Freshfield Nursery and Tithe Barn Primary

Information and IT Security Policy

How schools and colleges can use the right digital infrastructure and technology.
All schools and colleges should be working towards meeting 6 core standards by 2030:

- broadband internet
- wireless network
- network switching
- digital leadership and governance
- filtering and monitoring
- cyber security

Meeting these core standards will help make sure schools have the essential infrastructure and governance to:

- have a strong digital strategy
- make informed decisions to get the best use out of your digital technology
- use digital technology safely and securely
- meet the other digital and technology standards

IT Providers at our schools:

School	IT Support	Broadband	GDPR Support
Freshfield	**MGL**	**LA**	**LA**
Tithe Barn	**MGL**	**MGL**	**LA**

- IT support providers are responsible for ensure anti virus and smoothwall software are updated regularly.
- IT Licences are renewed with consultation IT Support and SBM.

All PCs at our schools should have:

- Anti virus protection
- Filtering and monitoring Smoothwall
- Backed up daily by IT support
- Smoothwall alerts are to be sent directly to the Headteacher email address and weekly reports are sent to the Headteacher email address

Staff Responsibilities

1. Staff are reminded not to use school devices for their personal use.

2. Memory sticks should not be used to transfer data/information and they can contact viruses.
3. Staff should sign the acceptable use policy as part of their induction
4. Regular reminders of these points are to be shared on the weekly bulletins
5. Staff should use complex passwords for their email and server accounts plus any software they use for school
6. Office staff, Headteacher and one governor to have completed cyber security course
7. Staff induction includes stay safe online course and data protection courses
8. Staff to lock their screen when leaving their PC
9. Staff to be informed of any phishing warnings as soon as they are received
10. Staff to report any phishing attempts to IT support immediately
11. Headteacher and SBM to attend annual Information Governance training
12. Staff to report any breaches immediately to IT Support and Headteacher/SBM

Staff Working at Home

1. Do not leave laptops/devices unattended at home when visitors are present
2. Ensure anti-virus protection is installed and updated on laptops/devices
3. Staff should not leave confidential information in cars/transport
4. Confidential information should be stored out of sight when not in use at home and returned to school at the earliest opportunity
5. Staff taking iPads home should sign the form in HT office

Governor Responsibilities

https://www.ncsc.gov.uk/collection/board-toolkit

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ncsc.gov.uk/sites/default/files/documents/Board-Toolkit-101.pdf

1. One governor to have completed cyber security course – this is to be made available to all governors
2. Governors to be aware of cyber security tooklit as above link
3. Consider GDPR documents and policies for approval

Artificial Intelligence

Schools aim to have an AI Policy and Cyber security Policy in place by 2030.

Assurance Dashboard

Schools should complete the IG Assurance Dashboard and submit this to IG support. This together with action points should be shared with Governors.

Record of Processing Documents

Schools should have a RPO documents which is updated regularly.

GDPR Policies and Privacy Notices

These should be updated regularly and uploaded to schools' websites.

Updated privacy notices are issued to the relevant stakeholder

Freedom of Information Requests

FOI requests received by schools are to be referred to IG Support at the LA igschoolsupport@stockport.gov.uk for their advice. IG templates are to be used for the schools' responses.

Records ae to be kept electronically for these responses.

FOI requests/requests for personal information – applicant should complete the relevant forms available on the individual school websites before school responds. The applicant should prove their ID and relkationship to the pupil, if this relates to pupil personal information.

Data Processing and Data Sharing Agreements

Any new contracts/software the school uses should be cecked with the LA IG support for approval. Due diligence forms are to be completed by the SBM and emailed to IG Support together with privacy notices, data protection policy and data processing/sharing agreements if available.

Governors should be informed of any new agreements via termly financial reports.