UKCP Data Protection Policy Statement

[For internal use]

Introduction and purpose

UKCP needs to comply with the requirements of the General Data Protection Regulation (GDPR), and related data protection legislation. The purpose of this policy is to set out the principles of data protection that UKCP adheres to, and what UKCP does to protect data subjects' personal data. UKCP will follow procedures which aim to ensure that all employees, volunteers, and consultants, who have access to personal data held by or on behalf of the UKCP are fully aware of and abide by their duties under the GDPR.

This policy may be amended from time to time to reflect any changes in legislation, regulatory guidance or internal policy decisions.

Scope

This policy applies to anyone who handles personal data on behalf of UKCP, this includes employees, volunteers and consultants.

Responsibilities

UKCP Staff must comply with this policy and with the related policies outlined in this document. Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

Definitions of data protection terms

The following terms will be used in this policy and are defined below.

Data Subjects include all living individuals about whom we hold personal data, for instance an employee or a member. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal Data means any information relating to a living person who can be identified directly or indirectly from that information (or from that information and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can also include an identifier such as an identification number, location data, and an online identifier specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Data Controllers are the people who, or organisations which, decide the purposes and the means for which, any personal data is processed. They have a responsibility to process personal data in compliance with the GDPR and data protection legislation. UKCP is the data controller of all personal data that is processed in connection with UKCP's work and activities.

Data Processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include other organisations such as website hosts, fulfilment houses or other service providers which handle personal data on our behalf. Data Processors also have obligations under GDPR.

European Economic Area (EEA) includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

ICO means the Information Commissioner's Office (the authority which oversees data protection regulation in the UK).

Processing is any activity that involves use of personal data, whether or not by automated means. It includes, but is not limited to:

- Collecting;
- Recording;
- Organising;
- Structuring;
- Storing;
- Adapting or altering;
- Retrieving;
- Disclosing by transmission;
- Disseminating or otherwise making available;
- Alignment or combination;
- Restricting;
- Erasing;
- Destruction of personal data.

Sensitive Personal Data (which is defined as "special categories of personal data" under the GDPR) includes information about a person's:

- Racial or ethnic origin;
- Political opinions;
- Religious, philosophical or similar beliefs;

- Trade union membership;
- Physical or mental health or condition;
- Sexual life or orientation;
- Genetic data;
- Biometric data;
- Other categories of personal data as may be designated “special categories of personal data” under the Legislation.

Data Protection Principles

UKCP needs to collect and use personal information in order to operate and carry out its functions. This personal information must be handled and dealt with in accordance with the principles below. UKCP shall ensure that personal data is:

- Processed fairly, lawfully and transparently, in particular, not processed unless these principles and the rules set out here are followed.
- Obtained only for specified, explicit and lawful purposes, and not processed in any manner incompatible with that purpose or those purposes.
- Adequate, relevant and limited to what is necessary for the purpose for which it is held.
- Processed for a specific purpose or purposes.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary (See Data Retention Policy).
- Processed in accordance with the rights of data subjects under the GDPR.
- Processed in a manner that ensures appropriate security of the personal data.

What is Data Protection?

The GDPR aims to protect individual's fundamental rights and freedoms, notably privacy rights, in respect of personal data processing.

The GDPR applies to paper and electronic records held in structured filing systems containing personal data, meaning data which relates to living individuals who can be identified from the data. Data protection gives data subjects a number of rights as explained further below.

Data Protection Lead (DPL)

The Data Protection Lead is responsible for:

- keeping the Board updated about GDPR responsibilities, risks and issues

- developing, implementing and reviewing the organisation's Data Protection Policy.
- advising on best practice and providing guidance to Data Protection Champions.
- advising and working with the Data Champions to ensure that each department is compliant with GDPR.
- overseeing all requests for information from data subjects including subject access requests.

Data Champions

The Data Champions are responsible for ensuring that their department are maintaining compliance with the UKCP policies on data protection and retention.

Data Champions will:

- Acknowledge initial responses from data subjects and work with the Data Protection Lead to ensure requests are dealt with in line with data protection law and UKCP data protection policies.
- Ensure that personal data within their teams is up to date and destroyed when necessary.

How does UKCP process personal data?

