The Lotus Academy Trust

Supporting children to find opportunities in every difficulty

The Damara School

Specialist SEMH Independent School

Digital Policy

Approved by: Trust Board	
Initial Ratification: March 2026	Review: Sept 2026
Next review due by: Sept 2027	

Contents

1. Introduction and Purpose

This policy sets out the expectations for all staff regarding the acceptable use of technology, internet, devices, and social media. It forms part of our staff behaviour policy (code of conduct) and is essential for safeguarding children, protecting staff, maintaining professional standards, ensuring data security, and protecting the school's reputation.

This digital policy will inform any and all digital activities within the Trust and will be reviewed annually or when:

- a serious safeguarding issue is identified
- the Trust's risk profile changes
- introduction of new technical devices
- introduction of new curriculum software, websites or systems
- curriculum changes
- the Trust changing how it uses technology
- the Trust's monitoring policy or processes changing
- safeguarding guidelines changing

All staff will receive this policy at induction and must sign to confirm they have read and understood it.

2. Scope

This policy applies to:

- All employees (teaching and support staff)
- Volunteers
- Contractors
- Trustees
- Anyone with access to school technology systems

It covers use of:

- School-owned devices (computers, laptops, tablets, phones)
- Personal devices on school premises or for school business
- School network and internet connection
- School email and communication systems
- Social media (personal and professional accounts)

3. Digital Leadership and Governance

3.1 SLT Digital Lead

The current SLT Digital Lead is Sandra Govender, CEO.

Core Responsibilities

Digital Strategy and Planning

The digital lead is responsible for creating and reviewing the Trust's digital strategy, ensuring it considers digital inclusion so everyone in the Trust can benefit and pupils can thrive online. This includes addressing barriers such as access to devices and internet connectivity, digital skills development, staff and pupil confidence, and understanding why using the internet is relevant and helpful. Strategy updates should be provided to SLT and the Trust Board on a termly basis, or sooner if needed.

Online Safety Leadership

The digital lead is responsible for online safety and understands the filtering and monitoring systems in place. This includes:

- Taking a whole-school approach to online safety
- Preparing pupils for online safety risks to help them feel more confident online
- Working closely with the Designated Safeguarding Lead (DSL)

Digital Accessibility and Inclusion

The digital lead ensures devices are accessible for all pupils, including those with visual, hearing or motor difficulties. This includes making sure hardware and software supports the use of accessibility features and that communications are accessible to everyone.

They ensure all pupils, including those with SEND, are able to access the curriculum related to digital skills, IT or computing, and consider how technology can address wider accessibility issues across the whole curriculum.

Supporting Digitally Disadvantaged Pupils

The digital lead will identify and support pupils who don't have digital access at home by providing lunchtime, before and after-school sessions for pupils who don't have access to a device or internet connection.

AI Policy and Safe Use

The digital lead will train staff to be aware of the potential for bias or errors in AI results, particularly relating to minorities and protected characteristics. Staff should correct and overrule AI suggestions if they spot anything that's not right.

Staff Development

The digital lead will support staff as well as pupils, helping staff identify gaps in their own knowledge through skills audits and providing appropriate training and support.

3.2 Succession Planning

Should the SLT digital lead change, leave or is unavailable, another member of staff, who has the right skills, takes over the role. In this event, the Network Lead will take on the role, reporting to

the Deputy Head of School. They will be accountable for the duties listed in this policy and will be given the relevant permissions and access to the relevant files and documents.

3.3 Digital Technology Proposals (DTP)

All DTPs will be taken to SLT by the Digital Lead, for support and challenge, thus ensuring that the digital strategy continues to meet the Trust's educational needs.

3.4 Digital Technology Registers

Information Asset Register

An information asset register (IAR) is a register of all the digital data sources in the Trust. This is kept by the DPO (Data Protection Officer) who is Sandra Govender and reviewed annually.

The DPO will work with the SLT digital lead to identify risks or issues that can be solved by digital equipment, services or contracts.

Digital Risk Management

Our Business Continuity Plan (BCP) details what a digital technology event would have on the Trust and how this is mitigated and what is in place should this happen.

The BCP is tested termly and reviewed annually by SLT.

4. Vision and Strategy

4.1 Digital Technology Vision

At The Lotus Academy Trust, we believe that digital technology is a powerful enabler that will transform learning, enhance operational efficiency, and prepare our pupils for success in an increasingly digital world. Our digital vision is to create an inclusive, safe, and sustainable technology-enhanced environment where every member of our school community can thrive.

4.2 How Digital Technology Will Support Our School Development Plan

Digital technology will be integral to achieving our strategic priorities by:

- **Enhancing teaching and learning**: Providing teachers with innovative tools and resources to deliver engaging, personalised learning experiences that meet the diverse needs of all our pupils
- **Improving assessment and tracking**: Using digital systems to monitor pupil progress more effectively, identify learning gaps quickly, and intervene early to support achievement
- **Strengthening communication**: Creating better channels for engagement with parents, carers, and the wider community through digital platforms
- **Increasing efficiency**: Streamlining administrative processes to reduce staff workload and free up time for what matters most – teaching and supporting our pupils
- **Supporting professional development**: Enabling staff to access high-quality training and collaborate more effectively through digital tools

4.3 Sustainability and Environmental Impact

We are committed to minimising the environmental impact of our digital technology use by:

- **Choosing sustainable hardware**: Prioritising devices with longer lifespans, energy-efficient specifications, and manufacturers with strong environmental credentials
- **Extending device lifecycles**: Implementing robust maintenance and repair programmes to maximise the usable life of our equipment
- **Responsible disposal**: Ensuring old equipment is recycled or refurbished through certified schemes rather than sent to landfill
- **Reducing paper consumption**: Using digital alternatives where appropriate to reduce our reliance on printed materials
- **Energy efficiency**: Configuring devices to use power-saving modes and ensuring equipment is switched off when not in use
- **Cloud-based solutions**: Utilising cloud services to reduce the need for energy-intensive on-site servers
- **Teaching sustainability**: Educating pupils about the environmental impact of technology and encouraging responsible digital citizenship

4.4 Meeting Pupil and Staff Needs

For Our Pupils

Digital technology will support our pupils by:

- **Ensuring accessibility**: Making sure hardware and software supports the use of accessibility features for pupils with visual, hearing or motor difficulties, and that communications are accessible to everyone
- **Providing inclusive access**: Ensuring pupils with SEND are able to take advantage of the same opportunities as other pupils, using technology to address wider accessibility issues across the whole curriculum
- **Supporting digital inclusion**: Addressing barriers to access by providing support for pupils who may not have devices or internet connectivity at home
- **Developing digital skills**: Embedding age-appropriate digital literacy and online safety across the curriculum so pupils can navigate the digital world confidently and safely
- **Personalising learning**: Using adaptive technologies and platforms that respond to individual learning needs and enable pupils to progress at their own pace
- **Preparing for the future**: Equipping pupils with the digital skills and competencies they need for their next phase of education, training, or employment

