



## **Data Protection Policy (Compliant with General Data Protection Regulations)**

The wording in this policy reflects the requirements of the General Data Protection Regulations (GDPR), which will come into effect in the UK on 25 May 2018. See Law relating to this document below for more information.

### **Introduction**

#### *Purpose*

Abington Community Out Of School Club (GAPs) is committed to being transparent about how it collects, stores and uses the personal data of its workforce and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

GAPs has appointed Louise Davison, Finance Manager, as its data protection officer. Her role is to inform and advise the organisation on its data protection obligations. She can be contacted at [abingtonannexefinance@gmail.com](mailto:abingtonannexefinance@gmail.com) . Questions about this policy, or requests for further information, should be directed to the data protection officer.

#### *Definitions*

**"Personal data"** is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

**"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

**"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

### **Data protection principles**

GAPs (the setting) processes HR-related personal data in accordance with the following data protection principles:

- The setting processes and stores personal data lawfully, fairly and in a transparent manner.
- The setting collects personal data only for specified, explicit and legitimate purposes.
- The setting processes and stores personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The setting keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The setting stores personal data only for the period necessary for processing.
- The setting adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

GAPs tells individuals the reasons for processing and storing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where GAPs processes and stores special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with guidelines from the Information Commissioners Office (ICO) on special categories of data and criminal records data.

### **Criminal Offence Data**

For further details on processing Criminal Offence Data please follow the link below to the Information Commissioners Office (ICO).

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/>

#### *"At a glance"*

- *To process personal data about criminal convictions or offences, you must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10.*
- *The Data Protection Bill deals with this type of data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.*

- *You can also process this type of data if you have official authority to do so because you are processing the data in an official capacity.*
- *You cannot keep a comprehensive register of criminal convictions unless you do so in an official capacity.*
- *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.”*

GAPs will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the employment for a worker, contractor or volunteer relationship, apprenticeship or internship is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems.

The setting keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

## **Individual rights**

As a data subject, individuals have a number of rights in relation to their personal data.

### *Subject access requests*

Individuals have the right to make a subject access request. If an individual makes a subject access request, the setting will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the setting has failed to comply with his/her data protection rights; and
- whether or not the setting carries out automated decision-making and the logic involved in any such decision-making.

The setting will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

If the individual wants additional copies, the setting will charge a fee of £5.00 which will be based on the administrative cost to the setting of providing the additional copies.

To make a subject access request, the individual should send the request to [abingtonannexefinance@gmail.com](mailto:abingtonannexefinance@gmail.com). In some cases, the setting may need to ask for proof of identification before the request can be processed. The setting will inform the individual if it needs to verify his/her identity and the documents it requires.

The setting will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the setting processes large amounts of the individual's data, it may respond within three months of the date the request is received. The setting will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the setting is not obliged to comply with it. Alternatively, the setting can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the setting has already responded. If an individual submits a request that is unfounded or excessive, the setting will notify him/her that this is the case and whether or not it will respond to it.

#### *Other rights*

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the setting's legitimate grounds for processing data (where the setting relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the setting's legitimate grounds for processing data.

To ask the setting to take any of these steps, the individual should send the request to [abingtonannexefinance@gmail.com](mailto:abingtonannexefinance@gmail.com) .

#### **Data security**

GAPs takes the security of HR-related personal data seriously. The setting has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Staff sign a confidentiality agreement on induction that takes into consideration the use of relevant personal data as well as the due process of dealing with Children's Records.

Please see our Confidentiality and Client Access to Records Policy, Provider Records Policy and our Information Sharing Policy.

Staff who have access to personal data regarding staff members and volunteers in the setting ensure that the data is stored securely and that it is only shared with the relevant suppliers, i.e. payroll processors.

All staff ensure that any paper documents containing personal data are stored securely.

All staff ensure that any electronic documents are stored with a secure provider, additionally making sure relevant documents are 'locked'.

When sending electronic documents all staff ensure that they are sending the information to the correct recipient.

Where the setting engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

### **Impact assessments**

Some of the processing that the setting carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the setting will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

### **Data breaches**

If the setting discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The setting will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

We follow the guidance on Data Breach Procedures from the Information Commissioners Office. See PDF in the additional information folder in the lobby.

### **International data transfers**

HR-related personal data may be transferred to countries outside the EEA to fulfil our contract with members of staff. If data is transferred outside the EEA it will be on the basis of legal Safeguarding and Child Protection Requests or to fulfil our contract

regarding staff employment with us. We ensure that all third parties comply with GDPR.

### **Individual responsibilities**

Individuals are responsible for helping the setting keep their personal data up to date. Individuals should let the setting know if data provided to the setting changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the setting relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the setting) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the setting's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Further details about the organisation's security procedures can be found in its data security policy.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the setting's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

### **Training**

The organisation will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

## **Law relating to this document**

### **Leading statutory authority**

#### **General Data Protection Regulation (2016/679 EU) Data Protection Bill**

The General Data Protection Regulation (GDPR) requires employers to:

- process personal data lawfully, fairly and in a transparent manner;
- collect data for specified and legitimate purposes and not process data in a manner that is incompatible with those purposes;
- collect data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- ensure that data is accurate and kept up to date, and take every reasonable step to rectify or erase data that is inaccurate without delay;
- keep data only for the period necessary for the purposes of processing;
- ensure that appropriate security is in place to protect data against unauthorised or unlawful processing, accidental loss, destruction or damage;
- process data in accordance with the rights of data subjects; and
- transfer data outside the European Economic Area (EEA) only if there is an adequate level of protection for the rights and freedoms of data subjects.

