ALDRIDGE EDUCATION

Information Security Policy

Document Control Table	
Version no:	2
Date of last revision:	July 2023
Approval Required By: (Adoption and full 5 Year Review)	Board of Trustees
Date approved:	August 2023
Policy owner:	Director of IT
Frequency of revision:	2 years
Next review date:	July 2025
Revision approval required by:	Chief Executive Officer
Policy family:	Information Technology
Policy status:	Approved

Applies to (Mark as appropriate)			
Staff	Pupils / Students / Adult Learners	Parents / Carers / Guardians	Contractors
✓			✓
Volunteers	Students on placement	Trustees / LGC / Members	Visitors
✓		✓	✓
Agency Staff	Other	a	a
✓	✓		

Published Locations				
Trust Website	Academy Website	Aldridge Intranet	Student/Parent planners	On-request
		✓		✓

Consultation (Complete as appropriate in line with master policy document)			
With	Reason for Consultation	Final Consultation Date	Version No

Version History (please note below if a policy has been replaced)					
Version	Reviewer	Revision Date	Nature of Change	Adopted/ Approved by	Approval Date
V1	JB and MG	August 2022	New Policy	Chair of BOT	May 2023
V2	TM,KF, MG	July 2023	Changed in line with KCSIE 2023, Filtering and Monitoring systems	CEO	August 2023

Content

1. Introduction

This policy forms part of the Trust's Information Governance Strategy and sets out minimum standards, guidance, and procedures for ensuring confidentiality, integrity and availability of Information and Information Management and Technology assets. This policy relates to the overlapping areas of Data Protection, Data Quality, Confidentiality, Information Sharing, Freedom of Information, Information Risk Management, IT Security, Information Security and Records Management.

2. Scope and purpose

2.1 Policy Coverage

The policy covers all aspects of information within the Trust, including (but not limited to):

- Student user information
- Staff//Governor/Contractor user information.
- Trust Information

This policy covers all aspects of information handling and processing, including (but not limited to):

- Structured record systems (paper and electronic)
- Transmission of information (Fax, post, email, and telephone)

This policy covers all information systems purchased, developed, managed, or utilised by the Trust, and any individual (directly employed or otherwise by the Trust) accessing information owned entirely or partially by the Trust.

2.2. Related Policy and Codes of Conduct

In setting out standards relating to information governance, a number of controls are specified relating to:

- Job responsibilities
- Applicant screening
- Terms and conditions of employment
- Disciplinary action
- Professional codes of conduct.

These controls must be integrated with related Human Resources policies.

3. Related policies

- E-safety policy
- Child Protection Policy and Safeguarding Policy
- AAL Adult Safeguarding Policy
- Social Media policy
- Data Protection policy
- Acceptable Use policy
- Records Retention policy
- CCTV policy

4. Legislation

The main relevant legislation affecting the stewardship and control of information for the Trust includes the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The UK General Data Protection Regulation (2021)
- The Data Protection Act (2018)

- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010
- Common law duty of confidentiality
- Computer Misuse Act 1990
- Communications Act 2003
- Limitations Act 1980
- The Education Regulations 2014 (with reference to educational record)
- Information Records Management Society 'Information Management Toolkit for Academies' 2020

5. Security roles and responsibilities

5.1 Ownership of information assets

The role of the information asset owner (IAO) is to understand what information is held, what is added and what is removed, how information is moved, who has access to it and why. Information asset owners must be trained as part of their induction training or when they assume responsibility for any information asset. The IT team will undertake compliance checks on permissions, users' management, and information security principles as part of the information security programme to make sure IAOs comply with the trust expectations on information security. As a result of compliance checks, where appropriate, staff will be given further training if required. IAOs must be able to understand and address risks to the information and ensure that information is fully used with the law, regulations, and UK standards. Information Asset owners hold responsibility and privilege roles for administering certain software, department file storage or team's information. Positions in the Trust that undertake the role of IAOs include; Trust Lead - Data MIS (Bromcom), Academy MIS leads, HR Business Partners, Finance directors, Senior IT Technicians, Data Protection Leads, Designated Safeguarding Leads, etc.

Information Asset Owners are recorded in the ROPA (Record Of Processing Activities) as part of the trust data protection responsibilities. The IT Team must hold records of all software administrators across the Trust.

All this information will be updated through our Information security programme, IT change management process and the trust data protection yearly activities.

5.2 DPO

- To inform, guide, advise and lead the Trust on data protection compliance and obligations.
- Ensure and monitor compliance with GDPR and all UK data protection laws and regulations, including raising awareness, staff training and audits.
- Produce, review, and advise on all data protection impact assessments.
- Liaising with the Director of IT, COO and CEO on all information security matters.
- Be the first contact point for all ICO, staff and external individuals on data protection, processing, and activities.
- Lead and advise on all subject access requests.
- The DPO will delegate some of these tasks to the DPL (Data Protection Leads) at each site as appropriate.

5.3 Director of IT

- Must be able to carry out information security duties in an independent manner.
- To be responsible for the implementation of the policy and monitoring for compliance.
- Implementing an information security programme and strategy that ensures compliance with all UK laws and regulations, sector industry standards, data protection, safeguarding and DFE digital standards.
- Review the information security programme and set a continuous improvement approach.

- Ensure that our information security governance is adequately controlled and directed, coordinating the security activities with the agreed information security programme.
- Ensure that all three information security principles (Confidentiality, Integrity, and Availability) are correctly identified, protected, and risks mitigated.
- Responsible for linking security activities to the organisational goals and objectives.
- Lead the IT Team and the organisation to a better information security posture, ensuring accountability for decision making and provide feedback to decision makers on the impact of their choices.
- Work alongside other areas and departments to implement a wider approach and embed security in every area of the organisation.
- Lead the organisation to create the right security configuration, administration and operation of the IT infrastructure and services and ensure compliance.
- Manage the implementation of security measures for IT systems and information during their entire life cycle.
- Ensure that all users carry out the correct information security training and awareness.
- The Director of IT will delegate some of these tasks to the IT Team as appropriate.

