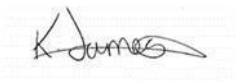
APF Activity Camps
Confidentiality Policy
&
Data Protection Act

Ownership and consultation	Signature	Date
Kaz James		June 01 2023

Revised by: Kaz James

Next review date: By 1st June 2024

Confidentiality Policy

At APF we respect the privacy of the children attending the Camp and the privacy of their parents or carers. Our aim is to ensure that all those using and working at APF can do so with confidence.

We will respect confidentiality in the following ways:

- Parents can ask to see the records relating to their child, but will not have access to information about any other children.
- Staff only discuss individual children for purposes of planning and group management.
- Staff are made aware of the importance of confidentiality during their induction process.
- Information given by parents to Camp Manager will not be passed on to third parties without permission unless there is a safeguarding issue (as covered in our Safeguarding Policy).
- Issues relating to the employment of staff, whether paid or voluntary, will remain confidential to those making personnel decisions.
- Confidential records are stored securely.

Statement of intent

APF takes the security and privacy of personal data seriously and intends to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security. We need to gather and use information or 'data' as part of our activities (via the booking system) to manage our relationship with a number of data subjects whose data we process: children, parents, carers, current and former employees, volunteers and Committee members.

EU GDPR

The **General Data Protection Regulation (GDPR)** was adopted as Regulation (EU) 2016/679 of the European Parliament and of the Council on April 27, 2016.

Information

The definition of information includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, biometric or genetic data, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites or communicated using social media.

Data Protection Act

APF is registered as a Data Controller under the Data Protection Act 1998. To process your booking, we need to collect personal details about you and your children. We will treat it as confidential and keep it secure, complying with all relevant UK legislation

The Camp Manager is responsible for ensuring the safe storage and access to any confidential documents relating to both parents and children. All staff are aware that the disclosure of any confidential information contravenes the Data Protection Act 1998 and any such disclosure may result in disciplinary action.

All parent and child paper information held on Camp is stored in a lockable box and accessed only by the Camp Manager, if, due to emergency, another member of staff needs to access the information they will ensure confidentiality of information at all times.

Data stored electronically will be password protected and accessed only by the Camp Manager.

It is not APF Policy to disclose any client data to third parties unless such request are made by legal authorities.

Day to Day Documents

We believe that Implementing a Shred-all practice is of utmost importance. This means that ALL documents (from post-its to customer information) are shredded or placed into the shredding bins. NO MATTER WHAT. This takes away the complication of your employees making the decision of what should be shredded and significantly reduces the risk of a security breach. This is a simple, yet extremely effective strategy to mitigate any risk.

Documents that need to be retained for a period of time

Documents such as tax files, employee records or medical records that need to be retained for a particular time period are stored and destroyed in a secure way. All documents are stored in a secure, locked area to ensure the safety of the information. Boxes are indexed so we know what is in the box and when it can be destroyed. Once the retention period has passed, all documents are shredded in a timely manner.

Limiting access to sensitive information

As we have confidential information, we are careful to limit access to confidential information to only those employees who have a "need to know". Hard copies of documents are kept locked, and electronic copies are all password protected on a Google cloud. We believe that one of the best ways to protect our privacy is to encrypt important information on our computers. This is done when we send personal information to someone, or we simply want to make sure that no one who gets access to our computer can see information we would rather keep private and therefore encryption embedded into our business.

Staff are not allowed to use their personal devices to access council data. Instead, the site manager has access to APF devices which are password protected and set-up for each individual member of staff using a 3-step verification process.

Data retention periods

- We destroy at 2 years after the last document was added to the case (EDRM) policies, guidance and manuals that have been updated and are no longer applicable to at the time or have been superseded and not relate to a particular case.
- We destroy at 6 years after the last document was added to the case (EDRM), financial records that are older than 6 years, compliance communications, phase 1 mergers, information gathering.

- We destroy 8 years after the last document was added to the case (EDRM), Ephemeral information which becomes out of date, commercial, HR and corporate services.
- We destroy 10 years after the last document was added to the case (EDRM), records management, FOI's, board papers.
- Permanent Preservation – significant Competition Casework such as Competition Act Investigations, Super Complaints, Phase 2 Markets or Mergers Inquiries and the related Phase 1 inquiries, court cases, and cases where undertakings have been given.

