HIGHLANDER PAPER RECYCLING LTD

COMMUNICATIONS POLICY STATEMENT

Our documented Integrated Management System (IMS) includes a procedure detailing what management system communications are in place including communication of any safety alerts and updates. The procedure also details who has the authority for any external communications and how these communications are managed and logged. This includes any communications with regulators for compliance obligations.

Use of Communication Facilities

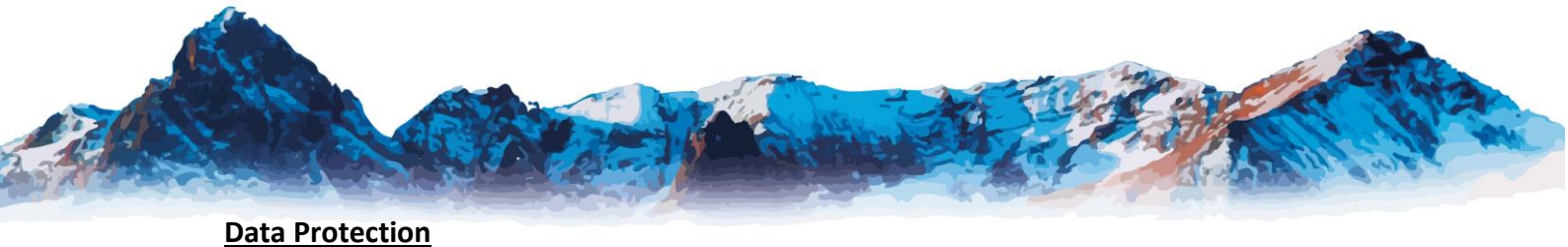
All company staff with access to information technology and communications facilities are required to use these facilities sensibly, professionally, lawfully and with respect for the company and interested parties and in accordance with this policy and other company rules and procedures.

The company is ultimately responsible for all business communications and although privacy of employees will be respected as far as possible, we may need to monitor business communications and internet traffic data for various reasons such as those stated below:

- Review of transactions/orders
- Compliance with legal regulations/requests from enforcement agencies
- Monitoring standards of service
- Preventing or detecting unauthorised use of communications systems or criminal activities and the maintenance of communication systems

The communication facilities are made available to users for the primary purpose of the business although a certain amount of limited and responsible personal use by users is also permitted during break times only. If our rules and procedures are not adhered to, then use of our facilities may be curtailed or withdrawn and disciplinary action may thereafter follow.

All messages sent on email systems or via the internet should demonstrate the same professionalism as that which would be taken when writing a letter. You must not use these media to do or say anything which would be subject to disciplinary or legal action in any other context such as sending any discriminatory (on the grounds of a person's sex, race, disability, age, sexual orientation, religion or belief), defamatory, or other unlawful material. If you copy an email to others, it may breach the Data Protection Act if it reveals all the recipients' email addresses to each recipient. Accordingly, it may be appropriate to use the 'Bcc' (blind carbon copy) field instead of the 'Cc' (carbon copy) field when addressing an email to more than one recipient.



Data Protection

Care must be taken to ensure all staff comply with Data Protection rules and GDPR. Whenever and wherever you are processing personal data you must keep it secret, confidential and secure, and you must take particular care not to disclose to any other person (whether inside or outside the company) unless authorised to do so.

Information Transfer

When transferring information internally or externally consideration should be given to the security of the transfer to ensure adequate protection of the information is in place. Confidential information should not be sent by email to an internal or external source or saved to removable media without additional security. Company information should never be stored to personal cloud storage or sent to a personal email account.

Approved by Board of Directors
February 2020