or disposing of personal data, you should ensure that you use the most appropriate and most secure methods available.

You should ensure that:

- In so far as you are able, all personal data in your possession is kept secure from unauthorised access;
- You lock physical files containing personal data in a secure cabinet;
- You are vigilant of your surroundings, if you are undertaking work off-site, and ensure that you do not place any personal data in a position where it can be stolen or lost;
- All devices used to handle personal data are password protected and never share your password with anyone;
- Keep your desk clear of personal data when you are absent.

16. Misuse of Personal Information

It is an offence for a person, knowingly or recklessly, without the consent of CAA-UK to:

- obtain or disclose personal data or the information contained in personal data, or
- procure the disclosure to another person of the information contained in personal data, or
- after obtaining the data, to retain it without the consent of the data controller who collected it.

Unless the disclosure was:

- necessary for the purpose of preventing or detecting crime;
- required by the order of a court or tribunal or authorised by law;
- justified as being in the public interest;
- based on the belief that you had a legal right to obtain, disclose or retain the data;
- based on the belief that the data controller would have consented if they had known.

CAA-UK will act against anyone, who, without good reason, is found to be supplying information to a third party or using information for their own purposes without the consent of CAA-UK, or a reasonable belief that they were working in accordance with the wishes of CAA-UK. Such actions may be criminal offences and may be punished with a fine and/or imprisonment.

Members who are found to have misused personal information may also be subject to compensation claims made by the data subject/s.

If you are asked to disclose personal information in an emergency and are uncertain about doing so, check with the Executive Steering Committee or the Information Governance Officer to get the necessary authorisation. If you are unable to contact any of the above prior to disclosing the information, you must ensure that you inform the Executive Steering Group as soon as reasonably practicable thereafter, in any event no later than 24 hours from the disclosure

17. Fact versus Opinion

When using personal data, you must ensure that you do not write comments about any individual that are unfair, untrue or offensive and that you would not be able to defend if challenged. You must assume that the individual will see anything and everything that you write. This includes emails. Although a certain amount of informality attaches to email writing, it should not be forgotten that these can provide a written record of your comments and they are potentially disclosable to a data subject if they contain personal data.

18. Data Breaches

A personal data breach means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed

You must report suspected or actual personal data incidents or breaches to the Data Protection Officer.

Where a breach is known to have occurred which is likely to result in a high risk to the rights and freedoms of individuals, CAA-UK will report this to the DPA within 72 hours and will co-operate with any subsequent investigation. CAA-UK will contact the affected data subject where it is necessary to do so.

Any data breach reported to the DPA must also be reported at the AGM, by the chair of Executive Steering Committee.

19. Appropriate policy

This policy and related policies comply with the requirements of Chapter 1 of the Data Protection Act 2018

Responsibilities

Executive Steering Committee are responsible for the approval and implementation of this policy and related policies, for informing the trustees, where applicable, of the relevant legislative requirements that may affect their criminal and civil liability; for ensuring that local organisational teams fulfil their responsibilities for data protection, for undertaking their own responsibilities as Information Asset Owners, and for supporting the DPO to undertake necessary tasks and duties.

Data Protection Officer

As stated in the policy, paragraph 1.

Information Governance Officer is responsible for the development of data protection policies, for the regular review and updating of this policy and related policies in line with legislative or organisational changes and ensuring appropriate approval is received; for publication and implementation of these policies across CAA-UK; for providing support, advice and guidance to CAA-UK in relation to these policies, for making the policy and related policies and guidance available to the UK Information Commissioner's Office on request, without charge, and for supporting the Data Protection Officer to undertake necessary tasks and duties.

All CAA-UK members (including volunteers and contractors) are responsible for ensuring they protect the information they create and that they use it appropriately and comply with this policy and related policies designed to secure and protect data and individual privacy. This includes being responsible for the information they create for CAA-UK on personal computer and mobile devices; reporting data breaches and assisting with any investigation of the cause of the breach. They should assist colleagues who are responsible for individual rights requests by providing the necessary information or changes to the information or processing of that information in a timely way. They should only share information where properly authorised so to do and report any receipt of information they are not entitled to have.

APPENDIX 1 – Lawful bases (Article 6)

Consent	**(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
	If Consent is used it must be valid (freely given, unambiguous, actively selected, can easily be withdrawn); Both giving and withdrawing consent must be recorded.
	For consent to be valid, i.e. the correct basis, it must be a choice - so if the data subject refuses to give consent, does that mean that the service can't be provided? If it is an essential service (e.g. pension, payroll etc) then the data controller cannot refuse the service, so there is effectively no choice, so consent is not valid.
Contract	**(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
Legal obligation	**(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
Vital interests	**(d) Vital interests:** the processing is necessary to protect someone's life.
Public task	**(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
Legitimate interest	**(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Legitimate Interest Assessment

When can you rely on legitimate interests?

- When processing is not required by law but is of benefit to you
- When there is a limited privacy impact on the data subject
- When the data subject would reasonably expect your processing to take place

In order to use legitimate interests as your lawful basis for processing, your processing must therefore meet all of the following criteria:

- Have a specific purpose with a defined benefit
- Be necessary – if your defined benefit can be achieved without processing personal data then legitimate interests is not appropriate
- Be balanced against, and not override, the interests, rights and freedoms of data subjects

For further information and assistance seek advice from the Information Governance Officer.

APPENDIX 2 - Special category data lawful bases (Article 9; 10)

Consent	**(a)** the data subject has given explicit consent for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.
Employment	**(b)** processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security or protection.
Vital interests	**(c)** processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
Legitimate activities	**(d)** processing is carried out in the course its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.
Public	**(e)** processing relates to personal data which are manifestly made public by the data subject.
Legal claims	**(f)** processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
Public interest	**(g)** processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
Health & social care	**(h)** processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards.
Public Health	**(i)** processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.
Archiving	**(j)** processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
Criminal Offences	Only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.
	Must have both a lawful basis and either legal authority or official authority for the processing. You must determine your condition for lawful processing of offence data (or identify your official authority for the processing) before you begin the processing, and you should document this.

APPENDIX 3 – Additional conditions for processing special category data

Employment

When relying on Article 9(2)(b) (see Appendix 2) to process employment personal data, you also need to ensure that you have a clear legal basis for performing rights or exercising obligations which are conferred or imposed on you.

You must be able to list the relevant legislation (i.e. which sets out these rights or obligations) in your privacy notice.

If you can't identify the relevant legislation you should seek advice from the Information Governance Officer or the Data Protection Officer.

You also need to have in place what is termed in the Data Protection Act 2018 "an appropriate policy document":

This policy and related policies will be construed as appropriate policy documents and will ensure compliance with the requirements in the (see para 20 Appropriate policy).

You must include reference to these policies in your privacy notice.

Substantial Public Interest

When relying on Article 9(2)(g) and processing personal data in the "substantial public interest", you must also have an appropriate policy document as set out above and this policy and related policies will fulfill this requirement. Similarly, reference to these policies must be made in any privacy notice, (Schedule 1, Part 2 – (Substantial Public Interest Conditions) provides further details). It should be noted that in certain circumstances when relying on "substantial public interest" you may be able to process the data without consent if, for instance, this includes where you are processing special category data in order to prevent or detect any unlawful act, (Schedule 1, Part 2, paragraph 10); or you are protecting members of the public from dishonesty, malpractice or other seriously improper conduct (Schedule 1, Part 2, paragraph 11) or safeguarding children and individuals at risk from harm (Schedule 1, Part 2, paragraph 18). There are many other circumstances listed in Schedule 1, Part 2 where you can process without consent. You must, however, comply with certain conditions before being able to rely on any of the paragraphs contained in Part 2. You must, therefore, seek advice from the Information Governance Officer or the Data Protection Officer.

Criminal Offences

To process criminal offence data, you must satisfy an Article 6 condition and an Article 10 condition of the GDPR. For further information contact the Information Governance Officer.