Data Protection Policy and Procedure

Sycous are committed to protecting the privacy of all our team members and clients personal information and complying with all data protection legislation, regulation and industry best practise.

We are committed to ensuring the highest levels of compliance and adoption of best practise to ensure any collected, stored and processed personal data is done so fairly and lawfully.

Our Policy

Sycous and our team members who process or use personal information must ensure that this is done in line with the principles set out under GDPR and the Data Protection Act. These key principles state that personal data shall:

- Be obtained and processed fairly and lawfully.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept longer than is necessary for that purpose.
- Be processed in accordance with the data subject rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic area, unless that country has equivalent levels of protection for personal data.

Sycous will not sell or share any personal data except as required to do so by law to any statutory body without the advance written consent of the individuals concerned.

Our Teams Responsibilities
Board of Directors

The Sycous board of directors are ultimately responsible for providing oversight, leadership and organisational implementation of this policy.

Senior Management Team

The Sycous senior management team are responsible for ensuring compliance with all elements of this policy, including communication to all team members, ensuring they receive the appropriate level of training and support.

Data Protection Officer / Responsible Person

The Sycous data protection officer is a nominated position with responsibility for the operational implementation of all elements of this policy. This person is trained and accredited as necessary.

Team Managers

The Sycous team managers are responsible for ensuring awareness, training and the operational application of this policy.

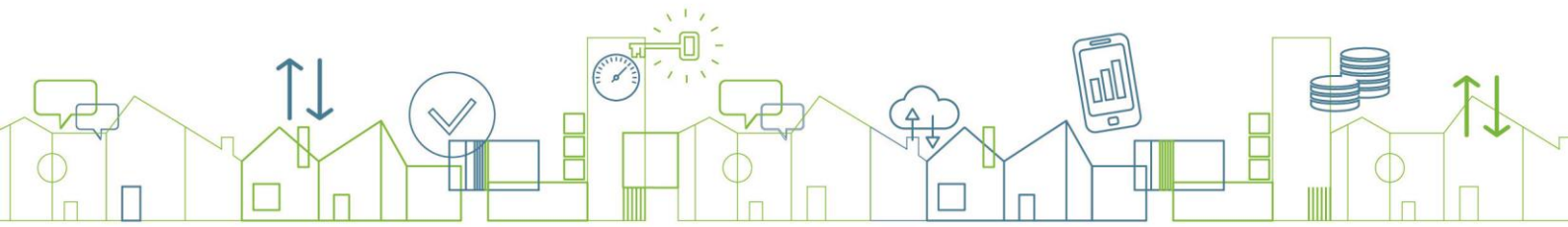
All Team Members

It is the responsibility of every member of the Sycous team to ensure compliance with this policy and the principles of the Data Protection Act 2018. It is every team member's responsibility to ensure all personal data is kept securely and not disclosed to any unauthorised person.

It is also the responsibility of all team members to be proactive in seeking to identify and highlight any potential risks so the necessary mitigation actions can take place. If a breach does take place it is the responsibility of every team member to notify the data protection office and your mentor immediately.

If you are at all concerned about highlighting any potential risks and the impact this may have on you as an individual, please refer to the Sycous whistleblowing policy for additional information

and support.



Our Procedures

Overview

Sycous is required to collect, process and store some personal information on our team members, our clients and other individuals. This information is used for a range of purposes including payroll, recruitment and legal compliance.

It is also necessary that personal information of our client's customers is stored on infrastructure operated by Sycous. This data is as much the responsibility of Sycous as a data processer as the information we collect on our team members.

All personal data must be treated equally. It must be collected, processed and stored against the principles of GDPR and the Data Protection Act 2018. These principles state that data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

All team members or any person processing data on behalf of Sycous must ensure these principles are adhered to at all times and be proactive in immediately notifying the responsible person of any potential or confirmed breach of these principles.

All Sycous team members are required to sign a confidentiality agreement as part of their 'Contract of Employment' further details of which can be found in the Employee Handbook.

Sycous will keep a register and store electronic audits of access to personal information, including those authorised to do so. This will ensure that only the relevant team members with the correct level of training are authorised to access and process personal data.

Information About You
All team members are individually responsible for ensuring the information you provide about you in relation to your employment is up-to-date and accurate.

If any of your personal information changes this should be notified to your mentor at the earliest opportunity.

All Sycous team members are able to securely access the information we hold about them in relation to their personal information through their 'MyPayroll' log-in. If you discover any error in this information, please notify your mentor immediately as Sycous cannot be held responsible for errors unless we have been informed.

