# Bromcom Cloud FAQs

Below is a list of Frequently Asked Questions about the Bromcom Cloud MIS.

## Hosting and Support

**Is it hosted (and will always be hosted) in UK?**

Yes. Bromcom's hosting provider is based in the UK and has a strict policy in place to prevent data being stored abroad.

**Hours of support/availability?**

Support hours will remain identical to the hours provided to standard MIS users. Bromcom's MIS Solution is hosted on the Microsoft Azure platform and uses the extensive features that this platform offers to provide an impressive 99.9% SLA for solution uptime/availability. This SLA statistic is closely monitored on a daily basis using enterprise level monitoring applications ensuring both performance and uptime is optimised.

**Will we have the flexibility we currently have with our own server for bespoke fixes/config?**

Each school has its own database so database level fixes are possible for each school however there is only one instance of the application. This means that any application fixes will be applied for all sites at once.

**What control do we have over the application of updates/releases?**

Though individual schools can influence when updates are run Bromcom have the final decision on when an update that will affect all schools running on the cloud server is implemented.

**If we delete something we shouldn't what are the procedures/terms for a restore?**

Bromcom will keep daily backups of data for every school on the cloud server for 30 days. A school can request a restore of data at any time to any overnight backup from the last 30 days. This will allow the restoration of the database and files to any one of these days. Bromcom do not provide a more granular restoration of files than this. Please note this level of backup and restore is the same for locally hosted MIS solutions.

**What is the recommended broadband capacity in order use your system?**

Bromcom recommends the following bandwidth according to school size:

- Up to 100 pupils – 2mb
- Up to 300 pupils – 4mb
- Up to 500 pupils – 6mb
- Up to 1000 pupils – 8mb
- Up to 1500 pupils – 10mb

## Disaster Recovery

Bromcom MIS solution is hosted with no single point of failure within the datacentre it is hosted in. this includes redundant web, SQL, Domain controller.

Bromcom has utilised the Azure availability sets feature ensuring system availability is maintained even when 'Microsoft competes its necessary regular maintenance tasks.

However in the unlikely event of a disaster that takes down the entire region where Bromcom MIS is hosted, backups are stored in geo redundant datacentres ensuring restoration of data will always be possible (outside of EU wide datacentre failure). Complete restoration of the entire solution into a functional Azure region will take no more than 36hrs to complete.

As we grow Bromcom has plans to expand its datacentre hosting across multiple regions to mitigate against the regional outages that rarely hit Microsoft datacentres.

## Access Controls

**Are access controls secure and robust?**

Bromcom only Support staff that require access to the Bromcom Cloud server are granted access. This includes the SupportDesk, Investigation, IT and Software Teams.

The type of access these teams have is highlighted below:

**Support Staff with access to the Bromcom Cloud Server**

| Bromcom Teams | Access to Application Front End | Access to Remote SQL Management Studio * | User Level Remote Control of Server | Admin Level Control of Server |
|---|---|---|---|---|
| Support Desk | ✓ | ✓ | × | × |
| Investigation Team | ✓ | ✓ | ✓ | × |
| Software Team | ✓ | ✓ | ✓ | × |
| I.T Team | ✓ | ✓ | ✓ | ✓ |

*** All Support Staff are given secure remote control access to a PC located at the data centre. This PC has SQL Management Studio installed and allows support staff limited access to run SQL queries necessary to provide support to Bromcom Cloud customers**

All staff that have access to schools data are DBS checked.

**Do passwords expire?**

Yes. Bromcom has a strict password policy in place whereby local accounts expire after 42 days and these accounts are changed on a monthly basis.

Each school is in charge of the configuration of its own database and can set their access to their database to have whatever password policy Bromcom MIS allows.

**Do accounts lock out if too many attempts are made with the wrong password?**

The cloud server's password policy is set to the following:

- Minimum Password length: 7 characters
- Min password age: 42 days
- Max Password Age: 15 days
- Password complexity: enabled
- Lockout threshold: 5 attempts
- Lockout duration: 30 mins
- Reset account lockout: 30 mins

**Can you authenticate against our Active Directory still (as we can with the local solution)?**

Active directory authentication is available to any Bromcom MIS customer. For this option to work for Cloud customers however schools will need to provide secure access to their Active Directory over the web.

**Is the transfer of data over the internet encrypted?**

All connections to the cloud are forced over an encrypted 128bit SSL connection. Preventing data from being readable in transit as well as preventing data from being cached on client PCs.

