
# INFORMATION SECURITY POLICY

Approved by BoD: September 2020
Policy Review Date: September 2022

**Introduction**

The purpose of this policy is to outline how we store data on computer systems throughout the academy, who has access to this data and how we ensure the security & reliability of this data and the systems it is stored on.

**Who has access to personal data stored on the computer system**

All users who access a computer throughout the academy must sign the acceptable usage policy (AUP), this details what the computer systems may and may not be used for and explains what steps need to be completed to ensure the safety and privacy of all users throughout the academy is upheld. A copy of the AUP is also displayed for all users before they login to ensure they are fully aware of their roles & responsibilities. All activity is monitored for safeguarding purposes and to ensure compliance of academy policies.

**What information do we store on the computer system and where is it stored**

Please find below a summary list of the some of the information we hold on the computer systems throughout the academy, the reasons why and where this data is stored:

| **Type of information:** | **Reasons:** | **Storage location:** |
|---|---|---|
| CCTV | CCTV is used throughout the academy for the purposes of crime prevention and safeguarding. Footage is stored on hardware based video recorders and is held between 2 – 4 weeks (depending on area). In the event of an incident occurring, footage will be extracted and stored on a file server to ensure it is not overwritten, footage would then be removed once any investigation has finished.<br><br>CCTV is only accessible to Site Staff and the ICT Support Team. | Network Video Recorders<br><br>Servers<br><br>Portable Backup Hard Drives (Encrypted) |
| Classroom Monitoring Software | Screenshots may be automatically taken of users computer activity when suspicious activity is detected, this is in accordance with safeguarding requirements including the PREVENT strategy. | eSafe<br>LanSchool |

| | | |
|---|---|---|
| Internet Browsing Activity | All internet activity conducted by users onsite is logged for the purpose of providing a safe and filtered connection and to identify any safeguarding concerns and to ensure we are compliant with the PREVENT strategy. The data logged will include websites visited, search terms entered, IP address of device and username of the person browsing the internet. | Sophos XG Web Filtering System<br><br>Stored in secure datacentre |
| Letting details including contact details | This is required to enable the co-ordination of lettings and to contact in the event of cancellation and for the purposes of providing invoices for services rendered. | PS Financials<br><br>Paper files stored in filing cabinets<br><br>Backed up and stored offsite by PS Financials. |
| Photographs | Photographs of students, staff or members of the public may be taken for the purpose of evidence of activities conducted throughout the academy, photographs will only be kept for those who explicitly consent to the use of their photographs. | Advertisements<br>Displays throughout the academy<br>Prospectus & publications<br>Servers<br>Social media platforms<br>Website |

| | | |
|---|---|---|
| Pupil & parent contact details, date of birth, gender, medical information (including medical practice), dietary needs, SEN details, disabilities, mode of transport, free school meal eligibility, ethnicity, nationality, first language, country of birth, religion, in care, achievement & behavior incidents, assessment data, previous test results items of consent (e.g. photo permission) | This information is collected to ensure students are placed in the correct teaching groups based on their ability, staff are made aware of medical conditions to ensure students are looked after whilst in our care and that we have adequate contact details to contact an appropriate adult in the event of issues and to discuss attendance, achievement, behavior, progress and other matters relating directly to students education. | MIS system<br>(SIMS)<br><br>Examination Software<br><br>Paper files based in locked filing cabinets<br><br>Backed up nightly to server in datacentre and offsite NAS and encrypted portable hard drives held in fire proof safe on a regular basis. |
| Staff contact details, date of birth, gender, next of kin, absences, ethnicity, religion, national insurance number, bank account details, qualifications, proof of ID and consent information | This information is collected to enable the academy to keep a record of staff employed, contact staff or next of kin if and when required and payment information to enable payment of salaries. Proof of ID is required for safeguarding purposes. | MIS System<br>(SIMS)<br><br>Payroll System<br><br>Paper files based in locked filing cabinets<br><br>Backed up nightly to server in datacentre and offsite NAS and encrypted portable hard drives held in fire proof safe on a regular basis. |
| Supplier details<br>(contact details and bank account information) | This is required for the processing of orders and to enable payments to be made to suppliers. | PS Financials<br><br>Paper files stored in filing cabinets<br><br>Backed up and stored offsite by PS Financials. |

**Security steps taken to ensure data is kept secure**

The following steps are taken to ensure all data held on computer systems is stored safely to prevent data losses:

- Storage areas have strict permissions to ensure information is only made available to those who require it
- Software holding personal data is secured with credentials and no users share details to allow for accountability, staff only have access to areas
- All staff laptops are encrypted to ensure only authorised users have access to the information stored within
- Remote access to systems is provided only to approved members of staff
- All portable storage devices used by staff to transfer data are encrypted
- Server locations are behind locked doors with limited staff having access, all sensitive data is stored in a central datacentre controlled by access control, CCTV and limited access
- Email encryption is configured for transmitting personal data over the internet
- Regular backups are taken and stored offsite or in fireproof locations for business continuity

**Destruction/disposal of data**

All data stored electronically is securely disposed of when no longer required and retention periods have been reached. All data is irretrievably destroyed by the use of advanced wipe procedures to Infosec Level 5 Standard, and where this is not possible, is destroyed physically so as to render any data thereon irretrievable, and where applicable in accordance with EN 15713:2009, certificates of data destruction are available to be viewed as evidence.

**Contact us**

If you have any questions, concerns or would like more information about anything mentioned in this document, please contact our **data protection officer:**

Miss F Sumner, Bishop Milner Catholic College, Burton Road, Dudley, DY1 3BY