

Xyrius Training Limited

GDPR and Data Protection Policy

Xyrius Training Limited keeps information about staff, clients, learners, and other parties confidential to allow it to operate as a successful organisation and meet its legal obligations. To comply with the data protection act 1998 information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Xyrius Training Limited must comply with the data protection principles in the act.

In summary, the principles state that personal data will:

1. Be processed fairly and lawfully
2. Be obtained for specified and lawful purposes, and will not be processed in a manner incompatible with those purposes
3. Be adequate, relevant, and not excessive for those purposes.
4. Be accurate and up to date
5. Not be kept for longer than is necessary
6. Be processed in accordance with the data subjects' rights
7. Be kept safe from unauthorised access, accidental loss or destruction
8. Not be transferred to a country outside the EEC, unless the country has equivalent protection for personal data

Personal data and processing:

Personal data is information relating to a person who can be identified from the information, whether stored electronically or in paper-based filing systems or any other medium.

Processing, for the purpose of the act, is accessing, altering, and adding to, using, changing, disclosing, or merging data.

Requirement to comply:

Staff, clients, learners, or other parties who process personal data collected in the name of Xyrius Training Limited must ensure that they follow the above principles.

Compliance with the act is the responsibility of all staff and learners who access business systems.

A breach of this policy may lead to disciplinary action and/or access to client's approval being withdrawn or even criminal prosecution.

Staff, clients, learners, or other parties who believe that the policy has not been followed in respect of their own personal data should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal complaint or grievance, in accordance with company procedures.

Notification of data held and processed:

Staff, learners, and other persons about whom Xyrius Training Limited holds data are entitled to:

1. Know what information Xyrius Training Limited holds and processes about them and why.
2. Know how to gain access to it.
3. Know how to update it.
4. Know how Xyrius Training Limited complies with the act.

Xyrius Training Limited will notify staff, learners, and other relevant parties of the nature of data that Xyrius Training Limited holds and processes about them, and the reasons for which it is processed.

Data controller:

Xyrius Training Limited is the data controller under the act, and the Xyrius Training Limited directors are therefore ultimately responsible for implementation of this policy and for compliance with the act.

Responsibilities of staff and managers:

1. Checking information provided to Xyrius Training Limited in connection with their employment is accurate and up to date.
2. Informing Xyrius Training Limited of changes to information provided.
3. Checking information from Xyrius Training Limited, detailing data stored and processed in relation to the client and individuals.
4. Informing Xyrius Training Limited of errors or changes in information stored. Xyrius Training Limited cannot be responsible for un-notified errors.
5. If information is collected from other parties, the guidelines for staff must be complied with.
6. Managers have a responsibility to ensure that their staff are aware of, and comply with data protection principles.

Clients and Learner obligations:

1. To ensure that their personal data provided to Xyrius Training Limited is accurate and up to date.
2. They should notify Xyrius Training Limited of any changes of personal details.

Data security:

Staff are responsible for ensuring that personal data they hold on behalf of Xyrius Training Limited is:

- A. Secure.
- B. not disclosed to an unauthorised third party.

Unauthorised disclosure will be a disciplinary matter and may be considered gross misconduct. Personal information should be physically secure and, if electronic, should be password protected or kept on a securely stored disk.

Rights to access information:

Staff, clients, learners, and persons hold the right to access their personal data stored by Xyrius Training Limited. Anybody wishing to access such data must gain approval first.

Xyrius Training Limited aims to comply with requests for access within 21 working days of the date of receipt of the request. If this timescale cannot be met, the reason for delay will be explained in writing to the person making the request.

Publication of information:

Information already in the public domain is exempt from the act. Xyrius Training Limited makes public information concerning its governance, annual accounts, rules, charters, significant policies, and media releases, except for confidential matters and personal data, unless consent has been obtained.

Any individual who has good reason for wishing their personal data to remain confidential should contact the data controller.

Data subject consent:

In many cases, Xyrius Training Limited can only process personal data with the consent of the individual concerned. In some cases, if the data is sensitive, express consent must be obtained. Agreement to Xyrius Training Limited processing specified classes of personal data is a condition of acceptance of a learner onto a qualification and a condition of employment for staff. This includes information about previous criminal convictions.

Xyrius Training Limited has a legal obligation to ensure staff are suitable for the duties and responsibilities of their role, and learners for the qualification offered. Xyrius Training Limited has a duty of care to all staff and learners and must therefore confirm that employees and those who use company facilities do not pose a threat or danger to themselves or others.

Xyrius Training Limited also asks for certain information about the health of staff, client and learners, which will only be used in connection with the health and safety of the individual and others but requires consent to process.

Processing sensitive information:

It is sometimes necessary to process sensitive information about a person's health, criminal convictions, race, gender, and family details. This may be to ensure Xyrius Training Limited is a safe place for everyone.

Because this information is sensitive, and it is recognised that processing may cause concern, staff and learners are asked to provide express consent for Xyrius Training Limited to do this. Offers of employment or qualification places may be withdrawn if consent is withheld without good reason.

Examination and assessment results/certification:

Learners are entitled to information about their results for examinations and assessments. However, this may take longer than other information to provide if third parties such as examining bodies have to be contacted. Certificates will be issued to the address held by the Xyrius Training Limited database therefore this information must be kept up to date by all parties. Re-issuing certificates due to incorrect information will incur charges.

