WSX Enterprise

Data Protection Policy

- Approved by board / management on: 28/05/2018
- Policy became operational on: 28/05/2018
- Next Review Date: 04/06/2023

Policy Summary

Overview	To demonstrate compliance with Data Protection Act (2018) and summarise the roles and responsibilities within WSX Enterprise around Data Protection.
Purpose	This policy sets out WSX Enterprise's commitment to protecting personal data and complying with relevant legislation and describes how that commitment is implemented.
Scope	It applies to all personnel whether staff, contractor, other third parties, or members of partnership organisations with access to WSX data or information systems.
Implementation and Monitoring	Data Protection Officer, WSX Board, Programme Managers – resources may be required to implement some elements.
Risk Implications	Failure to comply with the Data Protection Act (2018)

1. Policy Statement

WSX Enterprise may have business requirements to maintain certain personal data about our employees, client, suppliers, beneficiaries and other individuals. We recognise that the correct and lawful treatment of personal data maintains confidence in the organisation and provides for successful operations.

Personal information, whether held on paper, on computer or other media, is subject to the legal safeguards specified in the Data Protection Act 2018 and the General Data Protection Regulation (Regulation (EU) 2016/679).

WSX Enterprise fully endorses and adheres to the seven principles of the General Data Protection Regulation. These principles specify the legal conditions to be satisfied in relation to obtaining, handling, processing, transportation, and storage of personal data. Employees, partners and any others who obtain, handle, process, transport and store personal data for WSX Enterprise shall adhere to these principles.

2. Definitions

Act	Data Protection Act 2018
EU	European Union
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
WSX	WSX Enterprise
UK	United Kingdom

3. Purpose

This policy sets out WSX's commitment to protecting personal data and complying with relevant legislation and describes how that commitment is implemented.

4. Scope

This policy applies to all personnel who will have access to the information processing systems operated by WSX and its partnership organisations and to all data whether stored electronically on systems, applications or paper copy.

5. Exceptions

This policy applies without exceptions, exclusions, or restrictions.

6. Notification

WSX staff, contractors & partner organisations.

7. Roles and Responsibilities

Programme Managers shall ensure that all staff, partners and contractors are adequately briefed and comply with this policy.

Information Owners shall ensure that, where appropriate:

- documents containing personal information have appropriate classification applied
- retention polices are applied to personal information held on file
- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it

- Printed data should be shredded when it is no longer needed
- Digital data will be stored on the WSX network or an **agreed** 3rd party system that is approved by the IT Manager/DPO. Data on the network will be locked by permission based security – only staff that need access will have access
- The DPO must approve any cloud used to store data (3rd party system, as above)
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

The Data Protection Officer shall be responsible for setting out clear data protection procedures including responding to requests for information under subject access provisions of the act.

Personnel responsible for managing and handling personal information shall follow good data protection practice and comply with this policy.

8. Procedures

WSX shall:

- Maintain an up to date and accurate register entry with the Information Commissioner's Office (ICO) and pay the data protection fee to the ICO;
- Ensure that any changes are notified to the ICO within appropriate timescales;
- Ensure that there is someone with specific responsibility for Data Protection;
- Observe fully the conditions regarding the fair collection and use of personal data;
- Meet its obligations to inform individuals of data collection, processing sharing and retention as set out in the 'right to be informed' under the GDPR;
- Meet its obligations to specify the purposes for which personal data is used;
- Collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
- Ensure the quality of personal data used;
- Apply strict checks to determine the length of time personal data is held;
- Ensure that the rights of individuals about whom the personal data is held can be fully exercised under the Act and under the General Data Protection Regulation;
- Take the appropriate technical and organisational security measures to safeguard personal data;
- Ensure that appropriate safeguards are in place for personal information being transferred outside the UK. Note: Additional safeguards are required when the information is being sent outside the EU;
- Ensure that the rights of people, about whom information is held, can be fully exercised under the Act (These include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is incorrect or unnecessary);
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

9. Legislative Framework

General Data Protection Regulation (Regulation 2016/679 of the European Parliament and of the Council) and the Data Protection Act 2018.

10. Related Policies, Procedures, Guidelines and Other Resources

Additional guidance and procedures will be forthcoming to supplement this policy and make sure that WSX meets its obligations by guiding staff in how to achieve the purposes in section 8: procedures (above).

11. Version Control and Change History

Version	Date	Approved by	Amendment(s)	Author
0	28/05/2018	WSX Board	Updated slightly for post-GDPR use	(edited by DPO)
1	20/04/2019	WSX Board	Updated responsibilities	(edited by DPO)
2	15/03/2020	WSX Board	Review - No change	
3	29/06/2021	Senior Management	Removed obsolete references	(edited by DPO)
4				

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

Any WSX Enterprise Ltd employee who knowingly violates or attempts to violate this Data Protection Policy shall be subject to disciplinary action.

Any contractors working with data on behalf WSX Enterprise Ltd who knowingly violates or attempts to violate this Data Protection Policy shall be subject to penalties.

Any WSX Enterprise Ltd employee who mistakenly violates the Data Protection policy must inform the Data Protection Officer immediately.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.
I confirm that I have read and agree to the terms in the WSX Enterprise Data Protection policy above.

Name……

Signed……

Date……