PRIVILEGED ACCESS POLICY

Privileged access enables an individual to take actions which may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators, staff performing computing account administration, or other such employees whose job duties require special privileges over a computing system or network.

Individuals with privileged access must respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with any relevant laws or regulations, while pursuing appropriate actions required to provide high-quality, timely, reliable, computing services.

Privileged access is granted only to individuals authorised by Witney Benefice Data Controllers. Privileged access shall be granted to individuals only after they have read and signed this Agreement.

Privileged access may be used only to perform assigned job duties.

If methods other than using privileged access will accomplish an action, those other methods must be used unless the burden of time or other resources required clearly justifies using privileged access.

Privileged access may be used to perform standard system-related duties only on machines and networks whose responsibility is part of assigned job duties. Examples include:

- Installing system software;
- Relocating individuals' files from critically overloaded locations;
- Performing repairs required to return a system to normal function, such as fixing files or file processes, or killing runaway processes;
- Running security checking programs;
- Monitoring the system to ensure reliability and security.

Privileged access may be used to grant, change, or deny resources, access, or privilege to another individual only for authorised account management activities or under exceptional circumstances. Such actions must follow any existing Witney Benefice guidelines and procedures.

In all cases, access to other individuals' electronic information shall be limited to the least perusal of contents and the least action necessary to resolve a situation.
Individuals with privileged access shall take necessary precautions to protect the confidentiality of information encountered in the performance of their duties.

If, during the performance of their duties, individuals with privileged access inadvertently see information indicating serious misuse or Safeguarding concerns, they are advised to consult with the Data Controller(s) or Safeguarding Officer in the first instance or if the concern relates to a Data Controller, to pass concerns to the Archdeacon.

Anyone approved by the Data Controllers to have privileged access will sign to say they have read the Benefice Privileged Access Policy and agree to comply.

Adopted by Witney PCC	18 July 2023	
Adopted by Minster Lovell PCC	28 November 2023	
Signed	*Toby Wright*	
Counter-signed	*Kate Banks*	Witney PCC
Counter-signed	*Judith Warwick*	Minster Lovell PCC

Review date: 5 years from date of adoption