For Our Staff

Digital technology will support our staff by:

- **Reducing workload**: Implementing efficient systems that automate routine tasks and streamline administrative processes
- **Enhancing professional learning**: Using IT and computing skills audits to help staff identify gaps in their own knowledge and providing targeted training and support

- **Enabling collaboration**: Providing platforms for staff to share resources, plan together, and learn from each other's practice
- **Supporting wellbeing**: Ensuring technology enhances rather than burdens staff, with appropriate training and ongoing support
- **Improving communication**: Creating effective channels for staff to communicate with leadership, colleagues, parents, and external partners

4.5 Making It Happen

This vision will be realised through:

- **Clear leadership and governance**: With designated roles and responsibilities for digital strategy at all levels
- **Stakeholder engagement**: Involving staff, pupils, parents, Trustees, and trust leaders in shaping and implementing our digital strategy
- **Regular review and evaluation**: Monitoring progress against our vision and adapting our approach based on evidence of impact
- **Adequate resourcing**: Ensuring appropriate investment in infrastructure, devices, software, and professional development
- **Collaboration and partnership**: Working with our trust, other schools, and external partners to share learning and achieve our goals

4.6 Digital Technology Strategy

Direction and Focus

The Trust's vision will guide our digital technology strategy through the following strategic priorities:

1. Infrastructure and Systems

- Ensure robust, reliable, and secure IT infrastructure that supports teaching, learning, and administration
- Annually review the effectiveness of filtering and monitoring systems that block harmful and inappropriate content without unreasonably impacting teaching and learning
- Maintain systems that protect data and ensure compliance with GDPR and other statutory requirements

2. Teaching and Learning

- Integrate digital technology purposefully into curriculum planning and delivery
- Provide teachers with the tools, training, and confidence to use technology effectively
- Develop pupils' digital literacy and computational thinking skills progressively across all phases

3. Online Safety and Digital Wellbeing

- Take a whole-school approach to online safety, ensuring pupils understand risks and know how to keep themselves safe online

- Protect and educate pupils and staff in their use of technology, establishing mechanisms to identify, intervene in, and escalate concerns, addressing the four areas of risk: content, contact, conduct, and commerce
- Promote healthy relationships with technology and support positive digital citizenship

4. Inclusion and Accessibility

- Remove barriers to digital inclusion by ensuring everyone has access to devices, connectivity, skills, confidence, and motivation to use technology effectively
- Use technology to support pupils with additional needs and remove barriers to learning
- When using AI tools, train staff to be aware of potential bias or errors, particularly relating to minorities and protected characteristics

5. Professional Development

- Build staff capacity through high-quality, evidence-informed training
- Create a culture of continuous improvement where staff feel confident to experiment and innovate
- Share expertise within our school and across the trust

6. Sustainability and Value

- Make environmentally responsible choices in procurement and use of technology
- Ensure value for money through strategic planning and collaboration
- Monitor and evaluate the impact of technology investments on outcomes

The digital lead will ensure that both the Vision and Strategy are shared with all stakeholders. The digital lead will ensure that the strategy is actioned by the relevant people and reviewed annually.

SLT will:

- support the SLT digital lead to create the digital technology vision
- agree and approve the digital technology strategy
- agree budgets and funding
- ask for progress updates from the SLT digital lead at SLT meetings

Trustees will:

- ask SLT to show how the digital technology strategy meets the school's teaching, learning and administration needs
- challenge any decisions about digital technology that may not show how they meet school's needs or learning outcomes
- obtain assurance that the digital strategy complies with all relevant legislation or statutory guidance, including keeping children safe in education (KCSIE), and data protection laws
- ask for progress updates from the Deputy Head of School at Trustee meetings

5. Roles and Responsibilities

5.1 The CEO/Deputy Headteacher (SLT Digital Lead)

The CEO is the DPO (Data Protection Officer), First Level Cyber Response Monitor and SLT Digital Lead responsible for creating and reviewing the Trust's digital strategy, online safety leadership, understanding the filtering and monitoring systems in place, and taking a whole-school approach to online safety.

Contact: Sandra Govender, CEO - ceo@lotustrust.org.uk

5.2 The Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for online safety in school, supporting the leadership team in ensuring that staff understand this policy, working with staff to address any online safety issues or incidents, ensuring that any online safety incidents are logged and dealt with appropriately, updating and delivering staff training on online safety, and liaising with other agencies if necessary.

Contact: DSL and First Level Cyber Response Monitor: Julie Cox - Deputy Head - jcox@lotustrust.org.uk. Alternate Designated Safeguarding Lead and First Level Cyber Response Monitor: Sandra Govender – ceo@lotustrust.org.uk

5.3 Network Administrator

The Network Administrator is responsible for putting in place appropriate filtering and monitoring systems, ensuring that the school's ICT systems are secure and protected against viruses and malware, conducting security checks and monitoring the school's ICT systems, blocking access to potentially dangerous sites, and ensuring that any online safety incidents are logged and dealt with appropriately.

Contact: Network Administrator and First Level Cyber Response Monitor: Samantha Burgoyne- ict@lotustrust.org.uk

5.4 All Staff

All staff are responsible for maintaining an understanding of this policy, implementing this policy consistently, agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately, and understanding their expectations, roles and responsibilities around filtering and monitoring systems.

6. General Principles

Staff must:

- Use technology responsibly and professionally
- Protect children from harmful content and contact
- Maintain confidentiality and data protection standards
- Report any concerns or security breaches immediately
- Understand that school systems may be monitored for safeguarding purposes

Staff must not:

- Use school systems for any illegal activity
- Access, create, store, or distribute inappropriate material
- Compromise the school's security systems
- Breach professional boundaries with pupils Digital policy2

7. Use of School Devices and Networks

7.1 Acceptable Use

School devices are primarily for educational and professional purposes. Limited personal use is permitted during breaks provided it does not interfere with work duties, breach any other aspect of this policy, or consume excessive bandwidth or resources.

7.2 Security Requirements

Staff must:

- Keep passwords secure and confidential
- Never share login credentials
- Lock devices when unattended
- Report lost or stolen devices immediately
- Only install approved software
- Keep devices updated with security patches
- Use encryption when storing sensitive data

Passwords must be at least 10 characters long, containing letters and numbers. Staff must create a unique password that has not been used on other sites.

7.3 Taking Devices Off-Site

Staff must:

- Ensure that work devices are secure and password-protected when using them outside school
- Keep all data securely stored
- Keep portable electronic devices under lock and key when not in use
- Not leave devices on office and classroom desks, on staffroom tables, or anywhere else where there is general access
- Always log out of systems and lock equipment when not in use
- Log out of and close down equipment and systems completely at the end of each working day
- Use encryption software to protect portable devices and removable media, such as external hard drives and USB devices
- Follow the same security procedures at home or outside the school as in school

8. Internet and Email Usage

8.1 Internet Access

Staff may use the internet for:

- Educational research and resources
- Professional development
- School administration
- Reasonable personal use during breaks (as per section 7.1)

Staff must not:

- Access inappropriate websites (including pornography, gambling, extremist content, or illegal material)
- Attempt to bypass filtering or monitoring systems
- Download unauthorised software or files
- Stream video/audio content excessively (except for educational purposes)
- Use peer-to-peer file sharing

Should any content necessary for you to complete your work be blocked or reported, please ensure you contact IT support – ict@thelotustrust.org.uk – to advise what URL you need access to and a reason why.

8.2 Email Usage

The school provides each member of staff with an email address. This email account should be used for work purposes only. All work-related business should be conducted using the email address the school has provided.

Staff must:

- Use school email for all work-related communications
- Not share their personal email addresses with parents/carers and pupils
- Not send any work-related materials using their personal email account
- Take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract
- Take extra care when sending sensitive or confidential information by email
- Encrypt any attachments containing sensitive or confidential information

9. Mobile Phones and Personal Devices

9.1 Staff Mobile Phones

Staff are allowed to bring their personal phones to school for their own use but will limit such use to non-contact time when pupils are not present.

Staff must:

- Keep personal phones in their bags or cupboards during contact time with pupils
- Not take pictures or recordings of pupils on their personal phones or cameras
- Not give their personal phone number(s) to parents/carers or pupils
- Use phones provided by the school to conduct all work-related business

School phones must not be used for personal matters.

9.2 Personal Devices on School Network

Any personal devices using the school's network must:

- Have software updates, security updates and anti-virus products installed
- Be configured to perform such updates regularly or automatically

10. Social Media and Online Communications

10.1 Professional Boundaries

When drafting the staff behaviour policy, schools should bear in mind the offence under section 16 of The Sexual Offences Act 2003, which provides that it is an offence for a person aged 18 or over to have a sexual relationship with a child under 18 where that person is in a position of trust in respect of that child, even if the relationship is consensual.

Staff must not:

- Use personal accounts to conduct school business
- Accept 'friend requests' from or communicate with pupils past or present
- Complain about the school, individual pupils, colleagues or parents/carers
- Reference or share information about individual pupils, colleagues or parents/carers
- Post images of pupils
- Express personal views or opinions that could be interpreted as those of the school
- Link their social media profile to their work email account

10.2 Personal Social Media Accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

Staff should:

- Set privacy settings to maximum on personal accounts

- Be mindful that online activity may be visible to pupils, parents, and colleagues
- Avoid posting content that could bring the school into disrepute
- Never discuss pupils, parents, colleagues, or school business on social media
- Not identify themselves as working at the school in a way that could compromise professionalism

10.3 School Social Media Accounts

The school's official social media channels are managed by Sandra Govender, CEO. Staff members who have not been authorised to manage, or post to, the accounts, must not access, or attempt to access, these accounts.

11. Photography and Video

Staff must:

- Only use school-approved devices for photographing/filming pupils
- Obtain appropriate consent before taking images
- Store images securely on school systems only
- Delete images when no longer needed
- Follow the school's image use policy

Staff must not:

- Use personal devices to photograph or film pupils (except in exceptional circumstances with SLT approval)
- Share images of pupils on personal social media
- Store images of pupils on personal devices or cloud storage

12. Data Protection and Confidentiality

Staff must:

- Comply with GDPR and the Data Protection Act 2018
- Only access pupil/staff data necessary for their role
- Keep sensitive information secure (encrypted if electronic, locked if paper)
- Only share information with those who have a legitimate need to know
- Report data breaches immediately
- Ensure confidential conversations cannot be overheard
- Dispose of confidential information securely

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

13. Filtering and Monitoring

To keep staff and pupils safe online, the Trust have systems in place to filter and monitor usage. Any concerns will be treated as a safeguarding issue and dealt with under the Child Protection and Safeguarding Policy.

Governing bodies and proprietors should ensure their school has appropriate filtering and monitoring systems in place and regularly review their effectiveness. The appropriateness of any filtering and monitoring systems are a matter for individual schools and will be informed in part by the risk assessment required by the Prevent Duty.

Schools should:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems
- Review filtering and monitoring provision at least annually
- Block harmful and inappropriate content without unreasonably impacting teaching and learning
- Have effective monitoring strategies in place that meet their safeguarding needs

The Trust has implemented filtering and monitoring systems that block harmful and inappropriate content, have effective monitoring strategies, and are reviewed at least annually. Our monitoring system alerts the DSL to potential safeguarding concerns. Given our SEMH specialism, monitoring takes account of the particular vulnerabilities of our pupils.

13.1 Filtering Strategy

A well-maintained and effective filtering system is essential for ensuring students can learn in a safe online environment.

The Trust uses filtering software, which is assigned to users rather than devices and alerts users when signing in to a device that they are being monitored. This means that no matter what device is used (e.g. user's own device - BYOD), the filtering applies.

Our current filtering system is TrustLayer by USS. Inappropriate content and sites are blocked, according to user group and a comprehensive filtering list. USS are a member of IWF and CTIRU, with regularly updated block lists. To aid with teaching and learning, users can request to unblock a site if they deem it necessary, which is then reviewed by the Network Administrator.

The monitoring software creates weekly reports, which are sent to the Digital Lead and the Network Administrator. The Digital Lead shares these with SLT at least half termly to identify any patterns present.

In school, a combination of technical and in-person monitoring is used to check online activity, using the 4 areas of risk from KCSIE – content, contact, conduct, commerce.

13.2 Monitoring Strategy

Monitoring user activity on Trust devices is an important part of providing a safe environment for students and staff. Unlike filtering, it does not stop users from accessing inappropriate or illegal material through internet searches or software.

The Trust uses monitoring software, which is assigned to users rather than devices and alerts users when signing in to a device that they are being monitored. This means that no matter what

device is used (e.g. user's own device - BYOD), the monitoring system will highlight any concerns and email alerts directly to the Network Administrator and Digital Lead.