Information About Other People
It is important that we recognise that Sycous team members may from time-to-time have access to other personal information, including the potential for personal information on our clients.

As a result, all team members must fully comply with the guidelines detailed below. If you do not understand or would like additional training before undertaking any action, please speak to your mentor.

It is recognised that all Sycous team members are likely to process some personal data. It is the responsibility of Sycous and individual team members to ensure that all necessary consent for the processing and storage of data has taken place.

The information that team members will collect or process on a day-to-day basis will be 'standard' and will cover categories such as:

- General personal details such as name and address.
- Notes on performance of roles and associated HR information.

Information about an individual's physical or mental health; sexual orientation; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with consent.

All team members have a duty to make sure that they comply with the data protection principles, which are set out in this document and the Employee Handbook. In particular, team members

must ensure that records are:

- Accurate
- Up-to-date
- Fair
- Kept and disposed of safely, and in accordance with the Sycous Data Retention policy

Sycous will designate and provide additional training to team members in the relevant area as 'authorised team members'. These team members are the only team members authorised to access data that is:

- Not standard data
- Client related
- Sensitive data.

The only exception to this will be if a non-authorised member is satisfied and can demonstrate that the processing of the data is necessary:

- In the best interests of the individual, or a third person, or Sycous AND
- He or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.
- This should only happen in very limited circumstances. E.g. an individual is injured and unconscious and in need of medical attention, or a team member tells the hospital that the individual is pregnant.
- Once processing of this data has taken place the team members mentor should be informed at the earliest opportunity.

Authorised team members will be responsible for ensuring that all personal data is kept securely. In particular team members must ensure that personal data is:

- Stored in locked storage cupboards with only authorised team member key access
- Never left on unattended
- All computers, telephones and other devices must be locked when left for any period of time
- Personal data should not be stored on individual computers held off site, except where authorised and suitably password protected/encrypted
- Data should not be stored on CD or floppy disk or memory stick, if data is received in this manner it must be immediately passed to the nominated data protection officer for secure transfer to an acceptable format in line with the Sycous Security and IT

Policies

- Any email attachments used off-site containing personal data must be password-protected.
- Paper records containing personal data must be shredded, where appropriate.

Team members must not disclose personal data to any individual, unless for normal HR purposes, without authorisation or agreement from the data controller, or in line with the Sycous policy.

Before processing any personal data, all team members should consider the following.

- Do you really need to record the information?
- Is the information 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the individual been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the individual or the safety of others to collect and retain the data?

Right to Access Information

Team members and other individuals have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should put the request in writing and address it to "The Data Protection Officer, Sycous Limited, New York House, 1 Harper Street, Leeds, LS2 7EA".

Please note all Sycous team members are able to securely access the information we hold about them in relation to their personal information through their 'MyPayroll' log-in. If you discover any error in this information, please notify your mentor immediately as Sycous cannot be held responsible for errors unless we have been informed

Sycous aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days (in line with legislation) unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

Data Sharing Consent

In many cases, Sycous can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement for the processing some specified classes of personal data is a condition of employment for team members. This includes information about previous criminal convictions.

Sycous will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. Sycous will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

Therefore, all prospective team members and on-site contractors will be asked to sign either an appropriate HR form or an individual document regarding particular types of information when an offer of employment or contract is made. A refusal to sign such documents may result in the offer being withdrawn.

Data Controller

Sycous is a data controller under GDPR and the Data Protection Act 2018, and the board of directors is therefore ultimately responsible for implementation. However, the designated data controllers will deal with day-to-day matters.

Contact details of the nominated Data Protection Officer and deputies can be found on the Sycous online directory, or can be contacted through the dataprotection@sycous.com email address.

Data Retention

Data held by Sycous will be retained no longer than is necessary for its original purpose or any relevant legal or regulatory requirements. All personal data stored will be regularly reviewed/audited by the data controller and decisions made as deemed appropriate against the principles of GDPR and the Data Protection Act 2018.

Ensuring personal data is disposed of when no longer needed will reduce the risk that it will become inaccurate, out of date or irrelevant.

Once it is decided that any personal data should no longer be retained it will be securely deleted

or destroyed. Any information that is updated will also be stored for as long as necessary.

Changes to Processing Personal Data
Any changes to how Sycous processes personal data will be notified to all team members and relevantly impacted individuals.

Review and agreement
This policy is agreed by the board of Sycous who agree to review this policy and arrangements on an annual and more frequent basis, as necessary, to maintain our commitments.

Signed  Matthew Hall (Responsible Director)

Date 20th July 2020