

[Company]

INFORMATION TRANSFER POLICY

Transferring Information

Last Reviewed: [Last Reviewed] Page 1 of 14



1 Document Version Control

	Last Modified	Last Modified By	Document Changes	
0.1	[DATE]		Document first created	

Last Reviewed: [Last Reviewed] Page 2 of 14



2 Document Contents Page

1	Doo	cume	ent Version Control	2
2	Doo	cume	ent Contents Page	3
3	Info	rmat	tion Transfer Policy	5
	3.1	Pur	pose	5
	3.2	Sco	ppe	5
	3.3	Prir	nciples	5
	3.4	Info	ormation Virus Checking	6
	3.5	Info	ormation Encryption	6
	3.6	Dat	a Transfer Methods	6
	3.6	.1	Preferred Transfer Method	6
	3.6	2	Data Transfer by Email	6
	3.6	3	Data transfers by post/courier	7
	3.6	4	Data transfers on removable media / memory sticks	8
	3.6	5	Telephones, Mobile Phones and General Conversations	8
	3.6	6	Data Transfers over Bluetooth	9

Last Reviewed: [Last Reviewed]

Page 3 of 14

INFORMATION TRANSFER POLICY



Version: [Version Number] Classification: Internal

	3.7	Lost or missing information	10
4	Poli	icy Compliance	11
	4.1	Compliance Measurement	11
	4.2	Exceptions	11
	4.3	Non-Compliance	11
	4.4	Continual Improvement	11
5	Are	as of the ISO27001 Standard Addressed	12

3 Information Transfer Policy

3.1 Purpose

📊 HighTable

The purpose of this policy is ensuring that correct treatment when transferring

information internally and externally to the company and to protect the transfer of

information using all types of communication facilities.

3.2 Scope

All employees and third-party users.

Information that forms part of systems and applications deemed in scope by the ISO

27001 scope statement.

3.3 Principles

Data transfer must comply with all legal and regulation legislation requirements

including but not limited to the GDPR and Data Protection Act 2018.

Formal agreements that include non-disclosure and confidentially clauses must be in

place for data sharing prior to the data transfer.

Personal data must not be transferred outside the European Economic Area without

legal consent, justification, and legal mechanisms in place.

No personal or confidential information is to be transferred unencrypted.

Last Reviewed: [Last Reviewed]

Page 5 of 14

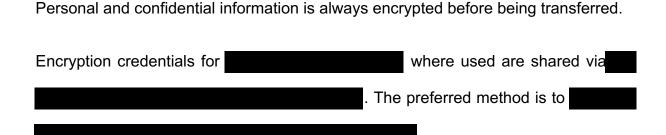


All transfers are in line with the Information Classification and Handling Policy

3.4 Information Virus Checking

Information that is transferred is virus checked before being sent or before being opened when received.

3.5 Information Encryption



3.6 Data Transfer Methods

3.6.1 Preferred Transfer Method



3.6.2 Data Transfer by Email

Email is never the best solution for transferring information as it is not secure and is not a guaranteed delivery mechanism.

Last Reviewed: [Last Reviewed] Page 6 of 14

📊 HighTable

Version: [Version Number] Classification: Internal

Consideration is always given to an alternative secure method of transferring sensitive

data wherever possible and practicable.

Email communication should not be used to transfer unencrypted personal or

confidential information.

Email messages must contain

3.6.3 Data transfers by post/courier

Data transfers which occur via physical media such as paper reports, memory cards

or CDs must only be dispatched via the company approved secure courier with a

record of collection and a signature obtained upon delivery. The use of Royal Mail first

class, second class, special delivery or recorded delivery is not permitted.

The recipient should be clearly stated on the parcel and the physical media must be

securely packaged so that it does not break or crack.

The recipient should

Last Reviewed: [Last Reviewed]

급 HighTable

Version: [Version Number] Classification: Internal

3.6.4 Data transfers on removable media / memory sticks

Only company owned removable media is to be used for transferring information in line with policy the device usage is approved, recorded in the asset register, assigned, and encrypted.

The removable media must

Clear instructions of the recipient's responsibilities and instructions on what to do if they are not the intended recipient must be given.

Any accompanying message or filename must not reveal the contents of the media.

The process described for must be followed.

3.6.5 Telephones, Mobile Phones and General Conversations

As phone calls may be monitored, overheard, or intercepted (either deliberately or accidentally), care must be taken as follows:

 Be conscious of your surroundings especially on public transport such as trains and public places such as coffee shops when discussing personal, confidential, or otherwise sensitive information.

Last Reviewed: [Last Reviewed]

Page 8 of 14



•	Personal data must not be transferred or discussed over the telephone unless
	you have confirmed the identity and authorisation of the recipient.

•	When using answer phones

3.6.6 Data Transfers over Bluetooth

Bluetooth is not approved as a communication method for unencrypted confidential, personal, or otherwise sensitive data.

- Ensure device mutual authentication is performed for all accesses.
- Enable encryption for all broadcast transmissions (Encryption Mode 3).
- Configure encryption key sizes to the maximum allowable.

•	Establish a —minimum key size	
		•

Last Reviewed: [Last Reviewed]

Document Owner: [Document Owner]

Page 9 of 14



 Note: A "secure area" is defined as a non-public area that is indoors away from windows in locations with physical access controls.

Users should not respond to any messages requesting a PIN, unless the user
has initiated a pairing and is certain the PIN request is being sent by one of the
users 's devices.

•	
	İ

3.7 Lost or missing information

If it is discovered or suspected that information has been lost, is missing, did not arrive, or has gone to the wrong person then the employee or external party user is required to inform at least one of their line manager, the information security management team, the management review team, or the senior management team immediately at which point the company Incident Management Process will be followed.

Last Reviewed: [Last Reviewed]

📊 HighTable

Version: [Version Number] Classification: Internal

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy

through various methods, including but not limited to, business tool reports, internal

and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information

Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action,

up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.

Last Reviewed: [Last Reviewed]

Page 11 of 14