5.4 Principal

- Principals must ensure that all employees receive the correct instructions, training, and resources in accordance with the Trust induction procedures, which must include, safeguarding, Health & Safety, cyber security, e-safety and GDPR training.
- Principals must work with the Trust to make sure that time is allocated to training and development of staff in information security and all related policies.
- Principals will review security incidents with the Director of IT and take appropriate action to safeguard our staff, students, information, and assets.

5.5 Staff, contractor, consultants, and any other users AE IT systems.

- All users of Aldridge Education IT hardware, software and IT systems must undergo all the Trust mandatory IT training.
- All users must comply with all Aldridge policies.
- User must ensure that no breaches of information result from their actions.
- Users must report any breach, suspected breach, hardware and software malfunctions, or cyber security incidents without delay.
- All users must use two factor authentication (2FA).
- Users must use unique passwords for accessing the Trust IT systems.
- Users are responsible for always keeping their passwords confidential, must never disclose them to anyone, including line managers, assistants, or IT staff.
- Written down passwords on paper or electronically are not permitted.
- Users must never access systems that they have not formally been authorised to use.
- Users must not bypass, disable or in any way circumvent our system systems and controls.
- Users shall always ensure that unauthorised individuals are not able to view any schools or Trust information on any device.
- Computers should always be locked when unattended.
- Users must never store confidential information on unencrypted portable media.
- Users must inform the IT team of any incidents that could risk the confidentiality, availability or integrity of our systems and information.
- This is not an exhaustive list, and it supplements the Staff acceptable use, E-safety, and social media policies which users must comply with as well.
- Staff that are main administrators for any software must follow the guidance in this policy to manage information (confidentiality, integrity, and availability), permissions, user provisioning, privileges and identify management.

5.5 Confidentiality agreements

- All IT staff should sign an NDA before having privileged access to any IT systems.
- Anyone not covered by an employment contract will be required to sign a confidentiality agreement before given access to any confidential information.

5.6 Line managers

- Managers should make sure that their departmental staff understand and abide by this policy and all Aldridge Education policies.
- Managers must ensure that all staff complete all required training within the timescales specified.
- Managers must ensure that staff return equipment, keys and inform the relevant staff and departments so their access is revoked immediately after leaving the organisation.

5.7 Terms and conditions of employment

- Terms and conditions must reflect the employee's responsibilities for information security and should explain the responsibilities are required in perpetuity and not just for the length of their employment. The terms and conditions will state these responsibilities are for all times, including outside the work environment. A breach of confidentiality could lead to a disciplinary, dismissal and or legal action.

5.8 User training

- The trust will provide appropriate and up to date user training on e-safety, cybersecurity, best practice, software guides and secure processes. All staff have a duty to carry out the training as scheduled or arranged by the Trust or their line manager.
- E-safety, safeguarding and cybersecurity training are mandatory for all staff.

6. Physical and environmental security

6.1 Working onsite

- All staff, contractors, agency workers, visitors and any other person in our schools must always wear their ID badge. The badge must be clearly displayed.
- Visitors must be always escorted.
- Visitors must follow the reception and site entrance procedures.
- CCTV and access controls systems must be always operational.

6.2 Physical security perimeter

- Reception areas must be staffed at all times during school day. Outside of these times, doors should remain secured to control access into the building.
- All school sites must be secured. This can be achieved through the use of physical buildings, walls, fences, entry gates and/or secured doors.
- No member of staff or the general public should be allowed access into the buildings without signing into reception.
- Anyone onsite without an enhanced DBS must always be escorted by a member of staff.
- All visits should be prepared well in advanced and enhanced DBS should be provided in a timely manner.
- CCTV must be used in all our school's sites for the security and safety of the trust staff, students, and visitors. Please refer to the CCTV policy for more information.
- All entry and exit systems should be part of the network access control system, so that events can be audited and reviewed periodically.
- CCTV and access control systems should be appropriate maintained, setup, audited and have accurate times, syncing with internet atomic clocks.

6.3 Physical entry controls and secure areas.

- The objective of this section is to prevent unauthorised access, damage or interruption to our organisation, staff, students, and information. All areas should be protected by a clearly defined security perimeter and access controls. The protection provided should be commensurate with the identified risks. The IT, Estates team and principals must use a risk-based approach to protect our sites and buildings.
- Entry to secure areas or rooms should be controlled at all times through appropriate access controls. Some examples are: Exam storage rooms, finance offices, network equipment rooms, server rooms, etc.

- External contractors and anyone not normally authorised in these areas/rooms that need access, should be always escorted and never to be left alone while inside these secure areas.
- Keys or codes to enter core infrastructure rooms must never be given to external companies or contractors.
- Any members of staff entering a code into a secure area or safe must take due care and avoid anyone looking over their shoulder or any other way to prevent access to confidential information.

6.4 Security of offices, rooms, and facilities.

- Staff processing or using information must always take appropriate measures to secure our information. Examples are lockable draws and cabinets, locking windows, restricted entry using network access controls systems, clear desk policy at all times and clear monitor desktop.
- These security measures should be reviewed regularly by all staff members, line managers and members of SLT. All staff members have a duty of care to ensure that we have adequate protection for all information whilst maintaining appropriate availability.
- Doors and windows should be closed and secured, blinds/curtains drawn (if available), and alarm systems set when the building is unoccupied.

6.5 Equipment security

- All staff must take due care in preventing any loss, damage or compromise of organisational assets and interruption to teaching, learning or other activities.
- All equipment should be adequately protected and physically secured from any threats or environmental hazards.
- Staff should always consider equipment location and disposal.