The benefits of using software are:

- Monitoring all devices/users at the same time
- Tracking all activity on a specific device, not just online
- Monitoring content that's difficult to filter, such as AI-generated content
- Tracking activity out of school hours
- Monitoring activity in unsupervised locations, for example, home or the library
- Providing alerts if concerning activity is identified
- Identifying the device or user that caused an alert
- Showing patterns of behaviour over time, highlighting risks or potential safeguarding issues

The software is called classroom. Cloud by NetSupport which monitors the online safety keywords and phrases the user types. The Trust can gain insight into any trending issues, as well as identify individual users who are engaged in concerning activity. The keyword monitoring tool is powered by a pre-supplied online safety database of keywords and phrases, containing over 20,000 terms. The database covers a wide range of topics from self-harm, gambling, bullying, and racism – to risks of radicalization, drugs, sexual exploitation, and more.

All alerts are reviewed immediately and filtered by the Network Administrator for false positives – the Network Administrator receives the same annual safeguarding training that all staff undertake. All concerns requiring further investigation will be sent to the DSL for action and recorded appropriately.

The monitoring software creates weekly reports, which are sent to the Digital Lead and the Network Administrator. The Digital Lead shares these with SLT at least half termly to identify any patterns present.

The Network Administrator creates a termly report for the Safeguarding Trustee, which are reviewed during Monitoring visits. At least half termly the Network Administrator will test that the software is working correctly.

In school, a combination of technical and in-person monitoring is used to check online activity, using the 4 areas of risk from KCSIE – content, contact, conduct, commerce.

13.3 Staff Awareness

Staff should be aware that:

- The school has filtering systems to block inappropriate content
- Internet use on school networks is monitored for safeguarding purposes
- Monitoring may include websites visited, emails sent/received, and search terms
- Attempts to bypass filtering will be logged and investigated
- The school may review internet/email usage if there are concerns

14. Online Safety and Safeguarding

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school to protect and educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **Content**: being exposed to illegal, inappropriate, or harmful content
- **Contact**: being subjected to harmful online interaction with other users
- **Conduct**: online behaviour that increases the likelihood of, or causes, harm
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and financial scams

Staff must:

- Report any online safety concerns immediately to the Designated Safeguarding Lead
- Be vigilant for signs that pupils are being exposed to harmful content online
- Understand the four categories of online risk: content, contact, conduct, and commerce
- Follow the school's safeguarding procedures if a pupil discloses online abuse
- Participate in online safety training

If staff encounter inappropriate material:

- Do not forward, share, or save it
- Report immediately to the Designated Safeguarding Lead
- Follow guidance on preserving evidence if required

If a pupil informs staff that they have found any material which might upset, distress or harm them or others, staff will let the designated safeguarding lead (DSL) and ICT manager know immediately and will also do so if they encounter any such material.

15. Remote/Home Working

When working remotely, staff must:

- Ensure a secure internet connection (avoid public Wi-Fi for sensitive work)
- Keep devices secure and out of sight of others
- Ensure confidential conversations cannot be overheard
- Lock devices when not in use
- Follow the school's remote learning safeguarding guidance
- Ensure appropriate backgrounds for video calls
- Dress professionally for video calls with pupils or parents

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site.

Communication must always occur via official school channels, and not through personal accounts or other websites. Permitted methods are:

- Email using school email addresses only
- Microsoft Teams
- Google Classroom

All communication should take place during usual office hours, with no expectation for colleagues to read or respond to emails after 4pm.

16. Physical Security

All laptops, tablets and mobile devices must be secured when not in use.

Staff must:

- Not leave devices unattended in vehicles or public places
- Not leave equipment unsupervised in unsecured areas
- Report lost or stolen devices immediately to the Network Administrator and CEO
- Ensure server rooms and areas containing IT equipment are kept locked

Access to server rooms is restricted to authorised personnel only.

If equipment is damaged, lost or stolen, staff will immediately inform CEO, Mrs S Govender.

17. Backup and Security Measures

Critical data is backed up daily. Backups are stored securely in the cloud and are encrypted. Backup restoration is tested termly to ensure data can be recovered.

All users should set strong passwords for their accounts and keep these passwords secure. All the school's ICT devices that support software updates, security updates and anti-virus products will have these installed and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

18. Broadband Internet and Network Infrastructure

18.1 Broadband Connection

The Trust has full fibre broadband installed, and the contract is reviewed annually as part of the Digital Strategy.

Our connection delivers a minimum of 700mbps download speed.

18.2 Backup Broadband

We have a mobile data broadband as a backup which has an automatic failover should the main broadband line be interrupted, preventing disruption and data loss.

The automatic failover is protected by the same Monitoring and Filtering standards as the main connection.

18.3 Network Cabling

Our cabling is category 6A, as specified in the DfE Standards.

We will use this as a minimum standard when looking at:

- New buildings
- Building changes
- New systems

Where possible, we use the Wi-Fi network instead of cabling, ensuring flexibility in the use of technology in teaching and learning, as well as administration.

18.4 Network Switching

Details of our Network switching is detailed in Appendix F.

Our network switches are managed by the Network Administrator with support from Netcentral. They are responsible for:

- Understanding the network
- Keeping network switch software and firmware updated
- Monitoring and documenting patching schedules
- Making sure equipment remains in warranty and having plans for when it nears end of life
- Putting a refresh plan in action
- Making sure any additions or changes to the network meet the networking switching standards
- Monitoring and addressing faults as they happen
- Updating the network documentation on setup and operation when there are network changes
- Reporting any changes to the Digital Lead
- Ensuring UPS is functioning

To ensure continuity of service for teaching and learning and administration, a document for all Digital Lead and Network Administrator roles and responsibilities and associated file links is available to SLT and kept in an electronic file with this policy.

18.5 Wireless Network

Our school's wireless network uses Wi-Fi 6E and is enterprise grade. The Network Administrator will:

- Review the network interface speeds of Wi-Fi access points
- Configure the wireless network to support network segregation and Quality of Service (QoS)
- Understand the wireless network

- Keep wi-fi software and firmware updated
- Monitor and document patching schedules
- Make sure equipment remains in warranty and have plans for when it nears end of life
- Put a refresh plan in action
- Monitor and address faults as they happen
- Update the network documentation on setup and operation when there are network changes
- Report any changes to the Digital Lead

The security of the wireless network is absolute. All regular users are given access to the school Wi-Fi once they have signed the acceptable use policy and must use MFA (multi factor authentication). Guests are given access to the free guest Wi-Fi, issued by our supplier.