More information about how UKCP observes the data protection principles is set out below. UKCP's Privacy Policy provides further information about how UKCP processes data. However, this section provides an overview. UKCP may process personal data regarding any of the following data subjects:

- Registrant Psychotherapists and Psychotherapeutic Counsellors
- Supervisors, students and trainees
- Complainants, correspondents and enquirers
- Advisors, consultants and other professional experts
- Research subjects
- UKCP Staff
- Volunteers

The types of personal data which are being or which are to be processed include:

- Personal Details
- Education and Training Details
- Website user name and password
- Your preferences of the types of information that you prefer to receive and what types of information about yourself you are willing to share with others
- Offences (including alleged offences)

- Criminal proceedings, outcomes and sentences
- Financial details
- Employment Details

Recipients

Recipients are individuals or organisations to whom UKCP as a data controller intends or may wish to disclose data. This list does not include any person to whom the UKCP as a data controller may be required by law to disclose in any particular case, for example if required by the police under a warrant (in this case, the processing is necessary so that UKCP can comply with a legal obligation to which it is subject).

This list should not be read as a list of those to whom data will be disclosed. UKCP is required to make clear all of the possible categories of 'recipient' to which they might need or wish to disclose data – either in pursuit of their regulatory and public protection functions or in relation to permissions sought from and granted by a data subject or an organisational member.

- Current, past or future employers
- Healthcare, social and welfare advisors or practitioners
- Education, training and accrediting establishments and examining bodies
- Suppliers, providers of goods and services
- Persons making an enquiry or complaint (For example with an organisational member or another regulatory body)
- Police forces
- Central government
- Voluntary and charitable organisations
- Ombudsmen and regulatory authorities

Purposes

The purposes to which UKCP as a Data Controller holds data are described here. This list is not exhaustive and the purposes may change as processes develop.

UKCP holds a range of data types. At various times the data held in respect of these subjects may be used in relation to some or all of the following purposes:

- **Administration of complaints processes** - The administration of complaint and grievance processes of all kinds, including professional disciplinary processes, and complaints against officers, committees

- **Administration of membership records**

- **Administration of data relevant to UKCP Staff** - Internal administration of data relevant to UKCP Staff

- **Advertising marketing and public relations** - Public relations work, advertising and marketing, including host mailings for other organisations and list broking.

- **Education** - The provision of education, training, accreditation and reaccreditation, supervision and/or research as a primary function or business activity.

- **Information and databank administration** - Maintenance of information or databanks as a reference tool or general resource. This includes catalogues, lists, directories and bibliographic databases.

- **Licensing and registration** - The administration of licensing or maintenance of official registers.

- **Realising the objectives of a charitable organisation or voluntary body** - The provision of goods and services in order to realise the objectives of the charity or voluntary body.

- **Research** - Research in any field, including market, health, and lifestyle, scientific or technical research.

Processing data fairly and lawfully

The first data protection principle requires that personal data is obtained fairly and lawfully and processed for purposes that the data subject has been told about. Processing will only be lawful if certain conditions can be satisfied, including where the data subject has given consent, or where the processing is necessary for one or more specified reasons, such as where it is necessary for the performance of a contract. The conditions are:

- The data subject has given their consent to processing (consent must relate to a particular purpose/particular purposes).
- The processing is necessary in order to perform a contract to which the data subject is party, or in order to take steps at the data subject's request prior to entering into a contract.
- The processing is necessary so that UKCP can comply with a legal obligation to which it is subject.
- The processing is necessary to protect the "vital interests" of a data subject or other living individual. In this regard, "vital" means essential for the data subject's life – it is likely to cover, for example, emergency medical situations.

- The processing is necessary for purposes of legitimate interests pursued by UKCP or a third party unless those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (in particular where the data subject is a child).

Much of the processing of personal data held in relation to UKCP members is necessary in order to perform our contract with them. For example, UKCP cannot provide its members with access to the benefits they're are entitled to unless we have their contact details. However, where services offered are optional, UKCP may seek consent to process personal data.

UKCP exercises some functions where it is necessary to process personal data (including that of non-members) for the performance of its regulatory functions. This includes data processed further to UKCP's complaints and conduct process. In these cases, UKCP may rely on its legitimate interests as a body set out to promote and maintain high standards in the profession. In some cases, there will be some prejudice to the rights and freedoms of members who are subject to complaints, as they may be subject to an adverse decision. However, any such prejudice will be outweighed by UKCP's legitimate interests in maintaining high standards in the profession.

UKCP may rely on legitimate interests in other cases, for example in relation to processing of personal data for the purposes of marketing and advertising. This is in our legitimate interests by promoting UKCP and the profession, and any prejudice to data subjects is likely to be minimal.

