ONLINE SAFETY POLICY 2026

At Link Academy Trust, our vision is clear:

Flourishing schools for all at the heart of our communities.

Inspired by, ***"Life in all its fullness" (John 10:10)*****,** we strive to create environments where every individual can thrive.

Our mission is underpinned by three core values that guide everything we do:

- **Belonging** – Every interaction matters; we nurture relationships and ensure everyone feels valued and included.
- **Curiosity** – We embrace ambition, creativity, and innovation to inspire lifelong learning.
- **Collaboration** – We foster an open culture of accountability and shared success, working together for the benefit of all.

These principles shape our approach to equality and diversity, ensuring that every policy, decision, and action reflects our commitment to inclusion and excellence.

Online Safety Policy 2026

The Link Academy Trust is a company limited by guarantee and an exempt charity, regulated by the Department of Education (DfE). All Members of the Board of Trustees of the exempt charity are also Directors of the company; the term 'Trustee' used in this Policy also means Director. This Policy applies to all academies within the Link Academy Trust.

The Link Academy Trust computing vision statement
We will use the teaching and learning of computing in all academies to empower our children to:

- Put computational thinking at the forefront of their learning across the curriculum.
- Become digitally literate.
- Be creative and resilient digital citizens.
- Keep themselves safe in an ever-changing digital landscape.
- Build solid foundations, based on sound knowledge, that prepare themselves for the world in which they will live and work.

Background and Rationale
The Trust recognises the importance of online safety and the need to keep this ever-developing area of technology under review.

Online safety is an ever-present serious safeguarding danger, which is implicit in all aspects of our computing and safeguarding policies and procedures throughout the academies. The policy reflects the importance of the procedures and practices that are implemented across the academies every day and links with all safeguarding policies and procedures.

Development, Monitoring and Review
The online safety policy has been developed through consultation with and between:

- CEO
- Executive Improvement Team (EIT)
- Executive/Academy Heads (E/AHs)
- Designated Child Protection Staff
- Teachers
- Support Staff
- Trustees and Governors
- Parents and Carers
- Pupils
- IT Support Partners

The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

The Trust will monitor the impact of the policy using:

- Logs of reported incidents
- Baytek monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity by Executive/Academy Heads (E/AHs), Local Advisory Committees (LACs) and Trustee scrutiny
- Surveys/questionnaires of pupils, parents, carers and staff

Scope of the Policy

This policy applies to all members of the academies within the Trust (including Trustees, Governors, staff, pupils, students, work experience, volunteers, parents and carers, visitors, community users) who have access to and are users of the Trust's ICT systems, both in and out of school. The Education and Inspections Act 2006 empowers E/AHs, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the academy. The Trust will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents or carers of incidents of inappropriate online behaviour that takes place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the Trust:

Trustees and Governors:

- Trustees are responsible for the approval of the online safety policy documents and for reviewing the effectiveness of the policy. The Trust Board and LACs, together with the E/AH, are responsible for the ongoing monitoring of the policy's implementation and effectiveness.

E/AH and Computing Leads:

- The E/AH is responsible for ensuring the safety (including online safety) of members of the academy community.
- The E/AH, Senior Teacher and Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (DDSL), must be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. The CEO must be informed of such allegations and consulted immediately.

The Academy Computing Curriculum Team:

- Leads the Online Safety group for each Academy comprising her/himself, the E/AH, the DSL/ DDSL and the Senior Teacher.
- Takes day to day responsibility for online safety issues and has a leading role in establishing, implementing and reviewing the Trust online safety policies and documents.
- Provides training and advice for staff.
- Liaises with the CEO, DCEO and Trustees.
- Liaises with the Trust Computing Support Company (CSC), currently Baytek
- Reports regularly to EIT.

The CSC is responsible for ensuring:

- That the Trust's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That each academy meets the online safety technical requirements outlined at Appendix 1 and any relevant National guidance.
- Users may only access the academy's networks through a properly enforced password protection policy.
- The CSC is informed of issues relating to the filtering and reports to the Central Business Team when the problem has been resolved to ensure individual E/AHs are informed. Inappropriate adverts are often the biggest offenders and 'pop up' blockers are in force.