18.6 Wireless Access Points

All buildings will be supplied with sufficient WAPs to ensure a consistent and secure signal across the site.

Any administrative accounts that have additional access permissions are secure and fully documented to prevent unauthorised access.

19. Cyber Security

19.1 Roles and Responsibilities

SLT Digital Lead's Core Responsibilities

The current SLT Digital Lead is Sandra Govender, CEO.

Responsibilities include:

- Cyber risk assessment, including termly review
- Cyber awareness plan, including annual review
- Provide annual cyber security training to staff, pupils, and trustees
- Oversee IT Support

IT Support Responsibilities

IT support are responsible for:

Technical Security:

- Check firewall every term
- Review anti-malware every term
- Review user accounts and permissions every term
- Review password policy every year
- Review multi-factor authentication (MFA) every year
- Record end of support dates on asset register

- Keep an up-to-date data backup and recovery plan and test it every year
- Follow the 3-2-1 backup plan
- Set up a firewall
- Configure firewall to the school's needs
- Create a policy for external devices
- Secure data and devices with anti-malware
- Set user permissions
- Set up a password policy and make sure systems meet it
- Use multi-factor authentication (MFA)
- Keep digital technology software licences record updated
- Keep software and hardware supported and up to date
- Perform security updates at the right time

19.2 Cyber Risk Assessment

The Trust will review the Cyber Risk Assessment (CRA) termly, or more often if:

- There are significant technology or process changes, or
- If an incident or attack affects the Trust

The CRA multi-disciplinary team:

- Digital Lead
- Network Administrator
- Data Protection Officer
- Deputy Head of School
- Finance
- Trustee for Technology

The Trust's CRA is included in the Strategic and Reputational Risk Register.

19.3 Cyber Awareness Plan

The following is how the Trust plans to raise awareness. This will be reviewed annually or more often if:

- There are significant technology or process changes, or
- If an incident or attack affects the Trust

The Cyber Awareness Plan multi-disciplinary team:

- Digital Lead
- Network Administrator

- Data Protection Officer
- Deputy Head of School

Understand What Cyber Risks There Are

Ensure that staff, pupils, parents and Trustees understand that risks can come from outside the Trust, such as deliberate attacks to your systems, theft or natural disasters, or from inside, for example, from Trustees, staff or pupils.

Threats could be malicious, such as pupils gaining unauthorised access to digital technology systems, or unintentional, such as plugging infected devices into computers on the school network.

This will be achieved through:

- Annual cyber security training
- Policies
- CPD
- Curriculum
- Newsletters

Create Awareness of Cyber Risks

Everyone using the Trust's digital technology should be aware of cyber risks and take steps to minimise them. Make sure they:

- Use secure passwords
- Avoid working in public places
- Sign out of their account when leaving their computer
- Check emails they receive are legitimate
- Do not use external devices, unless approved by the Trust and encrypted

This will be achieved through:

- Annual cyber security training
- Policies
- CPD
- Curriculum

Encourage Responsible Behaviour

Encourage and promote good practice among staff and pupils, for example:

- Staying vigilant for cyber risks
- Promoting a no-blame culture when reporting a suspected cyber incident
- Following the cyber response process when reporting incidents

This will be achieved through:

- Annual cyber security training
- Policies
- CPD
- Curriculum

Training

The Trust staff complete The National Cyber Security Centre (NCSC) cyber security training for school staff at the start of each academic year. Updates are communicated through email when needed.

19.4 Reporting Incidents or Data Breaches

Cyber incidents are reported as soon as possible to the Digital Lead – ceo@lotustrust.org.uk and ict@lotustrust.org.uk or in person to the Digital Lead and Network Administrator for immediate investigation.

All staff must report any security breach, suspicious activity, or mistake made that may cause a cyber security breach, to Network Administrator/CEO as soon as practicable from the time of the discovery or occurrence.

Investigation Process:

1. The Network Administrator will undertake the initial investigation and remediation needed, which should include:
    - Ensuring systems are safe and secure
    - Information about the suspected cyber incident or attack
    - Which systems are affected
    - How many users are affected
    - When the cyber incident or attack was first noticed and what the user did, if anything, before reporting the incident
    - Recommended remediation, i.e. suspension of user
2. The Network Administrator will report to the Digital Lead, who will review and involve the relevant staff members, i.e. DPO or DSL
3. Dependant on the level of attack, the Digital Lead will approve and remediation will be undertaken by the Network Administrator
4. External reporting completed, dependent on risk

19.5 Cyber Incidents and Attacks – Response Plan

Our cyber incident response plan can be found within the Trust's Business Continuity Plan (BCP). This is reviewed annually by a multi-disciplinary team from within the Trust.

20. Third-Party Suppliers and Cloud Services

Before engaging any third-party supplier who will access Trust systems or data, the Network Administrator must assess their cybersecurity measures.

Requirements:

- Suppliers must demonstrate appropriate security certifications
- All cloud services used by the Trust must be approved by the CEO
- Cloud providers must demonstrate UK GDPR compliance
- Data stored in the cloud must be encrypted

21. Use of AI Tools

This policy is based on the DfE's policy paper on generative artificial intelligence (AI) in education and guidance on AI product safety expectations. The Trust recognises that AI tools can support teaching, learning, and school operations when used safely and responsibly. The following sets out our approach to using AI across our school community and will be reviewed annually, and as technology changes.

21.1 Our Commitment

We will take a safe and responsible approach to AI, ensuring the benefits of using AI are always greater than the risks involved. We are committed to protecting pupils, staff, and school data whilst harnessing the potential of AI to enhance education and reduce workload.

The Digital Lead will oversee AI within the Trust. Their responsibilities include:

- Liaising with our data protection officer (DPO) and designated safeguarding lead (DSL)
- Seeking technical advice when necessary
- Making sure staff are appropriately trained to use AI
- Monitoring and reviewing

21.2 Risk Assessment

Before introducing any AI tool, we will assess whether it is suitable for our school. The risks will vary depending on:

- The type of AI tool
- Who is using it (staff or pupils)
- The age of our pupils

We will only use AI tools where the benefits are greater than the risks involved. We will complete a risk assessment for every AI tool we use, any new AI tool we might want to use in the future, and any tool that has had a significant update.

21.3 Approved AI Tools

We maintain a list of approved AI tools which includes both approved tools and approved uses of those tools. Staff and pupils should only use the tools included in the list for the specific purposes

set out in the list. This list is available on the Pupil and Staff Noticeboards and is regularly updated by our Digital Lead.

21.4 Data Protection and Privacy

Personal data must not be used in generative AI tools unless strictly necessary.