The GDPR not only requires employers to comply with the data protection principles but to demonstrate that they comply. This is known as the principle of accountability. Employers are also required to implement appropriate technical and organisational measures (including implementing appropriate data protection policies and providing employee training) to ensure and demonstrate that they carry out processing in accordance with the requirements of the GDPR.

An HR data protection policy should cover all of these areas, as well as the rights of data subjects (particularly subject access rights), as part of an employer's strategy to meet the principle of accountability contained in the GDPR and the duty to implement appropriate technical and organisational measures to comply with the GDPR.

Organisations are required to appoint a data protection officer under the GDPR if they are a public authority, if their core activities include the regular and systemic monitoring of data subjects on a large scale, or if their core activities consist of processing special categories of personal data or data on criminal convictions and offences on a large scale. Where appointed, a data protection officer will be responsible for advising the organisation on its obligations under the GDPR. Where an organisation is not required to appoint a data protection officer, it should still assign responsibility for data protection compliance to an individual. However, if the organisation is not required to appoint a data protection officer, it should not give the individual the title of data protection officer, as this would give him or her statutory protections particular to the data protection officer role.

The GDPR requires organisations that hire third parties to conduct data processing activities on their behalf (known as "data processors") to put in place certain contractual requirements, including that the third party processes data only on the basis of written instructions and that individuals processing the data will be subject to a duty of confidentiality. Additionally, the organisation must contract only with third parties that implement appropriate technical and organisational measures for GDPR compliance.

Where an employer conducts data processing that is likely to result in a high risk to the rights and freedoms of individuals, particularly if it is using new technologies, the GDPR requires the organisation to conduct a privacy impact assessment. Instances that are likely to qualify as high risk to the rights and freedoms of individuals include where an employer conducts systematic monitoring of employees, or processes special categories of personal data or data on criminal convictions and offences.

In the event of a data breach, the GDPR requires organisations to notify the Information Commissioner and individuals whose data has been breached within 72 hours of becoming aware of the breach. Where a breach is not likely to result in a risk to the rights and freedoms of individuals, the organisation does not need to notify the Information Commissioner or the individuals affected. However, the organisation must keep a record of all data breaches.

Under the GDPR, the transfer of personal data outside the EEA is subject to strict rules. Personal data can be transferred to countries that have received an adequacy decision from the European Commission without additional security protections. However, employers transferring personal data to non-EEA countries that have not received an adequacy decision will need to apply additional safeguards, such as binding corporate rules or standard data protection clauses. Transfers of personal data include instances where data is stored, backed up or accessed outside the EEA.

## Notes

The General Data Protection Regulation (GDPR) applies to all personal data that an organisation processes. This means that an HR data protection policy should cover the personal data of not only prospective, current and former employees, but also any personal data processed in relation to workers, contractors, volunteers, interns and apprentices.

The GDPR and the Data Protection Bill create new definitions for special categories of personal data and data on criminal convictions and offences. Under the Data Protection Act 1998, these types of data were previously known as "sensitive personal data". The GDPR and the Data Protection Bill place restrictions on the processing of special categories of personal data and data on criminal convictions and offences. To process such data, employers are likely to rely on the ground that processing is necessary to perform or exercise obligations or rights of the employer under employment law. Under the Data Protection Bill, employers must have a policy on the use, retention and erasure of the data where it is processed to exercise obligations or rights under employment law.

Although documents such as the data security policy are likely to be outside the scope of HR responsibility, employers should refer to such applicable policies where



relevant, and ensure that data protection measures are implemented consistently across the organisation.

Given the serious penalties for breach of the GDPR (see Warning below), employers should set out employees' responsibilities with respect to data protection and clearly state that the failure to follow data protection requirements can amount to a disciplinary offence.

#### Warning

Employers that fail to comply with their obligations under the General Data Protection Regulation (GDPR), including breaching the data protection principles, data subject rights and requirements regarding international data transfers, can be subject to significant administrative fines of up to €20 million or 4% of the undertaking's worldwide annual turnover, whichever is higher. Although the Information Commissioner will take into account a number of factors when determining the level of a fine, employers would be well advised to take the implementation of data protection measures seriously to mitigate the risk of liability or enforcement action.

Organisations may also be subject to direct claims for compensation by individuals who have suffered damage as a result of a breach of the GDPR.

The Data Protection Bill supplements the GDPR and contains additional requirements regarding special categories of personal data, data on criminal convictions and offences, information requirements for individuals and subject access requests. These requirements have been incorporated into this model policy where relevant. However, the Bill is still being considered by Parliament and is subject to change before it comes into force.

#### Future developments

The General Data Protection Regulation (GDPR) will come into effect on 25 May 2018.

The Data Protection Bill, which will repeal and replace the Data Protection Act 1998, is currently being considered by Parliament.

### **ADOPTION AND ANNUAL REVIEW OF THE POLICY**

This policy was adopted at a meeting of: **Abington Annexe (Pre-School, GAPS and AAS)**

Signed on behalf of the Management Committee / Proprietor:

Print Name:

Date:

May 2018

Role:

This policy was reviewed on:	Signature and name:	This policy was amended on:	Signature and name: