Ark Data Protection Policy

PURPOSE

This Ark policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the EU General Data Protection Regulation ("the GDPR") and other related legislation. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically. It applies to all data held by the charity Ark (legal name Absolute Return for Kids [ARK]) and its wholly owned subsidiary company Ark UK Programmes Limited, including data held by Ventures supported by Ark Ventures.

Date of last review:	April 2018	Author:	Governance Manager
Date of next review:	April 2021	Owner:	Director of Governance
Type of policy:	☒ Network-wide ☐ Tailored by school	Approval:	Board
School:	N/A	Key Contact Name:	Governance Team
Key Contact Email:	governance.team@arkonline.org	Key Contact Phone:	0203 116 6333

Contents

1. Introduction

1.1. As a charity, Ark collects and uses certain types of personal information about staff, beneficiaries, clients and other individuals who come into contact with the organisation in order to deliver public benefit. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (GDPR) and other legislation.

1.2. The GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

1.3. This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed every 3 years.

2. Roles and responsibilities

2.1. Ark and its wholly owned subsidiary company Ark UK Programmes Limited are both registered data controllers. The Ark board is ultimately accountable for ensuring that Ark complies with all relevant legislation including for data protection. Data protection sits under the remit of the Ark Director of Governance.

2.2. The Information Governance Manager is responsible for overall coordination of data protection including ICO registration and overseeing responses to subject access requests.

2.3. Individual teams, including those leading Ventures incubated by Ark, are responsible for ensuring that this policy and related procedures are followed.

2.4. The wider staff body are made aware of this policy and their duties under GDPR as part of their induction to Ark. In addition, regular training opportunities are made available to staff, in particular those for whom data protection is of particular relevance to their role.

3. Personal data

3.1. 'Personal data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1]. A sub-set of personal data is known as 'special category personal data'. This special category data is information that reveals:

- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- an individual's sex life or sexual orientation;
- genetic or biometric data for the purpose of uniquely identifying a natural person.

3.2. Special Category Data is given special protection, and additional safeguards apply if this information is to be collected and used.

3.3. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

[1] For example, if asked for the number of female employees, and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website.

3.4. Ark does not intend to seek or hold Special Category Data (previously known as sensitive personal data) about staff, beneficiaries, clients or other individuals except where we have been notified of the information, or it comes to the attention of our teams via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff, beneficiaries, clients or other individuals are under no obligation to disclose to Ark their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and/ or parenthood are needed for other purposes, e.g. pension entitlements).

4. Data protection principles

4.1. The six data protection principles as laid down in the GDPR are followed at all times:

4.1.1. personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;

4.1.2. personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

4.1.3. personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;

4.1.4. personal data shall be accurate and, where necessary, kept up to date;

4.1.5. personal data processed for any purpose(s) shall not be kept in a form which permits identification of individuals for longer than is necessary for that purpose / those purposes;

4.1.6. personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

4.2. In addition to this, Ark is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 6-8 below).

4.3. Ark is committed to complying with the principles in 4.1 at all times. This means that Ark will:

4.3.1. inform individuals about how and why we process their personal data through the privacy notices which we issue;

4.3.2. be responsible for checking the quality and accuracy of the information;

4.3.3. regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention schedule;

4.3.4. ensure that when information is authorised for disposal it is done appropriately;

4.3.5. ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;

4.3.6. share personal information with others only when it is necessary and legally appropriate to do so;

4.3.7. set out clear procedures for responding to requests for access to personal information known as subject access requests;

4.3.8. report any breaches of the GDPR in accordance with the procedure in paragraph 9 below.

5. Conditions for processing in the first Data Protection principle

5.1. The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.

5.2. The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.

5.3. The processing is necessary for the performance of a legal obligation to which we are subject.

5.4. The processing is necessary to protect the vital interests of the individual or another.

5.5. The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us.

5.6. The processing is necessary for a legitimate interest of the charity or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned.

6. Use of personal data by Ark

6.1. Ark, our subsidiary company Ark UK Programmes Limited, and individual Ventures process personal data on staff, beneficiaries, clients and other individuals. In each case, the personal data must be processed in accordance with the data protection principles as outlined in paragraph 4.1 above.

Staff

6.2. The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks and photographs, as well as information required to administer your terms and conditions of employment.

6.3. The data is used to comply with legal obligations placed on Ark as a charity in relation to employment. Ark may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

6.4. Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

6.5. Any wish to limit or object to the uses to which personal data is to be put should be notified to the Ark Information Governance Manager who will ensure that this is recorded, and adhered to if appropriate. If the Ark Information Governance Manager is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the charity cannot comply with their request.

Beneficiaries, clients and other individuals

6.6. Each programme run by, or hosted within, Ark will hold information on beneficiaries, in particular in order to understand programme impact in line with charitable obligations to demonstrate public benefit. Ark holds personal data on clients to provide a service and fulfill the obligations set out in our contracts. The level and detail of information held varies by programme – data is anonymised wherever possible, and is held securely. Each programme publishes a privacy notice tailored to their audience to clearly explain how data is held and processed.

6.7. The charity may hold personal information in relation to other individuals who have contact with the organisation, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.

7. Security of personal data

7.1. The charity will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR. The charity will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

7.2. For further details as regards security of IT systems, please refer to the ICT Policy. Ark's Incident Response Strategy outlines how data kept on Ark's servers/ cloud-based storage will be kept secure, and then recovered, in the event of a major incident.

