**IT Acceptable Use & GDPR Policy**

This policy document contains important information about your usage of all Activity Den computers and the information we store/process. It also details information regarding the protection of data we hold and your responsibilities. If you’re unsure of anything, please **ask before doing** to ensure neither you or the organisation is responsible for data loss or fines.

All users at The Activity Den (staff, trustees, visitors and volunteers) are bound by the provisions of this policy.

This Policy shall be governed by the laws of England and the parties submit to the exclusive jurisdiction of the Courts of England and Wales.

**The Information We Store**

We need different types of digital information to run our organisation. Some of this is of no use to anyone outside, but some of it may be sensitive or relate to people employed by or otherwise we work with. Some information could even be used to commit crimes such as financial fraud or identity theft.

Data which allows people to be personally identified gets additional protection under European Law called “GDPR”. That might include information such as names, addresses, telephone numbers, documents, or salary information. There is also a further definition of special personal data under the Act, which covers very sensitive personal data such as ethnicity, political opinions, religious beliefs, physical/mental health conditions or offences committed.

We can’t avoid storing this kind of data because it’s needed for things such as recruitment, retention, safeguarding and payroll. But in the same way we safeguard people we need to make sure that we limit who can access that data and we delete it once it’s no longer required (or there is no legal requirement to retain it). We also need to pay particular attention to protect the data if it’s sent outside the organisation by any means.

**The Information We Store About You**

During your involvement with The Activity Den, you’ve created a digital ‘footprint’.

As an organisation we retain information relating to your ‘employment’ for seven years for legal purposes. We delete this information after this time period.

You may have been provided with a username and password to log in to our computer systems and/or Google Cloud service account. If so, you need to ensure you safeguard your password and do not disclose it to any unauthorised person, or share use of the account with someone else.

You can optionally make your account even more secure by adding a recovery email and mobile phone number and enabling “multi factor authentication” on your account. Please ask for assistance if you’re unsure how to do this.

By using our computer systems, you are giving authorised individuals at The Activity Den the right to monitor your communications (Den e-mails, web and official social media accounts) for compliance of this policy; use this information for internal investigations and/or supply this information to any authorised agency (e.g. HMRC, police) when legally requested. We will fully co-operate with such agencies and maintain the information for as long as required for any investigations or queries to be resolved.

Your Den email account will be removed at 12 months after you have left the organisation.

**Your Responsibilities**

The over arching thing you need to consider is the **protection** of data – especially if it relates to an individual or allows them to be identified. Please ask for further guidance if you’re unsure about any aspect of this.

* Please inform a member of the board if any of your information changes. For example, if you get married, change address, or your bank details change.
* Keep any information which may allow identification of an individual within the organisation or who we work with secure.

In practical terms, this may include (but not exclusively)

* + **Never** email copies of data to your personal/home email accounts.
	+ **Avoid printing** out copies of personal data if possible.
	+ Ensure that any printed copies are in your possession and don’t get left on a printer, or worse anywhere else away from the building such as train, bus or university.
	+ If you need to download data relating to individuals, make sure it’s on an **encrypted device** like an encrypted hard disk or USB memory drive.
	+ If you need to email data relating to individuals to someone outside the organisation, make sure it’s **encrypted** so it can’t be read if intercepted.
* Delete any information relating to individuals within the organisation or we work with as soon as it’s no longer needed (or required for legal reasons).
* Ensure that if you use your own IT devices to access The Activity Den data (for example your mobile phone, desktop computer or tablet) then these are up to date with security patches, anti-virus software and if necessary firewall software.

**Acceptable Use Of Our IT Systems, Network and Communications**

* You must not directly or indirectly use any IT, network or communications equipment provided or supplied by the Activity Den for the download, creation, manipulation, transmission or storage of:
	+ any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
	+ unlawful material or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
	+ unsolicited “nuisance” emails or telephone calls;
	+ material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the University or a third party;
	+ material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
	+ material with the intent to defraud or which is likely to deceive a third party;
	+ material which advocates or promotes any unlawful act;
	+ material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
	+ material that brings The Activity Den into disrepute.

You must also not use any systems in order to:

* introduce data-interception, password-detecting or similar software or devices to the Activity Den’s network (unless specifically authorised);
* seek to gain unauthorised access to restricted areas of the Activity Den’s IT or Cloud based storage;
* access or try to access data where the user knows or ought to know that they should have no access;
* carry out any hacking activities; or
* intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

**Data Access Requests**

GDPR allows an individual special rights to their own data, including but not limited to:

* The right to be informed
* The right to access
* The right to rectification
* The right to erasure
* The right to restrict processing

These rights are normally requested via a Subject Data Access Request which must be requested in writing. Please refer any Data Access Requests to a member of the Board.

**Updated:** January 2021