Retention of data:

Xyrius Training Limited keeps some types of information for a longer period than others. Information about learners cannot be kept indefinitely. Generally, key information relating to learners that could be subject to audit may be kept for up to seven years. Other information will be destroyed within five years of the learner leaving Xyrius Training Limited.

Xyrius Training Limited are required to retain information on employees, generally for two years after staff leave. Some information will be kept longer, including information for pensions, taxation or for legal or audit reasons.

Staff guidelines for data protection:

Most staff process data about clients and learners, e.g. When marking registers, or company work, writing reports or references, or as part of their supervisory roles. Xyrius Training Limited will ensure that all clients and learners' consent to this sort of processing, and are notified of the categories of processing, as required by the act.

This information includes such categories as:

1. General personal details e.g., Name and address.
2. Details about attendance, grades, and associated comments.
3. Notes of personal supervision, including matters about behaviour and discipline.
4. Information about a client's or learner's physical health, sexual life, political or religious views, trade union membership, ethnicity or race is sensitive and can only be collected and processed with the learner's consent.

5. All assessors have a duty to make sure they comply with the data protection principles in the data protection policy. Staff must ensure that records are:
 - Accurate
 - Current
 - Fair
 - Stored and disposed of securely, and in accordance with company policy.
6. Staff must not disclose personal data to any learner or third party, other than the person whom the data is about, unless for normal academic or pastoral purposes, in accordance with company policy, or as required by law.
7. Staff should not disclose personal data regarding other assessors except in accordance with company policy or if the requesting employee needs the information to perform their duties. Seek advice from directors if you are asked to provide a reference.
8. Personal data must not be supplied to anyone you do not know unless you can confirm their identity and satisfy yourself that you can legally comply with the request. Particular care should be taken with telephone requests and alleged relatives or other employees of clients/learners and staff. Refer all difficult situations to the designated data controller.
9. Police or similar legal requests for disclosure of personal data should be referred to the data controller.
10. Personal data collected for a specified purpose should not be used for any other purpose e.g., unsolicited direct marketing.
11. Care should be taken with the use of e-mail or fax to transmit personal data. Seek assurance the data is received only by the intended recipient. The recipient should ensure the data is retained for the appropriate length of time, remains accurate and can be retrieved when required.

Staff have screen-based access to a considerable amount of personal data that is held within the company's central information systems:

Before processing personal data, consider the following checklist:

- a. Does the information need to be recorded?
- b. Is the information standard or sensitive?
- c. If it is sensitive, has the data subject's express permission been obtained
- d. Does the data subject know why this data will be processed?
- e. Has the data subject confirmed the data is accurate?

When data is processed, simple security measures are:

- a. File personal data out of sight of unauthorised persons
- b. Lock personal data away and/or lock the room if it is left empty
- c. Do not leave personal data (paper based or other media such as floppy disc) in bags or cases, in situations where it may be mislaid, damaged or stolen. Where possible, avoid taking such information off site
- d. Seal personal data transported by post (internal as well as external) in envelopes or packages.
- e. Ensure passwords are secure and not disclosed to unauthorised persons
- f. Log out before you leave your computer unattended
- g. Position computer screens away from unauthorised persons
- h. Screen savers should activate after a short interval
- i. Schedule regular back-ups of personal data
- j. Ensure the process for disposal of personal data is robust and does not allow data to fall into unauthorised hands.

Intellectual property:

Xyrius Training Limited holds the copyright to all the intellectual property as part of the Xyrius Training Limited, no documentation, material or systems/procedures may be copied or shared with an unauthorised or third party without consent in writing from the data controller.

Keeping Xyrius Training Limited systems and data secure:

Information may be stored in both electronic and paper-based systems. Whatever storage method used, keeping data secure and confidential will help safeguard the information required to run the business successfully and ensure relevant legislation is complied with.

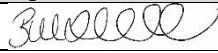
If business data is lost, misused, or accessed without authorisation, it can be difficult to make informed business decisions. This can also result in a competitive disadvantage. Serious data loss can put the whole business at risk and may also lead to offences under the Data Protection Act. This policy sets out the guidelines for looking after data and systems, including physical security, the principles of business continuity and the risks associated with using technology for storage.

Why data security is important:

Data security is of the utmost important to our business. Financial information such as accounts and tax details, or employee information - including payroll and personnel records - could be very difficult to replace. This could expose Xyrius Training Limited to certain risks that need managing carefully. If data is lost through human error, fire, theft or for some other reason, it would at the very least be costly in time and effort collecting and reproducing the information. More seriously, loss of confidential or sensitive data could expose Xyrius Training Limited to the risk of fraud or copyright breaches. Sales, distribution, and the reputation of the business could be directly affected. Projects in progress - e.g., new product designs could be compromised or delayed.

Losing data in a client database for example such as client names, contact details and information on their buying habits, could prevent Xyrius Training Limited from properly servicing its client's needs, targeting prospective clients with appropriate mail shots, or informing them of new products. This could lead to potential member resignations, lost sales, and revenue. A virus can damage the business by making documents stored electronically unusable. As more and more business is conducted via email, a virus can also make getting in contact with suppliers and clients more difficult. This can mean delays in making purchase orders and taking client orders.

Document control

Document title	Document owner	Signature	Version	Review date
GDPR and Data Protection Policy	Bethan Rhodes		May22 v.1	

This document should be a reviewed a minimum of annually.