6.6 Location and protection of information assets.

- Screens and paper records must be positioned to reduce any risk of being overlooked during use. Shoulder surfing is a very common hacking technique to steal or gain access to confidential information.
- Privacy barriers, folders, and privacy screens must be used when the information can be easily view from a public area or location.
- Papers with confidential, personal, or sensitive information must be shredded and disposed of securely using an accredited disposal organisation. Certificates of destruction must be provided and retained for audit purposes. Staff must not use normal bins for any paperwork containing confidential, personal, or sensitive information. Dumpster diving (foraging through someone's rubbish to obtain information) is a very common technique used by hackers.
- All equipment should be positioned away from windows (unless additional protection is in place) and areas of easy access.
- Any electronic equipment or paperwork which contains confidential information which is in public areas, must be secured through the use of locked cabinets, cages, or security cabling.
- Equipment should be positioned away from fire risks, water, dust, chemicals, excessive moisture, heat, and electromagnetic radiation.
- Critical IT equipment such as servers, switches, routers, and other core network infrastructure should be placed in an appropriate controlled environment, with isolated power supply, temperature controls, right levels of humidity, fire controls, controlled physical access, and redundant technologies in case of single components failure. All critical equipment must be regularly checked and monitored through environmental control equipment with adequate alerts.
- Eating and drinking is not permitted near organisational equipment, especially near critical equipment.
- Staff causing damage to any equipment due to spillage may be responsible for the cost of the repair or replacement.

6.7 Power supply

- Appropriate power supply for equipment should be considered when staff are working on new installations, projects, changes, or replacements.
- All equipment must be electronically tested to make sure it is safe to operate. PAT testing is conducted by the Estates team to routinely check for safety.
- Staff should do a visual check before using any electrical equipment and report any damages immediately.

- All critical equipment like servers and switches must be provided with power supply protection through the use of UPS (Uninterruptible Power Supplies) systems.
- UPS equipment used on IT equipment must be regularly checked by the IT Team to ensure it has appropriate capacity, suitable for use, and tested in accordance with the manufacturer's recommendations.
- All laptops and other portable equipment should be checked regularly for battery and manufacture recalls due to their risk of fire.
- All laptop, chrome books and tablet trolleys must be checked yearly checked by the IT team due to their portability and risk of cabling damage.

6.8 Cabling security

- All new cabling should be routed and patched to the central switch rooms in the appropriate cabling trays, conduits, or existing trunking.
- All new patching should be clearly labelled, and numbering should be in continuation of the existing numbering protocol.
- All new cabling should be a minimum of CAT6 certified cabling.
- All new cabling installed underground or externally should have the external protection appropriate to the location and take care of external factors, unauthorised access to cabling and rodents that can chew on the cables.
- Special care should be taken when installing fibre cabling due to their fragile nature.
- Avoid exposing cables to areas of condensation, direct sunlight, and high humidity.
- Avoid bending network cables, especially fibre cabling.
- Cabling must be reviewed yearly for security and health and safety reasons.
- Any cabling work, changes and new installations should be done through a change request so approval, appropriate consultation and assessment can be done at early stages of the project.
- All cabling should be installed in accordance with fire regulations to prevent the spread of fire between fire segregated compartments. Cables are required to be flame retardant and installed within containment, having the necessary resistance to flame propagation in line with current regulations.

6.9 Equipment maintenance

- All IT equipment should be maintained in accordance with the manufacturer's best practice and recommendations.
- All staff should be using due care and diligence when using all IT equipment provided to them for their work.
- All staff are responsible to carry out all training, instructions and follow guides provided to them for the appropriate maintenance and use of the equipment.
- All critical and core infrastructure equipment should be within manufactures support and not end-of-life. Manufactures must be releasing security patches and updates in a regular schedule and according to global security threats.

6.10 Security of equipment off-site

- All staff working off-site must be careful whilst working in public areas, where people can see or hear confidential information.
- Staff must never display confidential information in a public area, house, or common room where other people can gain access to it.
- Staff must be aware of shoulder surfing and other social engineering techniques that can be used to gain access to confidential information and systems.
- Usage should be kept to a minimum in public areas, internet cafes, outside the country, airports, busy environments.
- Staff using organisational equipment in public areas might result in a security breach. Staff must take all the necessary steps to protect the Trust information, systems, and assets.
- Staff must never leave equipment unattended, in cars, trains, unprotected areas where they are clearly visible.

6.11 Leased/Hired equipment

- All leased equipment like printers and photocopiers contain drives where information can remain (data remanence). All equipment being returned or disposed of needs to comply with UK GDPR, Trust policies, and all UK legislation. All information on these devices will need to be securely purged using appropriate current technology standards. A member of the IT team must be consulted prior to the return of any equipment that could contained any trust information.
- All equipment being serviced, going offsite, or returned must be always protected. The correct contract, information protection, technologies and processes must be in place before the start of the contract.
- When device parts are being sent offsite for repair or replacement, all information risks must be minimised, making sure information is never accessed by unauthorised individuals, lost, or disclosed.

6.12 Secure disposal or re-use of equipment

- All devices, hardware and software must be disposed in line with UK GDPR and WEEE (Waste Electrical and Electronic Equipment recycling) regulations.
- All PCs, laptops, tablets, printers, mobile phones, server, EPOS equipment, etc. must be securely disposed of to ensure that no personal or confidential information is held on them, and that all data is completely destroyed.
- All procedures must be documented with certificates of destruction for an appropriate disposal. Only the IT team must dispose IT equipment.
- IT disposal or recycling companies must have secure premises, secure logistics, data sanitation methods, industry expertise and appropriate accreditations.
- The accreditations for secure IT disposal must be in line with best practice and all UK regulations. Examples are ISO 9001, ISO 14001, ISO 27001, ADISA, Cyber essentials.

6.13 Clear desk/clear security

- All employees (staff, contractors, temporary staff, consultants) are required to clear confidential working documents, files, and other paperwork from their desks, working surfaces, walls, and shelves at the end of each day and place them in secure storage, draws or cupboards as appropriate.
- All paper and electronic information must be stored and disposed of in accordance with the Trust Records Retention Policy.

6.14 Removal, relocation of equipment

- All equipment must be disposed of appropriately when it no longer serves its intended purpose.
- The IT team will dispose of the equipment securely, backup (if required) and securely wipe any information on the device or dispose it through an accredited disposal organisation.
- Only IT can dispose of IT equipment. The IT team must use an ADISA accredited and GDPR and WEEE compliant disposal organisation. The organisation must offer 100% accuracy and accountability with the correct reporting so we can track every single one of our IT assets through the IT disposal process.
- All IT equipment must be relocated and moved by IT staff through a change request process. Movement of IT might require vlan changes, health and safety considerations, security threats or create a risk to confidentiality or safeguarding.
- No equipment, information or software should be taken, moved, or installed without authorisation.

6.15 Printing and photocopying

- All confidential printing must be carried out through the secure follow-me multi-function printers.
- When printing confidential information in large volumes, staff should not leave the machine unattended.
- Staff must always make sure that the entire document has been printed or copied, and never leave the original documents in the copier.
- If the printer has a fault or paper jam, staff must report it immediately. All issues must be reported to the reprographics department, and they must be notified of any confidential documents stuck inside.

6.16 Environmental monitoring

- All critical infrastructure equipment in a data centre or server room must be always monitored by the IT Team to prevent damage to equipment and minimise disruption.
- The minimum environmental conditions to monitor are:
    - Temperature
    - Humidity
    - Power outages
    - Water
    - Smoke
- Alerts and thresholds must be communicated automatically to the IT director so they can immediately respond to the incident.

7. Communications and operations management

The trust needs to ensure that the correct procedures and processes are in place to secure our people, facilities, and information. There are many processes, procedures, policies, and technical and organisational measures in place to protect the organisation and their information. In this section we try to highlight the most important ones in terms of information security.

7.1 Documentation of operating procedures

- All procedures should be documented.
- Training materials, user manuals, guidelines, best practices, and how-to guides should be shared with the correct audience, organised in one area and always communicated and shared timely.
- All IT systems should be documented appropriately and with detailed information. Taking special care on core and critical systems. All core infrastructure should be documented with all protocols used, component details, locations, specifications, protocols used, versions and maintenance logs.
- All documentation and operating procedures should be up to date and maintained regularly and after a change, as part of the change management process.
- All technical operations and critical systems must include or have:
    - maintenance and/or support contracts, contact information, hours of service, and response times.
    - contact details of the main administrators, supervisors, etc.
    - instructions for handling most common errors, including known issues.
    - procedures or advice for contingency planning.
    - documented administrative processes and procedures.
    - all processes and security must be regularly reviewed.

7.2 Cyber security system and protection

Patch management

Patch management is a key component of securing the IT infrastructure and services to protect the trust and users. Patching is managed by the IT Team for all IT services and systems, but it is also required for Estates team software and equipment.

- Security patches must be applied within 14 days, allowing time for any patch issues to come to light and be mitigated.
- If a critical vulnerability is identified, with a very high risk of affecting Trust information or services, it must be updated as soon as is possible.
- Standard updates and patches are applied on a scheduled basis automatically (normally 30 days from release).
- Zero-day security vulnerabilities that affect critical equipment like servers or core services must be applied immediately. All CVSS (Common Vulnerability Scoring System) scores with High severity or critical must be corrected or remediated as soon as possible.

Security patches might not be able to be applied from time to time for many technical and organisational reasons. For example, if it is incompatible with a piece of software or operating system, conflicting software might be running, there are permissions or security restrictions in place, or if it is blocked by antivirus or firewall software. To ensure that patches are installed securely and effectively, it is crucial to follow established

vendor patch management procedures, including thorough research and analysis of the problem, coordination with relevant software vendors and IT team, and implementing appropriate security measures to protect the system during the patching process

Whitelisting (Shadow IT)

Shadow IT refers to the use of IT-related hardware or software by departments or individuals without the knowledge of the IT Teams. Whitelisting of systems ensures that only systems or services that are approved are allowed access.

- All software, hardware and services used in the Trust must be approved by the change request process unless it is already included in the application whitelist or the trust IT catalogue.
- Due to security reasons and in compliance with GDPR and other standards it is important that all staff understand and comply the change management procedures.
  All equipment introduced into our IT infrastructure can bring a risk to our information and assets and must be fully assessed before access or integration into our IT ecosystems

Malware protection

- Aldridge IT have a trust-wide subscription for Sophos Antimalware products, which are installed on all devices within the trust, to monitor and help prevent infection. These products are kept up to date automatically daily. Additional prevention takes place within the Email and Internet filtering software.
- To further reduce the risks associated with malware, all software installed on the Trust's systems must be licensed and controlled by IT. Security controls are also implemented on the Trust end user devices to prevent the running of certain executable files (without administrator rights) and are also filtered in the various email systems.

Web filtering, content filtering, firewall policies.

- Aldridge use firewalls to protect our systems and provide secure connectivity to the internet. The firewalls provide class leading filtering and protection for education, safeguarding the pupils and staff/admin from threats and unwanted Internet content.
- The content filtering is based on groups, which allow different ranges of access, so 6th form students are not as restricted as the younger students.
- In addition to the filtering system, we have also implemented managed monitoring systems as a safeguarding package which monitor all trust user activities 24/7 and inform the appropriate staff of any safeguarding issues.
- The firewall policies are maintained in a master parent system, and then pushed to the other schools, to keep all sites compliant. Most firewall policies allow outgoing web internet traffic only.
- All internal services needed to be accessed externally must be assessed and be approved by the change management procedures as this increases our exposure to a range of attacks.