To comply with the first data protection principle, every time UKCP receives personal data about a person directly from that individual, which UKCP intend to keep, UKCP needs to provide that person with the following "fair processing information":

- The type of information UKCP will be collecting (categories of personal data concerned)
- Who will be holding their information, i.e. UKCP including contact details and the contact details of Data Protection Lead
- Why UKCP is collecting their information and what it intends to do with it (for instance to process their membership application, or send them mailing updates about UKCP activities)
- The legal basis for collecting their information (for example, legitimate interests).
- If we are relying on legitimate interests as a basis for processing what those legitimate interests are.
- Whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of the data subject not providing that data;
- The period for which their personal data will be stored or, where that is not possible, the criteria that will be used to decide that period;
- Details of people or organisations with whom UKCP will be sharing their personal data;
- If relevant, the fact that we will be transferring their personal data outside the EEA and details of relevant safeguards.

UKCP aims to achieve this by using its Privacy Notice, which is available on its website and made available prior to any data subject providing the UKCP with their personal data or, where the personal data is collected from a third party, as soon as reasonably possible thereafter.

Where UKCP obtain personal data about a person from a source other than the person his or her self, it must provide that individual with the following information in addition to that listed above:

- The categories of personal data that we hold
- The source of the personal data and whether this is a public source.

In addition, in both scenarios, (where personal data is obtained both directly and indirectly) UKCP must also inform individuals of their rights, including the right to lodge a complaint with the ICO and, the right to withdraw consent to the processing of their personal data.

This fair processing information can be provided in a number of places including on web pages, in mailings or on application forms. UKCP must ensure that the fair processing information is concise, transparent, intelligible and easily accessible.

Finally, the processing carried out by UKCP must be fair. This includes not acting in a way that would not be reasonably expected by the data subject, for example, because the data subject had been misled about why the personal data was required. Fairness also means not using personal data in a way that have unjustified effects on data subjects

Processing data for the original purpose

The second data protection principle requires that personal data is only processed for the specific, explicit and legitimate purposes that the individual was told about when UKCP first obtained their information.

This means that UKCP should not collect personal data for one purpose and then use it for another. If it becomes necessary to process a person's information for a new purpose, the individual should be informed of the new purpose beforehand. For example, if UKCP collect personal data such as a contact number or email address, in order to update a person about our activities it should not then be used for any new purpose, for example to share it with other organisations for marketing purposes, without first getting the individual's consent.

Personal data should be adequate and accurate

The third and fourth data protection principles require that personal data that we keep should be accurate, adequate and relevant. Data should be limited to what is necessary in relation to the purposes for which it is

processed. Inaccurate or out-of-date data should be destroyed securely, and UKCP must take every reasonable step to ensure that personal data which is inaccurate is corrected.

Not retaining data longer than necessary

The fifth data protection principle requires that UKCP should not keep personal data for longer than it needs to for the purpose it was collected for. This means that the personal data that UKCP hold should be destroyed or erased from our systems when it is no longer needed. If you think that we are holding out-of-date or inaccurate personal data, please speak to your Data Champion.
For guidance on how long particular types of personal data that we collect should be kept before being destroyed or erased, please see the Retention Policy and speak to your Data Champion.

Rights of individuals under the GDPR

The GDPR gives people rights in relation to how organisations process their personal data. Everyone who holds personal data on behalf of UKCP needs to be aware of these rights. They include (but are not limited to) the right:

- to request a copy of any personal data that we hold about them (as data controller), as well as a description of the type of information that we are processing, the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will be stored (known as subject access rights).
- to be told, where any information is not collected from the person directly, any available information as to the source of the information.
- to object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests.
- to have all personal data erased (the right to be forgotten) unless certain limited conditions apply.
- to restrict processing where the individual has objected to the processing.
- to have inaccurate data amended or destroyed.
- to prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else.

If you become aware of a data subject who would like to exercise their rights, please speak to the Data Protection Lead.

Data security

The sixth data protection principle requires that UKCP keeps secure any personal data that it holds. UKCP are required to put in place procedures to keep the personal data that it holds secure, including protection

against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

When UKCP is dealing with sensitive personal data, more rigorous security measures are likely to be needed, for instance, if sensitive personal data (such as details of an individual's health, race or sexuality) is held on a memory stick or other portable device it should always be encrypted.

When deciding what level of security is needed, your starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.

The following security procedures and monitoring processes must be followed in relation to all personal data processed by UKCP:

- Measures to restore availability and access to data in a timely manner in event of physical or technical incident
- Regular (at least weekly) back-ups should be taken of all data on the system and storing data on local drives or removable media should be avoided where possible, as these will not be backed up
- UKCP Staff should ensure that individual monitors do not show confidential information or sensitive personal data to passers-by and that they log off from their PC when it is left unattended
- Paper documents should be shredded, memory sticks, and other media on which personal data is stored should be physically destroyed when they are no longer required
- Personal data must always be transferred in a secure manner (the degree of security required will depend on the nature of the data - the more sensitive and confidential the data, the more stringent the security measures should be)
- Other measures to ensure confidentiality, integrity, availability and resilience of processing systems
- Desks and cupboards should be kept locked if they hold confidential or sensitive personal data
- UKCP Staff must keep data secure when travelling or using it outside the offices
- UKCP operates a system of data anonymisation when processing personal data to collect statistics on the activities facilitated by its website.

Transferring Data outside of the EEA

The GDPR requires that when organisations transfer personal data outside the EEA, they take steps to ensure that the data is properly protected. UKCP may transfer personal data outside the EEA in the following circumstances:

- Where it uses cloud storage to back up its servers
- Where it uses service providers who are based outside the EEA

The European Commission has determined that certain countries provide an adequate data protection regime. These countries currently include Andorra, Argentina, Canada, Guernsey, Isle of Man, Israel, New Zealand, Switzerland, Faroe Islands, Jersey and Uruguay, but this list may be updated.

As such, personal data may be transferred to people or organisations in these countries without the need to take additional steps beyond those you would take when sharing personal data with any other organisation. In transferring personal data to other countries outside the EEA (which are not on this approved list), it will be necessary to enter into an EC-approved agreement, seek the explicit consent of the individual, or rely on one of the other derogations under the GDPR that apply to the transfer of personal data outside the EEA.

The EU-US Privacy Shield is an instrument that can be used as a legal basis for transferring personal data to organisations in the US, although specific advice should be sought from the Data Protection Lead before transferring personal data to organisations in the US.

Please note that this section may need to be revised depending on the outcome of the UK's negotiation with the EU as part of the Brexit process. For more information, please speak to the Data Protection Lead.

Processing sensitive personal data

In addition to the lawful bases for processing personal data described above, UKCP must comply with an additional condition in respect of sensitive personal data. Sometimes this will involve obtaining explicit consent from the individuals involved. There are a limited number of other circumstances in which the GDPR permits organisations to process sensitive personal data, including processing which:

- Is in compliance with employment law obligations
- Is necessary to protect the vital interests of the data subject
- Relates to information made public by the data subject
- Is necessary for legal advice and establishing/defending legal rights
- Is necessary for reasons of substantial public interest (as defined in Schedule 1 to the Data Protection Act 2018)

There are also particular rules about personal data relating to criminal convictions and offences or related security measures, where reasons of substantial public interest can also be relied on

As with any other type of information UKCP will also have to be absolutely clear with people about how it is going to use their information

Note that in some cases we may process "special categories" of personal data, and information about criminal convictions and offences. For example:

- Information in relation to our employees (such as health data), which is necessary for the performance of our contract with them or under employment law (in the case of our volunteers, we obtain their consent to process these types of information)
- Information in relation to our members (for example, whether they have criminal convictions) which is necessary to uphold high standards in the profession and to protect the public (a reason of substantial public interest)
- Information provided by complainants (such as health data), which is necessary in order to process complaints and therefore protect the public (a reason of substantial public interest).

The reason of substantial interest above is that processing information about whether members have criminal convictions and processing special categories of personal data from complainants in order to consider a complaint are necessary in our role as a regulator to protect members of the public from dishonesty, malpractice or other seriously improper conduct, and unfitness or incompetence. Sometimes it is necessary to carry out these checks or investigate a complaint without the consent of the data subject concerned (for example, if members were able to refuse consent to give conviction information, there would be a risk of unsuitable individuals being register as members; equally, if we cannot investigate complaints without consent there may be a danger to the public in respect of unsuitable individuals practising)

The Data Protection Act 2018 requires us to have in place an appropriate policy document in respect of these types of processing. The appropriate policy document must explain UKCP's procedures for securing compliance with the data protection principles in connection with the processing of personal data in reliance on the condition in question (in this case, substantial public interest). These have been set out above in this policy. In addition, particular security measures are applied in respect of the above information. Information regarding complaints is only accessible initially by the complaints team, who will consider whether it is necessary to use the information as part of the investigation (in which case it may need to be disclosed to the relevant member, and those dealing with the investigation and deciding the complaint. As well as being mentioned in our privacy policy, the fact that this information may be used is drawn to the attention of complainants after they submit a complaint

The appropriate policy document must also explain UKCP's policies as regard the retention and erasure of personal data processed in reliance on the condition in question (in this case, substantial public interest), giving an indication of how long such personal data is likely to be retained. UKCP has a retention policy which sets out this information. However, information on unsuccessful applicants for membership regarding criminal offence data is normally kept for 6 years before being deleted, in order to deal with any complaints or claims

about how UKCP have dealt with their application, and so that UKCP is aware for the purposes of subsequent applications for membership. In the case of successful applications, UKCP keeps information for the duration of the membership and 6 years after, in case of any legal claims. In relation to sensitive personal data regarding complainants, UKCP usually keeps this for 6 years after the complaint has been decided, in case of any legal claims arising