**Can we restrict access to only certain IP addresses?**

Unfortunately the cloud solution is used by multiple schools and by staff outside of schools so it is not possible to lock down access to the Cloud server.

**Can we restrict timings for access for certain users or block access during school holidays etc?**

The school are in charge of the accounts that can access their data base and so can control which accounts are active and when. Please be aware that this is a manual process.

## Storage/Downloads

**Are there limits on how much information we can store/how big the DB can get?**

Bromcom MIS Cloud has no limits on how big a school database can get. However files saved in Bromcom MIS cloud are stored in its DMS. The Document Management System is limited to a total storage capacity. Please refer to the standard terms and conditions for information on storage limits.

If you require any further assistance please contact the Bromcom support team on 020 8290 7177.

# Bromcom MIS Cyber Security Protection

**HTTPS Encryption**

Bromcom MIS has a single URL for access (https://cloudmis.bromcom.com). This is made available to users over the web only via encrypted SSL port 443. Using the HTTPS Protocol ensures that data is encrypted in transit at 128-bit level (the same as used for internet banking) and not cached on the local PC.

**Login Protection**

Bromcom MIS has the facility to implement extensive login security including two factor authentication, memorable information, password policy and Active directory integration.

**Roles and Permissions**

A single role will be applied to all students in the system which will govern what information Students can access. This role can be edited allowing control of what data is shared with students.

**Active Directory Integration / SSO**

The Bromcom MIS system supports access being authenticated against any existing Active Directory infrastructure via LDAP. This allows Single Sign to be put into place and enforce the schools password policy.

The login process will automatically authenticate against the active directory details and link to the Bromcom MIS accounts

**Firewall**

Bromcom MIS utilises the firewall capabilities offered by the MS Azure platform and locks access to the solution down to 2 entry points:

1. HTTPS web front end to the MIS solution (as explained above)
2. RDC access to the backend via a single jumpbox for Support purposes. This connection is locked down to only accept traffic from Bromcom Head offices and uses a non-standard port for access.

The solutions internal network also utilises firewall protection to ensure only necessary communication between servers is allowed.

**Backup**

The Cloud backup policy includes the following:

1. Weekly full and daily differential backups with a retention period of 30 days of individual school databases
2. Full VM level backup of each VM in the solution with a 6 day retention

Backups are regularly tested to ensure restoration capabilities are available

**Anti-Malware**

Every VM that makes up the Bromcom MIS solution is protected by Azures built in Antimalware extension. Updates and patching of this extension is completely handled by Azure and ensure that the solution is always kept up to date with the latest signatures. Scans are also scheduled to be performed outside of work hours to have minimal impact on performance.

**Staff Education**

We have clearly defined network security policies that ensure all staff are aware of their responsibilities and best practices for supporting the Bromcom MIS solution.

**Accreditation**

Bromcom has the following accreditations:

**ISO 27001 Certified (from April 2020) -** is an information security standard which ensures our information security has robust management controls in place.

**ISO 9001 Registered -** which encompasses our policies on cyber security and ensures they meet customers and stakeholder needs within statutory and regulatory requirements. This standard also ensures these policies are continually managed, maintained and enforced.

**Cyber Essentials Security Certified –** is a UK government information assurance scheme operated by the National Cyber Security Centre (NCSC) that encourages organisations to adopt good practice in information security.

## Microsoft Azure Platform

### Azure Penetration Testing

The Microsoft Azure platform is regularly audited the results of which are readily accessible.

You can find a general overview on Microsoft G-Cloud Page:
https://www.microsoft.com/en-us/TrustCenter/Compliance/UK-G-Cloud

Reports are held on Microsoft's Service Trust Portal and can be made available on request.

### Azure Security

The features listed in the table below are security capabilities that the Azure Platform offers as standard. Further detail on this info can be found here:

| Secure Platform | Privacy & Controls | Compliance | Transparency |
|---|---|---|---|
| Security Development Cycle, Internal audits | Manage your data all the time | Trust Center | How Microsoft secures customer data in Azure services |
| Mandatory Security training, background checks | Control on data location | Common Controls Hub | How Microsoft manage data location in Azure services |
| Penetration testing, intrusion detection, DDoS, dits & logging | Provide data access on your terms | The Cloud Services Due Diligence Checklist | Who in Microsoft can access your data on what terms |
| State of the art data center, physical security, Secure Network | Responding to law enforcement | Compliance by service, location & Industry | How Microsoft secures customer data in Azure services |
| Security Incident response, Shared Responsibility | Stringent privacy standards | | Review certification for Azure services, Transparency hub |