Security monitoring

- As part of our security operations the IT teams monitor all systems and services, as well as keep up to date on security information and threats from the Internet. All tasks are managed within in the Information Security programme and are checked and maintained regularly.
- Our security operations include threat prevention, detection, and incident management procedures. Some of this monitoring includes (this is not a complete list):
  - Data lost prevention management and alerts.
  - Hardware and software management and alerts.
  - Automated patch and updates to some systems and components.
  - Log analysis and correlations to servers and critical infrastructure.
  - Antivirus management and alerts
  - Incident response procedures with lessons learned and subsequently improvement to our auditing, compliance, and monitoring.
  - Identify management and risk detention monitoring and alerts.
  - Risk management, auditing, compliance sample checks and improvements.
- Urgent critical security discovered vulnerabilities, workarounds or manual mitigations that prove a risk to the Trust's systems or services are implemented as soon as available and possible.
- The various companies that provide our internet connectivity also provide a monitoring service and several range of security features and tools to protect our systems.

- All IT teams have a responsibility for auditing and monitoring secure threats within our IT systems and software. Our information security programme covers all areas of information security from security design, maintenance, response, compliance, training, and awareness.
- The continual monitoring, measurement and reporting practices must support decision-making and continual security improvement by decreasing the level of risk and uncertainty of our infrastructure and services. All staff will be aware of online safety which includes:
    - the expectations, applicable roles and responsibilities in relation to filtering and monitoring as described in the Aldridge Child Protection and Safeguarding Policy
    - Review the DfE's filtering and monitoring standards
    - Training about filtering and monitoring devices and networks
    - The duty to review the child protection and safeguarding policy, including online safety, annually, and to make sure the procedures and implementation are reviewed regularly

Security baselines for hardware, software, and systems.

- Our hardware, software and systems are maintained to a security baseline and kept up to date according to those baselines. This is mostly through patching, upgrading, hardware upgrades/replacements and keeping everything up to date, but in certain instance, we might implement security hardening for an Internet facing system or internal device or service.
- The baselines are designed and managed as a security conscious organisation to mitigate most risks. The baseline enforces a default security state for our services, core infrastructure, hardware, and software.
- The IT staff must work alongside consultants, technology partners and suppliers to deliver a secure environment that is up to date with the current security controls and features to tackle most security threats in our sector.
- Security baselines must be kept up to date with emerging threats to make the required change to security settings to help mitigate those threats.

Security awareness training

- It is the responsibility of all staff to maintain a good level security awareness. The Trust and the IT team will provide the tools, training, and resources for all schools to keep up to date with different methods, such as:
    - Phishing campaigns
    - Cyber security awareness
    - Fraud and social engineering training

7.3 Change management

- The purpose of change management is to make sure that changes, new purchases, and project are smooth, secure, successfully implemented, and that lasting benefit are achieved by managing the organisational and human aspect of the changes.
- Change management is a key factor in the Trust commitment to mitigate risks, ensure privacy, security by design and default, and adds compliance checking before changes are agreed. Change management improves privacy, security, safeguarding, value for money, and data protection. GDPR also introduced the legal requirement for a DPIA (Data Protection Impact Assessment) which must also be considered.
- Change management, privacy, and data protection must be considered at the start of every project, every change, maintenance, upgrade, new hardware, software, trials, equipment donations, new processes, procedures, policies and throughout the entire systems, devices, and information lifecycle.
- The change management approach must be incorporated into the existing project management and risk management methodology and policies to ensure that:
    - Potential issues are always identified early.
    - Increased awareness of privacy, improve cyber security, and data protection.
    - Legal obligations, standards, and best practices are met, and breaches are minimised.
    - All changes to IT systems, processes and procedures must be in compliant with the requirements and principles set out in UK GDPR and other UK legislation.
- Good communication is key on any successful change process. Staff involved in any change that involves confidential data and process change will need to create the right communication channels, consultation, and dialogue to effectively navigate risks, the risk of fear, frustration that any change may incite.

- All staff should adhere to the best practices and core principles to change management, understand, plan, implement and communicate change.
- All changes must be approved or declined within 2/3 weeks. Most changes should be approved/declined after 3 working days. Most changes and introduction of new software and hardware require contacting different vendor, suppliers and checking for security, provisioning, compatibility, compliance with UK regulations and safeguarding

7.3.1 The process

The change process supports the assessment, prioritisation, authorisation, and scheduling of changes with the Trust. The change management process will need from time-to-time area or subject experts on the different educational, operational, and technical areas with the organisation. These experts might include:

- COO
- DPO / Head of compliance
- CPO
- CGDO
- CEO
- Subject Leads
- CFO
- Director of Estates
- Principals/SLT members.

The Change management process:

- Change requests will be made via the Change request portal on the Aldridge Education Intranet and controlled by the IT Director and Cluster Manager/Senior Technician who will undertake analysis of the impact and cost of the changes at first instance.
- Depending on the nature of the change, detailed assessment and/or plans must be developed for each change request. The Director of IT will seek further information, assistance, advice, and approval depending on the nature of the change request.
- If approved, changes will be scheduled and communicated with the users to ensure minimal disruption to the Staff and Pupils. If not approved, we will communicate alternatives, different ways to achieve the same goals or decline the change.
- System management will ensure any changes to system documentation resulting from the change will be put in place.
- The IT department will lead the process for all changes, like modifications to operating systems, patches occur, but all changes will need to be approved before implementation.

7.3.2 Control of operational software

- All software must have a main administrator. The main administrator most times is the person requesting the software through the change request.
- The IT team will support the main administrator initially with the project implementation, security, user provisioning and DPIA technical paperwork.
- All main administrators must undertake the appropriate training and make sure they take required notes to help them with the new solution.
- All administration and user provisioning for the software is responsibility of the main administrator. IT will assist the main administrator if there are any functions or errors on the system that do not work as expected or require IT involvement.
- IT administrators must liaise with the supplier of the software in order to setup the system in the correct way according to supplier best practices.
- IT will schedule security compliance checks every year to ensure all systems are working as expected and processes and protocols are being followed.

7.3.3 DPIAs

- As part of GDPR, Data Protection Impact Assessments are mandatory where personal data processing it deemed to be 'high risk', or if the DPO requests it.

- It is necessary to conduct a DPIA for any new or existing major processing activity, which encompasses processing of large amounts of personal data.
- All new projects go through a change request process, this process will highlight the need for a DPIA.
- The DPIA must:
    - describe the nature, scope, context, and purposes of the processing.
    - assess necessity, proportionality, and compliance measures.
    - identify and assess risks to individuals; and
    - identify any additional measures to mitigate those risks.
- To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.
- You should consult the Data protection Officer and, where appropriate, individuals and relevant experts. Any processors may also need to assist you.
- If you identify a high risk that you cannot mitigate, you must consult the DPO before starting the processing.
- We always carry out a DPIA if we plan to:
    - use systematic and extensive profiling or automated decision-making to make significant decisions about people.
    - process special-category data or criminal-offence data on a large scale.
    - systematically monitor a publicly accessible place on a large scale.
    - use innovative technology in combination with any of the criteria in the European guidelines.
    - use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity, or benefit.
    - carry out profiling on a large scale.
    - process biometric or genetic data in combination with any of the criteria in the European guidelines.
    - combine, compare, or match data from multiple sources.
    - process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines.
    - process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines.
    - process children's personal data for profiling or automated decision-making or for marketing purposes or offer online services directly to them.
    - process personal data that could result in a risk of physical harm in the event of a security breach.

7.3.4 Encryption, email, files, USB devices, mobile devices, pcs, laptops, media, tapes, DVD, cd.

- Staff should not use external drives but if it is needed staff must not use them to store personal or confidential information and they must be secured using encryption. Please speak to the IT team for advice on current technologies.
- Emails must be sent using encryption when we are trying to send personal or sensitive information.
- Staff should avoid password protecting files like word or excel documents with a password unless they are sending them outside the organisation via email. Staff might forget the password for the encrypted file or leave the organisation in which case we will not be able to access the contents of the file. Instead, other available security measures should be discussed and considered with IT for these situations. If staff need to send an email with the password protected file, the user must create a copy of the file and always leave an unprotected version of the file in the appropriate secure trust filing systems.
- All users must protect sensitive and confidential information during the entire lifecycle of the data. This includes creation, storage, retrieval, usage, and disposal.
  Data in transit can be intercepted, lost, or compromised so data on laptops, USBs, and other mobile devices must be encrypted according to manufactures best practices.

7.4 Risk management

- A risk-based approach is taken to all system, services, and projects. Risk registers for projects are a key part of our plans for risk management and mitigation.

- Our change management process is also designed to mitigate risks on any changes to the software, services, or system within the trust. This provides evidence that all changes have been considered and risks checked or mitigated before being actioned.
- As a trust we have different risk registers for each department area, project, trust-wide, and individual schools.

7.5 Compliance management

We regularly check our IT infrastructure, services, and processes for compliance with all of our policies, UK law and regulations. All these compliance checks are part of our information security programme.

7.5.1 Regular review of all IT systems against this information security policy.

To ensure compliance of systems to the Trust's security standards, regular reviews of the implementation and applicability of the policy will be carried out annually by the IT Team. An annual audit or spot-checks will be carried out in all areas of the trust.

7.5.2 Technical compliance checks.

As part of the Trust's security compliance, regular checks of the technical elements of the IT infrastructure and associated security will be carried out.

7.5.3 Penetration testing, vulnerability testing.

- We use the NCSC and Police Cyber Alarm websites and accompanying services and run several of their solutions to test our external defences and test for vulnerabilities. These are reported to us monthly and enable us to review any issues and mitigate any security risks.
- We monitor security of our SPF, DKIM and DMARC policies and security controls for all our domains.
- We review vulnerabilities discovered in our systems regularly and apply the appropriate and cost-effective measures in line with the information security policy and programme.
- We may also use external Penetration testing websites and dedicated 3rd party companies to perform tests on our perimeter networks, web sites and services.

7.6 Incident Management Procedures

7.6.1 Business continuity and impact analysis

- Business continuity plans are required to keep the trust running during a disaster or outage. The Business Impact analysis help us determine the ways to continue running the trust without all and some services being available.
- Every year we review and analyse our IT core infrastructure and services, servers, switches, MIS, HR and finance software, and other IT and educational systems. Each system is identified and assessed with the relevant department to plan for business continuity. MIS software business continuity plan is a clear example in this area due to their safeguarding impact.
- The impact analysis must be reviewed when we moved or change software, hardware, or system. This will be part of the change request process.
- Analysing the impact uses the standard scoring system used for IT services, we have a list of threats for tabletop scenarios that we review regularly.

7.6.2 Testing and assessment of business continuity plans

- We test our continuity plans during specially during the holiday. Our disaster recovery test allows us to run real disaster recovery of servers and some services. We use these tests to run tabletop scenarios and improvement ideas to build a more robust business continuity plans and disaster recovery procedures.
- Occasional actual outages of services, such as the Cloud MIS system, will allows us to test in a live scenario. Where there is an issue with accessing the cloud MIS system, the schools fall back to a manual system, whist the service is recovered. These outages and switch to manual systems, should all be recorded in the BCP logs for evidence, assessment, and improvements. We report these to the Trust leadership monthly.
- An IT disaster recovery plan is regularly maintained to reduce the amount of time it takes to recover IT services.
- All IT senior staff must know the recovery procedures, incident recovery plan and communication procedures during a disaster scenario.

- Annual disaster recovery training will be provided to the IT team to be confident and skilful during this type of scenario.
- The IT team will conduct several tabletop scenarios annually, such as ransomware attacks, insider threats, virus infection, etc.
- System focussed business continuity planning will be incorporated into wider Trust continuity plans, so that the schools are able to maintain a working environment in the event of an incident.
- Plans should be tested every 6 months to confirm that technical recovery works well.
- Tabletop scenarios should be run, to ensure that all staff understand their specific responsibilities and are aware of the procedure and roles.