Disaster Recovery

We rely upon the replication of data and computer processing in an off-premises location (14 Strathespy Gate Broughton mk107du) not affected by the disaster.

When servers go down because of a natural disaster, equipment failure or cyber attack, we can recover lost data from this second location where the data is backed up.

Data Protection Training

All staff receive annual GDPR training which explains what your responsibilities are under data protection law so that you understand how to collect data legally, obtain consent where required, process data in accordance with the law and ensure data security. The module include:

- Introduction to Data Protection and the EU and UK GDPR
- The Principles of Data Protection
- Legal Grounds for Processing and Obtaining Consent
- Data Subject Rights
- Data Protection Responsibilities

Data Breach Procedure

What is a personal data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following:

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper
- file (this includes accidental loss)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error (for example sending an email or SMS to the wrong recipient)
- Unforeseen circumstances such as a fire or flood
- Hacking, phishing and other “blagging” attacks where information is obtained by deceiving whoever holds it

When does a personal data breach need to be reported?

APF must notify the Information Commissioner's Office of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes:

- potential or actual discrimination
- potential or actual financial loss
- potential or actual loss of confidentiality
- risk to physical safety or reputation
- exposure to identity theft (for example through the release of non-public identifiers such as passport details)
- the exposure of the private aspect of a person’s life becoming known by others

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

Reporting a data breach

- If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should:
- Complete a data breach report form
- Email the completed form to Kaz James (kjames@apfactiviycamps.com)
- Notify Kaz James verbally that a breach has taken place
- Breach reporting is encouraged throughout APF and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The APF Business

Manager will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the Data Protection Officer.

Managing and recording the breach

The Data Protection Officer will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:

- Where possible, contain the data breach
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed
- Assess and record the breach in the APF's data breach register
- Notify the Information Commissioner's Office
- Notify data subjects affected by the breach
- Notify other appropriate parties to the breach
- Take steps to prevent future breach.
- Notifying the ICO

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer will notify the affected individuals without undue delay including the name and contact details of the Information Commissioner's Office, the likely consequences of the data breach and the measures the camp have (or intended) to take to address the breach. When determining whether it is necessary to notify individuals directly of the breach, we will cooperate with and seek guidance from the Information Commissioner's Office and any other relevant authorities (such as the police).
If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the APF will consider alternative means to make those affected aware (for example by making a statement on the Camp).

Data audit process

We follow the following when completing a data audit, which takes place annually, we ask these FIVE simple questions …

- What data is being held?
- Where did the data come from?
- Who is holding the data?
- Who are you sharing this data with?
- What are the data flows?

This will allow us to better understand how we process personal data and how this processing is linked into the rights of the individual under the DPA and GDPR, as well as new provisions for children.

Information and procedure for responding to subject access requests

The personal data requested should be clearly identified. It may be necessary to confirm the identity of the data subject and/or the person making the request. APF will respond to requests within 1 calendar Month of receipt of the completed form (provided sufficient information has been given to the APF to enable the APF to process the request), or, in the case of exam marks, up to five months from the time when the camp has sufficient information to process the form.

General guidance when requesting subject access to emails

Data subjects are entitled to have access to their personal data held in the form of emails under the Act. However, data subjects must supply enough information to enable the APF to locate the relevant emails. As a minimum, the following information must be provided to the Information Rights Officer when completing the form:

The fact that the data may be held in the form of emails;

The names of the authors or recipients of the messages;

The dates or ranges of dates upon which the messages have been sent;

Any other information that might assist the APF in locating the data.

Please note that failure to provide information reasonably required to narrow down the search could result in the APF being unable to comply with a subject access request.

Information containing personal data about other people (third parties)

Some information may contain personal data relating to third parties. The request may therefore lead to a conflict between the data subject's rights of access and the third party's rights over their own personal information. In responding to subject access requests the APF will need to ensure that the rights of those third parties are not compromised by releasing the information. As the obligation on APFl is to provide information rather than documents, redaction or editing may be used so that the third party information does not form part of the requested information.

The APF may also ask for consent from the third party. Where consent is not given, in line with the Information Commissioner's Subject Access Code of Practice (we are currently awaiting an updated version of this document), APF will consider whether it is reasonable in all the circumstances to disclose the email without the third party's consent.