8. Disclosure of personal data to third parties

8.1. The following list includes the most usual reasons that the charity will authorise disclosure of personal data to a third party:

8.1.1. To give a confidential reference relating to a current or former employee, volunteer or beneficiary;

8.1.2. for the prevention or detection of crime;

8.1.3. for the assessment of any tax or duty;

8.1.4. where it is necessary to exercise a right or obligation conferred or imposed by law upon the charity (other than an obligation imposed by contract);

8.1.5. for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

8.1.6. for the purpose of obtaining legal advice;

8.1.7. for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress)

8.1.8. should concerns be raised by a beneficiary that must be disclosed for safeguarding reasons

8.2. Ark and our Ventures may receive requests from third parties (i.e. those other than the data subject, Ark, and employees of Ark) to disclose personal data it holds about beneficiaries, staff, clients or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned, Ark or our Ventures.

8.3. All requests for the disclosure of personal data must be sent to the Ark Information Governance Manager, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

9. Subject access requests

9.1. Anybody who makes a request to see any personal information held about them by Ark or an individual Venture is making a subject access request. All information relating to the individual, including that held in electronic or manual files, should be considered for disclosure, provided that they constitute a "filing system" (see clause 1.2).

9.2. The individual's full subject access right is to know:

- Whether personal data about him or her are being processed
- The purposes of the processing
- The categories of personal data concerned

- The recipients or categories of recipient to whom their personal data have been or will be disclosed
- The envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data are stored
- The existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing
- The right to lodge a complaint with the Information Commissioner's Office
- Where the personal data are not collected from the individual, any available information as to their source
- Details of the safeguards in place for any transfers of their data to locations outside the European Economic Area

9.3. All requests should be sent to sar@arkonline.org within 3 working days of receipt, and must be dealt with in full without delay and at the latest within one month of receipt.

9.4. Where a child or young person who is a beneficiary of Ark does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Information Governance Manager must, however, be satisfied that:

9.4.1. the child or young person lacks sufficient understanding; and

9.4.2. the request made on behalf of the child or young person is in their interests.

9.5. Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the charity must have written evidence that the individual has authorised the person to make the application and the Information Governance Manager must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

9.6. Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

9.7. A subject access request must be made in writing. The charity may ask for any further information reasonably required to locate the information.

9.8. An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

9.9. All files must be reviewed by the Information Governance Manager before any disclosure takes place. Access will not be granted before this review has taken place.

9.10. Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

10. Exemptions to access by data subjects

10.1. Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

10.2. There are other exemptions from the right of subject access. If we intend to apply any of them to a request then we will usually explain which exemption is being applied and why.

11. Other rights of individuals

11.1. The charity has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the charity will comply with the rights to:

11.1.1. object to Processing;

11.1.2. rectification;

11.1.3. erasure; and

11.1.4. data Portability.

Right to object to processing

11.2. An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (grounds 5.5 and 5.6 above) where they do not believe that those grounds are adequately established.

11.3. Where such an objection is made, it must be sent to the Ark Information Governance Manager within 2 working days of receipt, who will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

11.4. The Ark Information Governance Manager shall be responsible for notifying the individual of the outcome of their assessment within twenty of working days of receipt of the objection.

Right to rectification

11.5. An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the Ark Information Governance Manager within 2 working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

11.6. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of a review under the data protection complaints procedure, or an appeal direct to the Information Commissioner.

11.7. An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

11.8. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

11.8.1. where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;

11.8.2. where consent is withdrawn and there is no other legal basis for the processing;

11.8.3. where an objection has been raised under the right to object, and found to be legitimate;

11.8.4. where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);

11.8.5. where there is a legal obligation on the charity to delete.

11.9. The Ark Information Governance Manager will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to

other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

11.10. In the following circumstances, processing of an individual's personal data may be restricted:

11.10.1. where the accuracy of data has been contested, during the period when the charity is attempting to verify the accuracy of the data;

11.10.2. where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

11.10.3. where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;

11.10.4. where there has been an objection made, pending the outcome of any decision.

Right to portability

11.11. If an individual wants to send their personal data to another organisation they have a right to request that the charity provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where the charity is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to the Ark Information Governance Manager within 2 working days of receipt, who will review and revert as necessary.

12. Breach of any requirement of the GDPR

12.1. Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is/ they are discovered, to the Ark Information Governance Manager.

12.2. Once notified, the Ark Information Governance Manager shall assess:

12.2.1. the extent of the breach;

12.2.2. the risks to the data subjects as a consequence of the breach;

12.2.3. any security measures in place that will protect the information;

12.2.4. any measures that can be taken immediately to mitigate the risk to the individuals.

12.3. Unless the Ark Information Governance Manager concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the charity, unless a delay can be justified.

12.4. The Information Commissioner shall be told:

12.4.1. details of the breach, including the volume of data at risk, and the number and categories of data subjects;

12.4.2. the contact point for any enquiries (which shall usually be the Ark Information Governance Manager);

12.4.3. the likely consequences of the breach;

12.4.4. measures proposed or already taken to address the breach.

12.5. If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Ark Information Governance Manager shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

12.6. Data subjects shall be told:

12.6.1. the nature of the breach;

12.6.2. who to contact with any questions;

12.6.3. measures taken to mitigate any risks.

12.7. The Ark Information Governance Manager shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed at board level and a decision made about implementation of those recommendations.

13. Contact

13.1. If anyone has any concerns or questions in relation to this policy they should contact the Ark Information Governance Manager via dataprotection@arkonline.org.

13.2. If you are not satisfied with the assistance that you get or if we have not been able to resolve your complaint and you feel that a formal complaint needs to be made then this should be addressed to: Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5A, telephone: 0303 123 1113, website: www.ico.org.uk