7.7 Security principles

- Segregation of duties - Allocation and use of privileges e.g., system administration, will be restricted and controlled. They will be allocated on a 'need to use' or 'event' basis. All system administration users will be required to use multi factor authentication to protect the accounts.
- Least privilege principle - Account privileges will be provided on least principle, providing only the permissions that a user requires to perform their role. Line management will need to provide authorisation confirming the user has a 'need to use or know' the information that they will be provided access to.
- Need to know – User should be assigned only the necessary access to carry on their duties.
- Regular security reviews - Regular reviews of rights must be carried out by IT and check for any changes in roles, that have been missed and remove access to information that they no longer require. HR must provide a change of role notification, which should provide the information to enable IT (or main software administrator) to assign the correct permissions. HR must inform all relevant departments (IT, estates, finance, etc) of any starters, movers, and leavers process immediately.
- System owners - (software main administrators) will regularly review access rights of privileged user accounts every 3 months. Main administrators must follow the correct procedures for securing their software/system.
- All software should have granulated security and staff must seek confirmation during the project to make sure users in the system can be assigned different level of access.
- Job rotation – When a user is the main administrator of a critical software or system, the trust will seek to have rotation of duties and job sharing for a while if needed. This is especially critical for IT core infrastructure systems. This protects against a single point of failure from critical job roles.
- Implicit deny – All system should follow the implicit deny rule and principle. This follow the current network security best practices, making sure that security access is explicitly granted.

7.8 Test, trials, donations, and beta systems

- All test systems, trials and beta systems must be approved before going ahead with suppliers or consultant organisations.
- Donations of IT equipment, software and hardware must be approved via the trust change management process.
- All these systems can bring different risks that will need to be assessed and approved.

7.9 Capacity planning

- Systems are regularly monitored, and performance counters are verified to confirm that all trust systems and services are optimally configured. User identified issues will go through the helpdesk and would be raised as a change request if modifications are required to improve computing or storage capacity.
- New systems are checked and sized against the manufactures or suppliers' specifications. All system must be flexible and elastic, meaning that those services can grow and be reduced if needed easily.
- The IT team will run different tools against the trust systems (such as Dell EMC's Live Optics), these tools can be run to analyse workloads and gain accurate performance benchmarks.

7.10 Backup strategy

- Our backup strategy is based on the 3-2-1 principle. 3 copies of data at any point in time, 2 copies of that data in different storage media and 1 copy on a different site or away from the main server room.

- We use Veeam backup software as our main on-premises backup solution. Although our Google and Microsoft cloud solutions are SLA protected, We also backup our cloud-based systems daily.
- Backups are regularly tested for restoring files and regular test are run for disk-based and tape-based recovery to confirm that the backups are available and useable.
- Where appropriate, shadow copies are setup on the file servers to enable instant recovery

7.11 Logging, auditing, and monitoring

- Infrastructure system event logs are generated and managed internally with the system, and where possible these will be managed centrally:
    - Application logs – the application log contains events logged by programs
    - Security logs – contains security log events, such as valid and invalid logon attempts.
    - System logs – The system log contains events logged by system components, for example, if a driver fails to load during start-up.
    - Firewall logs – The firewall generate logs, some of these are forwarded to specific applications/ security services, to create standard reports.
- Auditing of logs will be carried out as part of the Information Security programme.
- Monitoring of logs and other services will be automated where possible and reviewed on an as required basis unless there is a specific incident.

7.12 Network management

- Segregation of networks to separate logical networks are configured as appropriate by the IT department in the development of infrastructure.
- Network access controls (ACLs) is and must be implemented to further secure the network where possible.
- Network management tools are used to operate our wireless, wired, servers and cloud systems.
- The IT team has been provided with remote management tools to solve most network problems.

7.13 Security of Microsoft 365 and other cloud systems

- Staff sharing calendars, files, folders, etc with staff, external etc.
    - Staff must only share confidential information in a secure way and never with anyone with the link feature.
    - Staff must review access to group, share files and information regularly.
    - All shared files and folder should be sent with an expiration date that is appropriate to the needs of the project or the security principles or least privilege and need to know.
    - All users must be careful when sharing their calendars externally.
    - All staff should seek advice from the IT team when sharing resources and information externally.
- Publicly available systems.
    - All trust sites must be reviewed regularly to comply with this policy and other statutory requirements.
    - All information publicly available must be approved by the marketing and communications department.
    - All main website administrators and contributors must always double check that confidential information is not shared publicly.
    - All sites must be always up to date and all known security vulnerabilities mitigated.
    - All website major changes to redesigns and structural layout should go through the change request process.
    - All websites must use secure protocols, https security, and comply with all current security standards.
- Vendors, suppliers, and design organisations must be compliant with modern security and coding standards.

7.14 Other forms of information exchange

- Fax - There are no fax facilities setup within the trust. Fax communication must not be used to send any confidential information.
- Post:
    - Always check that the address on post is correct.
    - Ensure that only the relevant information is in the envelope.
    - If the information or item is confidential, or contains sensitive data, the most secure method must be used, this could be recorded, special or courier delivery.

- Phones - With phone calls, care should be taken to avoid being overheard when discussing any sensitive personal information.
    - Never disclose passwords or other confidential information in any of the types of information exchange.
    - IT staff will never ask for staff passwords.
- Audio/ video conference calls
    - Audio / video conference calls should be conducted with security and confidentially in mind.
    - If sensitive personal data is being discussed, these should be held in a more secure room, not in an open office.
    - Security login information should not be passed via a call or video call, in case of eavesdroppers.
- Staff should always make sure that their screen is free of any confidential information and that all files are closed or minimised before sharing the screen.
- Bluetooth and NFC technologies
    - Users must disable Bluetooth services by default or when not needed and after use due to the security risks.
    - NFC users must be taking care of several risks with this technology like theft, data tampering, data interception and even get infected with malware. When possible, these technologies should be turned off.