This policy (together with the data retention policy) meets the requirements of an 'appropriate policy document', provided that, for the duration of the processing in reliance on one of the above conditions, and for 6 months after that processing ceases:

- UKCP retains and periodically reviews this document; and
- Makes it available to the ICO on request

If you are concerned that you are processing sensitive data outside of the circumstances above, please speak to the Data Protection Lead

Entering into contracts with data processors

UKCP uses data processors to carry out certain data processing activities on its behalf – for example, to produce and send surveys or UKCP's magazine. Where UKCP engages data processors, there are a number of obligations it must comply with:

- Where the activities undertaken pursuant to a data processing contract involve transferring personal data outside of the EEA, please refer to the section on Transferring Data outside the EEA above.

- UKCP may only use data processors who offer sufficient guarantees to meet the requirements of GDPR and protect data subjects' rights. In general, where you are instructed to perform a task in relation to a data processing agreement by a senior member of staff, you may assume that the UKCP is satisfied that the data processor in question has provided sufficient guarantees. However, if you have any reason to doubt:

    i. that sufficient guarantees have been given, and/or
    ii. that the data processor in question is complying with its obligations under the data processing agreement or GDPR, and/or
    iii. that the person instructing you is senior enough to know with certainty that UKCP is satisfied that data processor has offered sufficient guarantees; please contact the Data Protection Lead in the first instance.

- UKCP must enter into a written agreement with the data processor which sets out (i) the subject matter, duration, nature and purpose(s) of the processing; (ii) the type(s) of personal data and (iii) the categories of data subjects which will be processed.

- In relation to the data processor, the data processing agreement must provide:

  i. that the data processor will not engage another data processor without the prior specific or general written authorisation of UKCP.
  ii. that the data processor will only process personal data based on documented instructions from UKCP.
  iii. that the person(s) authorised to process the personal data on UKCP's behalf commit to the confidentiality of the personal data.
  iv. that the data processor will take organisational and technical security measures appropriate to the nature, scope, context and purposes of processing, the type(s) of personal data involved and the associated risks to data subjects;
  v. that the data processor will facilitate UKCP's obligations to comply with data subjects' request to exercise their rights as detailed above;
  vi. that, bearing in mind the nature of the processing and information available to the data processor, the data processor will assist UKCP in complying with the following obligations:

     A. UKCP's security obligations as set out above
     B. UKCP's obligation to report security breaches as set out in below – in particular, the data processor must notify the UKCP without undue delay after becoming aware of a security breach and, where appropriate, must provide information as to the nature of the breach, the categories and approximate numbers of data subjects involved and the measures taken to mitigate potential adverse effects; and
     C. Where appropriate, conducting a data protection impact assessment ("DPIA") and/or consulting with the ICO prior to commencing processing likely to result in a high-risk to the rights and freedoms of natural persons. To the extent that UKCP conducts a DPIA and/or consults with the ICO and you become involved, you will receive appropriate training and information at the relevant time.

  vii. that the data processor is obliged, at the choice of UKCP, to delete or return all the personal data concerned to UKCP at the end of the provision of data processing services.

  viii. makes available to the UKCP all information necessary to demonstrate compliance with obligations under GDPR.

- In general, if you have any reason to believe that the UKCP and/or the relevant data processor is not

complying with its obligations, or that the underlying agreement does not comply with GDPR, please contact Information Compliance Lead in the first instance.

The role of the ICO

UKCP recognizes that whilst there is no obligation to make an annual notification to the ICO under the GDPR, it will consult with the ICO where necessary when we are carrying out "high risk" processing.

UKCP will report breaches (other than those which are unlikely to be a risk to individuals) to the ICO where necessary, within 72 hours. UKCP will also notify affected individuals where the breach is likely to result in a high risk to the rights and freedoms of these individuals. More information is available in the data breach policy. Please contact the Data Protection Lead if you think there may have been a data breach.

Record keeping

We must keep a record of our data processing activities, to demonstrate that we are complying with them. These records will include the purpose of processing, descriptions of categories of data subjects and categories of personal data, details of transfers to third countries and retention periods of personal data.

Monitoring and review of the policy

This policy is reviewed regularly to ensure that it is achieving its objectives.

Other relevant documents related to this policy:

(b) Subject Access Request
(c) Retention
(d) Data Breach Reporting