

Intranet Acceptable Usage Policy

This Acceptable Usage Policy covers the security and use of all the Julian Harris Financial Consultants and Julian Harris Mortgages Ltd (hereafter referred to as 'Julian Harris') information and IT infrastructure. This policy applies to all employees, network members, contractors and agents (hereafter referred to as 'individuals'). This policy applies to all information, in whatever form, relating to Julian Harris and members' business activities, and to all information handled by Julian Harris relating to other organisations with whom it deals.

Access Control – Individual's Responsibility

Access to the Julian Harris Intranet system is controlled by the use of usernames and passwords. All usernames and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Julian Harris Intranet.

Individuals must not:

- Allow anyone else to use their username and password.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's username and password to access the Julian Harris intranet.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to the Julian Harris intranet, Julian Harris IT infrastructure, or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need.
- Use unencrypted devices to access the intranet.
- Use unsecured network connections when accessing the intranet.
- Access personal data held on the intranet in public where it might be seen by others.
- Use devices to access the intranet that do not have adequate anti-virus protection in place.

Users must also adhere to the Julian Harris Guide to GDPR and the Julian Harris Guide to GDPR.

It is your responsibility to report any breaches of this usage policy without delay to Head Office on 01233 661960/Agencies@julianharris.net.

All breaches of the Intranet Usage Policy will be investigated and any data security breach will be reported immediately to the ICO where applicable.