



## **Families Growing Together IT/Network Security Policy**

I take security and confidentiality seriously and has ensure I have a robust IT system in place to ensure the safe storage of information.

This policy should be read in conjunction with GDPR Policy and Reporting Data Protection and information Security Incidents Policy

I subscribes to Microsoft 365 Business Premium. This provides;

- Sophisticated software to protect me from cyber threats
- Protection of confidential and sensitive information through encryption services
- Secure One Cloud storage
- Security for devices that connect to data

### **Keeping Data Secure**

Guidance to ensure data security includes;

- Nondisclosure of any personal data either verbally, in writing or accidentally to an unauthorised third party
- Confidential paper files kept in locked cabinets in locked premises. Files should be transported in a locked case
- Users must ensure that they always log off from their computer when away from it.
- Keeping data and devices secure (password protection, encryption, secure file storage and destruction);
- Password protection for any electronic files/documents containing confidential personal data.
- Taking particular care when transferring personal data onto a memory stick, laptop or any other mobile device and using password protection and encryption.
- Securing the sharing of personal data by email by using Egress or password protection on documents if they contain more than one piece of identifying information.
- Not storing personal data on local drives or on personal devices that are used for work purposes.
- Avoiding copying confidential personal data unless it is strictly necessary.

Policy devised by Heidi Pannell

Policy Operational Date 1.2.24

Policy review date 2.8.27