7.15 Supplier management and relationship

- All suppliers must comply with GDPR and other UK legislation and regulations.
- All suppliers working with any Aldridge Education confidential information must follow Cyber Essential certification practices and be certified when appropriate.
- All supplier management practice must include assessment of supplier security, performance, service level agreements in place, quality of delivery, and relationship.
- All staff thinking of entering a new contract with a supplier that might have access to personal, sensitive, or confidential information or need access to our systems, must seek advice from IT first. A change request is needed as we need to comply with UK GDPR, Trust policies and UK regulations and legislation.
- All departments must have an up-to-date supplier management information database for all services, software, and hardware.
- All new suppliers must be evaluated against their capacity and capability to provide the necessary goods and services to the security and operational standards needed by Aldridge Education. We have schools in different parts of the country and a supplier that can provide stable, consistent, nationwide, secure, elastic, and reliable services must be considered through the procurement process.
- All contractors working onsite from any of our suppliers must have Enhanced DBS checks.
- All contractors must be escorted at all times when accessing switch and server rooms.
- All suppliers accessing our IT system remotely must be supervised at all times or have the necessary agreements in place for them to access our confidential or personal information of our staff and students.
- All suppliers holding any trust confidential information should have security certifications like Cyber Essentials plus and ISO 27001.
- All contractors and consultants must provide information on security practices and how they protect our data, IT team and DPO must be consulted before gaining access to our systems and information.
- For security reasons, any information exchange between suppliers or any trust system must be always approved through the change request process.

8. Access controls

8.1 Access management controls (starters, movers, and leavers process)

- All access to information must be controlled securely.
- All staff leaving the organisation must return all equipment, software, keys, and any other organisational equipment.
- All equipment must be returned by the employee to the nearest site to a member of the IT team

8.2 Access management

- In the event that access must be provided to a user account in periods of absence, or when an employee has left the Trust, the access approval must be approved by:
    - Principal if the staff is line managed by the school.
    - Central head of service if the function has a line manager in the central team.
    - CEO/COO if it is a central or special role.
- Under any serious cyber security incident, the Director of IT or Cluster IT manager might have to block, restrict, or gain access to employee's storage areas, emails, and services. These instances are rare, and the IT team will seek out the appropriate notification and approvals. Please refer to the Trust incident response plan for more information.
- Employees must have the information and access necessary to do their job. All systems and software must have segregated, granular and role-based security access.

8.3 Password standards and management

- The password standards for the Trust are detailed below and all academies are subject to these standards. Different standards may apply to Admin, Staff, Teachers and especially Pupils due to varying levels of ability and needs.
- All trust staff members must use 2FA/MFA for all software and systems. Most of the trust systems now use SSO (Single Sign On) for easier access.
- Active Directory - The default Password Policy configured in Group Policy should be:
    - **Minimum** password length 8 characters
    - Password complexity (3 out of the 4 of the following: lower case character, uppercase character, number, or symbol)
    - No Minimum password age set
    - Passwords do not expire
    - No password history
- Active Directory lockout policy - 10 minutes account lockout duration based on 10 failed attempts. Reset lockout after 10 minutes (this is enabled as students will not have access to any sensitive data)
- Software and IT Administrators - Administrators passwords need to be stronger than standard users, as they have access to all of the systems and data. The Administrators password policy should be:
    - Minimum password length 14 characters
    - Password complexity (4 out of the 4 of the following: lower case character, uppercase character, number, or symbol)
    - No Minimum password age set
    - Passwords do not expire

8.4 Network segregation

Network segmentation helps to improve network security by breaking the network into isolated segments. This makes it more difficult for an attacker to move laterally through the network after gaining an initial foothold.

However, there are a number of legitimate data flows that need to be permitted. All data flows across all of the systems on the network should be mapped, including:

- North-bound Traffic: North-bound traffic is leaving the corporate network, like employees visiting Bromcom.com from managed devices connected to the corporate network.
- East-West traffic: East-west traffic moves between systems inside the network perimeter, such as an application and back-end database servers in the data network.

- South-bound Traffic: South-bound traffic includes data entering a network segment or zone, for instance customers or employees accessing a remote desktop service.

The use of access control lists can further control the flow of traffic and must be used for certain vlans.

9. Asset controls

- All information is audited regularly, mapped, and secured into the correct location where change is control through the IT team.

- All information produced by staff must be save into the designated secure locations, these locations provide high levels of confidentially, integrity and availability.
- All our systems are backed up daily.
- The IT department is responsible for monitoring the security of the infrastructure and services to protect all our information assets; therefore, the IT team will regularly check for staff and process compliance to these practices.
- IT staff will keep an updated list of assets.
- All information retention and disposal should follow the trust data retention policy.

9.1 Inventory, information, and software assets

- An information asset register exists as part of our information security programme, operational documents, and system documentation, identifying our data assets, where they are, how they are protected and how they would be recovered in a security incident. It also contains classification and retention periods for the data. Also included in the documentation are data maps and site network information and diagrams, to assist with identification of the data, where it is stored and protected.
- It is important to consider the sensitivity of the data assets within the trust. Assets holding very sensitive data, such as Staff and Pupil information, require additional security controls for compliance with data protection regulations or our information security policy.
- All software must be audited at least once a year.
- All information, procedures and information sharing practices for each department need to be reviewed regularly by managers and it must be checked for compliance against the information security policy from time to time.
- All IT staff must update the assess register weekly and immediately after a new device is purchased, changes location or owner.
- All devices handed over to departments or individuals must be signed for. The trust will provide the necessary paperwork for staff to sign.

All IT hardware assets over the agreed value must be registered, asset tagged and up to date in the trust cloud-based asset management system

10. Incident response

- As part of our IT governance and in order to protect our confidentiality, integrity, and availability of our systems, we have an incident response plan that is updated regularly.
- Our incident response plan includes regular technical tabletop scenarios with IT team members and also leadership tabletop scenarios with our departments leads, finance, marketing and communication, HR, Estates, compliance, governance, education, executive leaders, and technical authority. These scenarios allow us to simulate different incidents and emergency situations and how we will deal with them, actions to be taken and improve our disaster recovery and business continuity processes.
- The IT team must have regular training on different disaster recovery scenarios and practices.
- The incident response plan must be updated every year and reviewed when we incorporate new technologies, software, and new processes.