Data Protection

As a business it is critical that we protect our customer's information and data to ensure that we only disclose sensitive or commercial information to those authorised.

Inevitably as we grow and new staff come on board, it's crucial that we have some rules and protection place, It is not designed to slow things down and tie us up in knots, as that leads to unhappy customers.

It is merely there as a common sense approach that protects both us and the customer from financial penalty.

So there are some rules, document, system enhancements that will be put in to place to help us achieve this;

Customer information sheet: this now includes a 'page 2' titled 'Authorised Account Access' customers will need to fill this section in if they wish to grant account access, to anyone other than those listed in Page 1 **(who must be CRM Contacts)**

Common sense: If you aren't sure that the person you are speaking to is either the decision maker or an authorised person on the account. Then please follow basic DPA rules by asking a couple of simple questions. Such as;

- Full postal address
- Name of tariff
- Amount of handsets on account

If they answer the question correctly and with little hesitation then proceed with request. Should you not be satisfied with the how the questions were answered.

Place the caller on hold and call the decision maker to verify that the request is genuine or escalate to a member of the management team.

If you know the caller by voice due to them being a legacy customer or one whom you speak with frequently then its business as usual.

Decision maker and those with Authorised Access; will have full access to account including

- Lifting of BAR'S
- Tariff information
- Equipment Orders
- PAC Code requests *

*Please note that all PAC Requests will also be emailed to the account decision maker

General users on the account can still call us directly to perform general tasks, such as;

- Activate sim swaps
- Place lost or stolen BAR'S on handsets
- Obtain international call charges
- Voicemail PIN resets
- Faulty handset exchanges

Storage of customer data:

Sensitive customer data such as, Personal details, bank details and sensitive information such as billing and mobile numbers must be stored securely on the CRM within the customers' folder.

It should never be printed and left on desks and it should not be kept on your email.

- Please delete or archive emails that contain customer information sheets from your inbox once they have been uploaded into CRM
- Once you have finished with 'paper' bills and other 'paper' customer docs. Please place these in the secure waste disposal bins.

Accurate Records:

It is essential that customer records are kept up to date and accurately entered in to our systems, so as to prevent the possibility of data being disclosed to the wrong people.