Staff must not:

- Write anything that contains pupils' names
- Enter sensitive data to help plan a safeguarding report
- Use pictures of pupils as part of a prompt for image-generating AI tools

If staff are unsure whether it's necessary to add personal data into an AI tool, they should check with the DPO or the Digital Lead.

If we intend to process personal data using AI, we will complete a data protection impact assessment (DPIA) first. Any AI product we use to process personal data must have a robust approach to data handling and be transparent about how the data is processed.

21.5 Safeguarding

We understand and appropriately handle the safeguarding risks associated with AI. We will do all we reasonably can to make sure that our filtering and monitoring practices prevent users from accessing harmful or inappropriate content when using AI.

All staff have been trained on the safeguarding risks of AI and understand how to recognise and handle inappropriate use of AI by pupils.

21.6 Staff Use of AI

Staff must know how to spot and correct errors or bias in AI outputs.

Staff may use approved AI tools to support their work, such as:

- Creating resources and materials
- Administrative tasks
- Planning and preparation

Staff must use AI tools as a starting point and always check and adapt the results, so they are:

- Taking the best interests of staff, pupils and the school into account
- In line with our school policies

The digital lead will train staff to be aware of the potential for bias or errors in AI results, particularly relating to minorities and protected characteristics. Staff should correct and overrule AI suggestions if they spot anything that's not right.

21.7 Pupil Use of AI

Pupils must know that using AI without crediting it isn't allowed in exams, coursework or any work that's internally assessed to count towards a qualification. We will have open dialogue with pupils about how and when AI tools can be used to support learning, and when they shouldn't be.

Pupils may use AI tools and generative chatbots as a research tool to help them find out about new topics and ideas when directed to do so, and when specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed.

If pupils use AI tools, we have appropriate filtering and monitoring in place, adjusted based on different levels of risk, age, appropriateness and the user's need.

21.8 Intellectual Property

We must have consent from pupils or staff (unless an exception to copyright applies) to enter their intellectual property into any AI tool that will store or collect this information for commercial purposes. If pupils are too young to give consent, we will get permission from their parents/carers.

21.9 Training

Staff receive training on the safe use of AI, including:

- Understanding AI in education
- Interacting with generative AI
- Safe use of generative AI
- Use cases of generative AI in education

22. Reporting Concerns

Staff must report any concerns or incidents immediately using the following procedures:

22.1 Safeguarding Concerns

Any staff member who has any concerns about a child's welfare should follow the processes set out in the child protection policy. Staff should expect to support social workers and other agencies following any referral. The designated safeguarding lead (and any deputies) are most likely to have a complete safeguarding picture and be the most appropriate person to advise on the response to safeguarding concerns.

If a pupil informs staff that they have found any material which might upset, distress or harm them or others, staff will let the designated safeguarding lead (DSL) and ICT manager know immediately, and will also do so if they encounter any such material.

Contact: Julie Cox, Deputy Head - jcox@lotustrust.org.uk

22.2 Cybersecurity Incidents

Cyber incidents are reported as soon as possible to:

- Digital Lead – ceo@lotustrust.org.uk
- IT Support – ict@lotustrust.org.uk
- Or in person to the Digital Lead and Network Administrator for immediate investigation

The investigation process includes:

1. The Network Administrator will undertake the initial investigation and remediation needed, which should include:

- Ensuring systems are safe and secure
- Information about the suspected cyber incident or attack
- Which systems are affected
- How many users are affected
- When the cyber incident or attack was first noticed and what the user did, if anything, before reporting the incident
- Recommended remediation

2. The Network Administrator will report to the Digital Lead, who will review and involve the relevant staff members, i.e. DPO or DSL
3. Dependant on the level of attack, the Digital Lead will approve and remediation will be undertaken by the Network Administrator, with external reporting completed, dependent on risk

22.3 Data Breaches

If staff send an email in error that contains the personal information of another person, they must inform the Network Administrator immediately and follow our data breach policy (19.4 in this document).

Staff must report data breaches immediately to the Data Protection Officer/CEO.

Contact: ceo@lotustrust.org.uk

22.4 Online Safety Incidents

Staff must report the following immediately:

To IT Support (ict@lotustrust.org.uk):

- Lost or stolen devices
- Suspected malware or viruses
- Phishing emails or suspicious communications
- Technical issues with filtering/security

To the Designated Safeguarding Lead (jcox@lotustrust.org.uk):

- Any online safety concerns about a pupil
- Inappropriate content accessed by pupils
- Concerns about staff conduct online
- Safeguarding disclosures made online

To the CEO/Deputy Headteacher (ceo@lotustrust.org.uk):

- Serious breaches of this policy
- Concerns about data breaches
- Allegations against staff

22.5 Security Breaches

All staff must report any security breach, suspicious activity, or mistake made that may cause a cyber security breach, to Network Administrator/CEO as soon as practicable from the time of the discovery or occurrence.

23. Consequences of Misuse

Breaches of this policy will be taken seriously and may result in disciplinary action.

23.1 Minor Breaches

Minor breaches may result in:

- Verbal/written warning
- Additional training
- Temporary restriction of access to systems

23.2 Serious Breaches

If staff engage in unacceptable use, they may be liable to disciplinary action. Unacceptable use includes:

- Accessing, creating, storing or linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Sharing confidential information about the school, its pupils, or other members of the school community
- Setting up any software, applications or web services on this device without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Carrying out any activity which defames or disparages the school, or risks bringing the school into disrepute
- Using inappropriate or offensive language

Serious breaches may result in:

- Formal disciplinary action in line with the staff disciplinary procedures
- Suspension of access to systems
- Dismissal (potentially gross misconduct)
- Referral to police (if illegal activity)
- Referral to Teaching Regulation Agency (for teachers)
- Referral to Disclosure and Barring Service (if safeguarding concern)

If staff engage in any activity that constitutes 'unacceptable use', they may face disciplinary action in line with the school's policies on staff discipline and staff code of conduct.

Examples of serious breaches include:

- Accessing, creating, or distributing illegal or inappropriate material

- Inappropriate contact with pupils online
- Breaching professional boundaries
- Deliberate attempts to bypass security
- Serious data breaches
- Using school systems for personal financial gain

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

23.3 Illegal Activity

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

24. Training and Support

24.1 Induction Training

All staff should receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction. The training should be regularly updated. Copies of policies and a copy of Part one (or Annex A, if appropriate) of Keeping Children Safe in Education should be provided to all staff at induction.

All staff will receive cybersecurity training as follows:

Induction Training (for all new staff) includes:

- Overview of cyber threats and the Trust's security measures
- How to create and manage strong passwords
- How to recognise phishing emails and suspicious activity
- Acceptable use of Trust IT systems
- Reporting procedures for security concerns
- Responsibilities under this policy

Induction training is mandatory and must be completed within 1 month of starting. This includes:

- Confirmation of reading this policy
- Completion of NCSC Cyber Security Training For School Staff training module via Smartlog

24.2 Annual Refresher Training

In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.

All staff must complete annual cybersecurity refresher training. Training covers:

- Updates to threats, policies and procedures
- Practical examples and scenarios

Completion is recorded and monitored.

Staff receive training on the safe use of AI, including:

- Understanding AI in education
- Interacting with generative AI
- Safe use of generative AI
- Use cases of generative AI in education

24.3 Additional Training

Additional training is provided when:

- Significant new threats emerge
- Following any security incident affecting the Trust
- There

are changes to legislation or policy

- For specific roles (e.g., DSL receives additional training on monitoring alerts)

24.4 Training Records

The School Business Manager maintains records of all cybersecurity training. Training completion is reported annually to the Trust Board. Non-completion is followed up and may result in system access being suspended.

24.5 Support Available

The school will provide:

- Induction training on this policy for all new staff
- Annual online safety training updates
- Guidance on specific systems and tools
- Support from IT staff for technical issues
- Access to the Designated Safeguarding Lead for safeguarding concerns

If staff require support with any aspects of technology use, they are encouraged to consult their line managers or the Digital Lead.

25. Related Policies

This policy should be read alongside:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct/Staff Behaviour Policy

- Data Protection Policy
- Complaints Procedure
- Anti-Bullying Policy
- Staff Disciplinary Procedures
- Business Continuity Plan
- Keeping Children Safe in Education

---

26. Policy Review

This policy will be reviewed annually (as a minimum) and updated if needed, so that it is kept up to date with safeguarding issues as they emerge and evolve, including lessons learnt, and is available publicly either via the school or college website or by other means.

This digital policy will inform any and all digital activities within the Trust and will be reviewed annually or when:

- A serious safeguarding issue is identified
- The Trust's risk profile changes
- Introduction of new technical devices
- Introduction of new curriculum software, websites or systems
- Curriculum changes
- The Trust changing how it uses technology
- The Trust's monitoring policy or processes changing
- Safeguarding guidelines changing

Appendices

Appendix A: Staff Declaration Form

I confirm that I have read, understood, and agree to comply with the Digital Policy.

I understand that:

- Failure to comply may result in disciplinary action
- The school may monitor my use of school systems
- I must report any concerns or breaches immediately
- This policy is essential for safeguarding children

Name: _____

Signature: _____

Date: _____

Role: _____

Appendix B: Device Loan Agreement

1. This agreement is between:
    - The Damara School (The Maltings, Raymond Street, Thetford, Norfolk, IP24 2EA) ("the school")
    - _____ ("the employee" and "I")

And governs the use and care of devices assigned to individual staff members. This agreement covers the period from the date the device is issued through to the return date of the device to the school. All issued equipment shall remain the sole property of the school and is governed by the school's policies.

2. The school is lending the employee a digital device ("the equipment") for the purpose of supporting teaching and learning and working at home.

   Description of laptop/portable electronic device and Asset ID:

   _____

3. This agreement sets the conditions for the employee taking the equipment home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I have read and agree to these terms.

Damage/Loss - By signing this agreement I agree to take full responsibility for the equipment issued to me and I have read or heard this agreement read aloud and understand the conditions of the agreement. I understand that I am responsible for the equipment at all times whether on the school's property or not. Please include the device in your home insurance (contents) if you have one. Ensure that this is communicated with the administrator.

If the equipment is damaged, lost or stolen, I will immediately inform CEO/Deputy Headteacher and I acknowledge that I may be responsible for full replacement costs. If the equipment is stolen, I will also immediately inform the police. I will not leave the equipment unsupervised in unsecured areas. I agree to keep the equipment in good condition and to return it to the school on demand from the school in the same condition.

Please include the device in your home insurance (contents) if you have one. Ensure that this is communicated with the administrator.

Unacceptable Use - I am aware that the school monitors my activity on the equipment. I will not carry out any activity that constitutes 'unacceptable use' according to the Digital Policy. I accept that if I engage in any activity that constitutes 'unacceptable use', I may face disciplinary action in line with the school's policies on staff discipline and staff code of conduct.

Personal Use - While I am permitted to use this device for personal use, abiding by the usage rules within the Digital Policy, and I will not loan the equipment to any other person including family members.

Data Protection - I agree to follow the measures in the Digital policy.

Return Date - I will return the device in its original condition to the office within 7 days of being requested to do so.

If I need help doing any of the above, I will contact the Network Administrator on the email ict@lotustrust.org.uk

Consent - By signing this form, I confirm that I have read and agree to the rules and conditions above.

FULL NAME

SIGNATURE

DATE

Appendix C: eSafety and Online Safety Training Needs – Self-Audit

Name: _____

Date: _____

Please complete this self-audit to help us identify your training needs in relation to online safety.

Question	Yes	No	Unsure
Do you know the name of the person who has lead responsibility for online safety in school?			
Do you know what you must do if a pupil approaches you with a concern or issue?			
Are you familiar with the school's acceptable use agreement for staff, volunteers, Trustees and visitors?			
Are you familiar with the school's acceptable use agreement for pupils and parents?			
Do you regularly change your password for accessing the school's ICT systems?			
Are you familiar with the school's approach to tackling cyber-bullying?			
Do you understand the school's filtering and monitoring systems?			
Do you know how to recognise phishing emails and suspicious communications?			
Are you confident in creating and managing strong passwords?			
Do you understand your responsibilities around data protection and GDPR?			
Do you know how to report a cybersecurity incident or data breach?			
Are you aware of the four areas of online risk (content, contact, conduct, commerce)?			
Do you understand the school's policy on social media use?			
Are you familiar with the school's guidance on using AI tools?			
Do you know how to keep devices secure when working remotely?			
Are you confident in recognising and responding to online safeguarding concerns?			

Are there any areas of online safety in which you would like training/further training? Please record them here:

Additional comments or concerns:

Signature: _____

Date: _____

Please return this completed form to: Deputy Head of School

Appendix D: Quick Reference Guide for Staff

Key Contacts

Issue	Contact	Details
Safeguarding concerns	Designated Safeguarding Lead (DSL)	Julie Cox - jcox@lotustrust.org.uk
IT/Technical support	Network Administrator	ict@lotustrust.org.uk
Cybersecurity incidents	Digital Lead (CEO)	ceo@lotustrust.org.uk
Data protection queries	Data Protection Officer (DPO)	ceo@lotustrust.org.uk
Policy queries	Deputy Head	Julie Cox - jcox@lotustrust.org.uk

What to Do If...

...You receive a suspicious email:

- Do NOT click any links or download attachments
- Do NOT reply to the email
- Forward to ict@lotustrust.org.uk
- Delete the original email

...You lose a school device:

- Immediately contact the Network Administrator and CEO
- If stolen, also report to the police
- Do not attempt to locate the device yourself

...You accidentally send confidential information to the wrong person:

- Immediately inform the Network Administrator and DPO
- Follow the data breach procedure
- Do not attempt to recall the email yourself

...A pupil discloses something concerning online:

- Listen carefully and do not promise confidentiality
- Reassure the pupil they have done the right thing
- Immediately report to the DSL
- Record the disclosure using CPOMS

...You need access to a blocked website for teaching:

- Email ict@thelotustrust.org.uk
- Provide the URL and explain why you need access
- Wait for approval before attempting to access

...You forget your password:

- Contact the Network Administrator
- Do NOT write passwords down or share them
- Do NOT use the same password for multiple accounts

Remember:

✓ Always use school email for work communications
✓ Lock your device when you leave it unattended
✓ Never share your password
✓ Report concerns immediately
✓ Maintain professional boundaries online
✓ When in doubt, ask!

Appendix E: Social Media Guidelines for Staff

10 Rules for School Staff on Social Media

1. **Change your display name** – use your first and middle name, use a maiden name, or put your surname backwards instead
2. **Change your profile picture** to something unidentifiable, or if you don't, make sure that the image is professional
3. **Check your privacy settings regularly**
4. **Be careful about tagging other staff members** in images or posts
5. **Don't share anything publicly** that you wouldn't be happy showing your pupils
6. **Don't use social media sites during school hours** (except for approved school accounts)
7. **Don't make comments about your job, your colleagues, our school or your pupils online** – once it's out there, it's out there
8. **Don't associate yourself with the school on your profile** (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. **Don't link your work email address to your social media accounts.** Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. **Consider uninstalling the Facebook app from your phone.** The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check Your Privacy Settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your old posts and photos – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't search for you by name – go to bit.ly/2zMdVht to find out how to do this
- Remember that some information is always public: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to Do If...

A pupil adds you on social media:

- In the first instance, ignore and delete the request

- Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers
- If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the Deputy Headteacher about what's happening

A parent/carer adds you on social media:

It is at your discretion whether to respond. Bear in mind that:

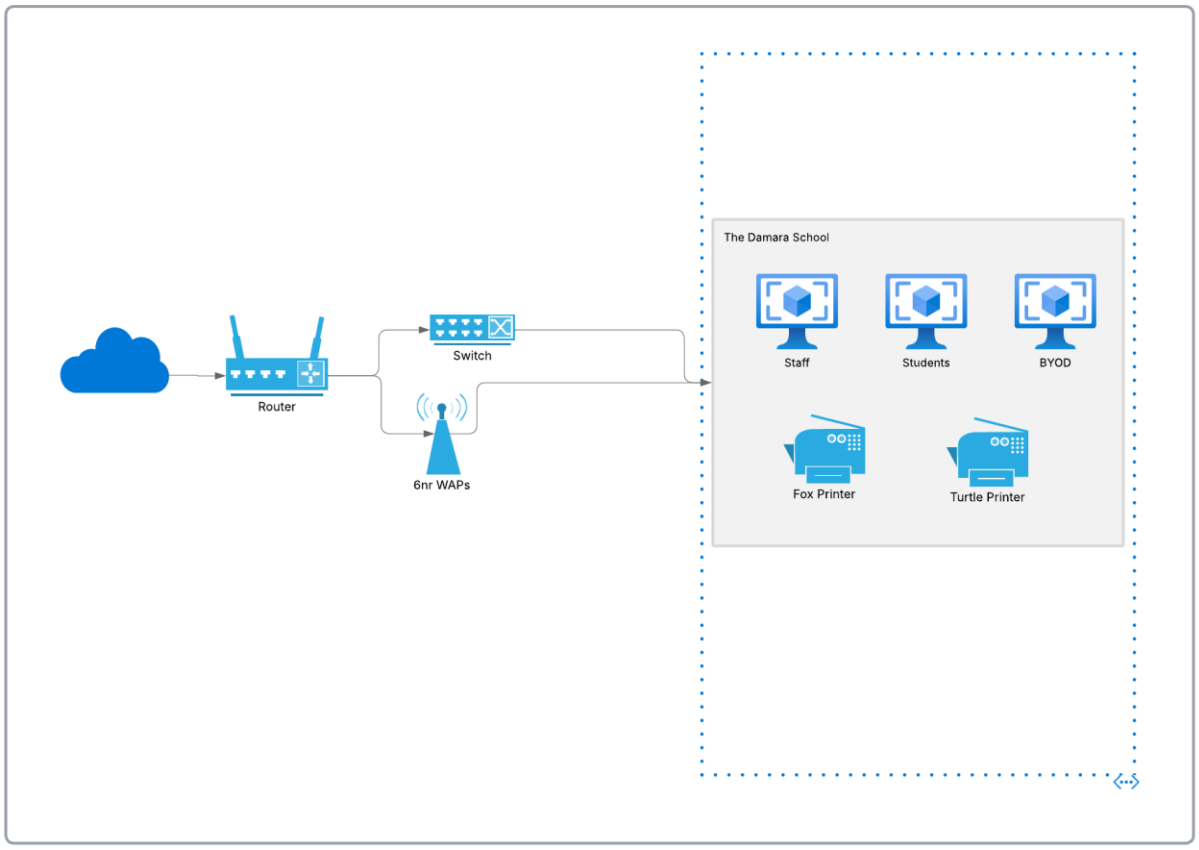
- Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you:

- Do not retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix F: Network Documentation

Network Diagram



Switch Details

Make	Model	Purchase Date	Warranty Expiry	Software Support Ends
Ubiquiti	USW-48-POE	12/01/2024	12/01/2031	12/01/2032

Specifications:

- Managed L2 Gigabit Ethernet (10/100/1000)
- Power over Ethernet (PoE)
- 1U Stainless Steel
- 48 RJ-45 Ports, L2, PoE+
- 4x SFP Ports
- 104 Gbps Switching Capacity

Switch Location Map

IP Address Ranges

[To be completed with specific IP address ranges for different network segments]

Switch Configuration

[To be completed with detailed switch configuration information]

Updates

Network documentation is maintained by the Network Administrator and updated whenever changes are made to the network infrastructure. All updates are reported to the Digital Lead.