Teaching and support colleagues are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current Trust policy and practices.
- They have read, understood and signed the Staff Acceptable Use Agreement (Appendix 3)

- They report any suspected misuse or problem to the DSL or DDSL for investigation, action or sanction in collaboration with the E/AH.
- Digital communications with pupils should only be on a professional level and only carried out using official academy systems. When a member of staff leaves the Trust, such communications must cease.
- Pupils understand and follow the Trust's Online Safety policy and Pupil Acceptable Use Agreement (Appendix 2)
- Older pupils should be introduced to the need to avoid plagiarism and uphold copyright regulations.
- They monitor computing activity in lessons, extra-curricular and extended academy ICT activities.
- They are aware of online safety issues related to the use of mobile phones, cameras and handheld devices like iPads and smart watches and that they monitor their use and implement current Trust policies with regard to these devices.
- In lessons where the internet is used, pupils in Key Stage 1 should be guided to sites checked as suitable for their use. In Key Stage 2, pupils are taught about safe searching and website reliability to allow for more independent use of the internet.
- To facilitate a more independent approach to the gathering of information when this process is not used, there is a focused procedure in place for guiding pupils in dealing with any unsuitable material that is found in internet searches.
- The webpage details of any inappropriate sites accessed are emailed to the CSC for immediate blocking.

Designated Safeguarding Lead (DSL)
The DSL is trained in online safety issues and is aware of the potential for serious child protection issues to arise from:

- Sharing of personal data and their vulnerability to others accessing their information for financial gain or other criminal activity.
- Access to illegal and inappropriate materials, including those with extremist content.
- Inappropriate on-line contact with adults including strangers.
- Potential or actual incidents of grooming (child sexual exploitation).
- Sexting, where personal photographs of a sexual nature are attached to text messages.
- Cyber-bullying.
- Mental health issues that can arise from addictions to gaming and sites with extreme content.

Pupils
- Are responsible for using the Trust's ICT systems in accordance with the Pupil Acceptable Use Agreement, which they will be expected to sign before being given access to academy systems.
- Have an age-appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand Trust policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand Trust policies on the use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Trust's online safety policy covers their actions out of school, if related to their membership of the academy.

Parents and Carers
Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and literature. Parents and carers will be responsible for endorsing (Pupil Acceptable Use Agreement).

Policy Statements

Education – pupils
Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the Trust's online safety provision. Children and young people need the help and support of the academy to recognise and avoid online safety risks and build their resilience. Online safety education will be provided in the following ways:

- A planned online safety programme will be provided as part of Computing curriculum and will therefore be taught to all pupils at the start of every new term– this will cover both the use of computers and new technologies in school and outside school.
- Key online safety messages will be reinforced as part of assemblies and pastoral activities.
- Pupils will be taught in all lessons to be critically aware of the materials and content they access online and be guided through discussion to recognise that not all information found online is accurate.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use of computers, the internet and mobile devices both within and outside school.
- Rules for use of ICT systems and safe internet use will be displayed in all classrooms.

Education – parents and carers
The Trust seeks to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, Facebook, text to parents
- Parents' evenings
- Drop-in clinics.
- Reference to relevant websites such as thinkyouknow.org.uk

Education and Training – Staff
All staff receive online safety training and understand their responsibilities, as outlined in this policy.

All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the Trust Online Safety policy and they sign the Staff Acceptable Use Agreement. Training will be offered as follows:

- Basic online safety training including cyber security will be refreshed annually for all staff.
- INSET, staff meetings and online training will further update staff throughout the year as appropriate.
- Parents, governors and other stakeholders including parents will also be offered regular training opportunities.

Education – Local Advisory Committees
LACs will receive regular information updates on online safety training and monitoring. In addition, they will receive training as part of their annual CPD provision.

Technical – Infrastructure, Equipment, Filtering and Monitoring
The Trust, through the CSC, will be responsible for ensuring that the Trust infrastructure and network is as safe and secure as is reasonably possible.

- Academy ICT systems will be managed in ways that ensure that the academy meets the online safety technical requirements outlined in Appendix 1 and any relevant National guidance.
- There will be regular; at least annual, reviews and audits of the safety and security of Trust and individual academy ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to Trust/academy ICT systems. Details of the access rights available to groups of users will be recorded and managed by the CSC and will be reviewed at least annually.
- All users will be provided with a username and password. Two form authentication will be implemented for adult users.

- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security to the E/AH.
- The CSC maintains and supports the filtering service provided by Netsweeper across the Trust.
- Any filtering issues should be reported immediately to the CSC.
- The CSC will regularly monitor and record the activity of users on the Trust ICT systems and users are made aware of this in the Acceptable Use Agreements (Appendices 2&3).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices etc. from accidental or malicious attempts which might threaten the security of the Trust/academy systems and data.
- An agreed policy is in place regarding the downloading of executable files. This can only be done by Baytek
- Within the Staff Acceptable Use Agreement there is a section relating to the use of staff laptops regarding the extent of personal use that users and their family members are allowed on laptops and other portable devices that may be used out of school. We believe that confidence comes from regular use and encouraging personal activity is a good way to ensure that. Essentially it is acceptable to use laptops for personal use provided that only appropriate information and websites are accessed, and no illegal activity is undertaken whilst using them.
- The Trust/academy infrastructure, individual workstations and all laptops are protected by up-to-date virus software. We ask that all staff ensure that personal computers, not owned by the Trust, are also protected by up-to-date virus software to protect any virus contamination.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Data pens are not permitted to be used to transfer files between computers. Such is the potential to cause critical damage to our systems that failure to comply with this requirement may lead to action being taken.
- See Appendix 1 – Technical Security Policy

Use of digital and video images – Photographic and Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images in an appropriate way. Many pupils are already on social networking sites, despite the fact that they are significantly below the age limit. In particular, pupils should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.
- Staff are allowed to take digital and video images to support educational aims, but must follow Trust policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Trust equipment, the personal equipment of staff should not be used for such purposes, unless with the permission of the E/AH.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Images should be focussed on the activity and will ideally show small groups of children, rather than individuals. Images used must not cause distress, upset or embarrassment to pupils. Any image published will be considered to not be open to misuse by others.
- Pupils' names will not be used anywhere on a website or blog, in association with photographs.
- We maintain a list, with photographs, of pupils whose parents do not wish their image to appear on our websites. Staff need to refer to this list, held by E/AH, DSL and School Office. These pupils will not have any photograph, face-on, published in any way.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.

- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they comply with the Data Policy by:

- At all times taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Using personal data only on secure password protected computers and other devices, ensuring that they are properly "logged off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Communications

When using communication technologies, the Trust considers the following as good practice:

- The official Trust email service may be regarded as safe and secure; however, this is dependent upon your own personal password security. You must sign out of your office 365 on public machines.
- Users must immediately report, to the E/AH, in accordance with the Trust policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents or carers (email, chat, text, etc.) must be professional in tone and content.

Unsuitable or Inappropriate Activities

The Trust believes that the activities referred to in the Acceptable Use Agreements would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using academy equipment or systems.

If any apparent, suspected or actual misuse appears to involve illegal activity i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist or extremist material
- Other criminal conduct, activity or materials

The Trust and Academy protocol on Child Protection and Online Safety must be followed. This Policy is reviewed by the E/AH, Trust Computing Curriculum Team, LACs and the Standards and Curriculum Committee on an annual basis and approved by The Board of Trustees thereafter.

Approved by the Board of Trustees: 12 July 2021
Reviewed by S&C Committee: 9th July 2024
Approved by the Board of Trustees: 22nd July 2024
Reviewed by S&C Committee: 3rd February 2026
Approved by the Board of Trustees: 9th February 2026
Next Review: Spring 2027

Appendices

Technical Security Policy (including filtering, monitoring and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. This is informed by the Department for Education (DfE) guidance, Keeping Children Safe in Education, and the Digital and Technology Standards and therefore applicable for schools in England. The Trust is responsible for ensuring that the *school infrastructure/network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- access to personal data is securely controlled in line with the school's personal data policy
- system logs are maintained and reviewed to monitor user activity
- there are effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems, including filtering and monitoring provision

Responsibilities

Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. The management of technical security is the responsibility of Trustees and Senior Leaders, supported in this by the Designated Safeguarding Lead, Online Safety Lead and IT Service Provider.

Policy statements

The Trust is responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- Cyber security is included in the school risk register.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems, and cabling must be securely located and physical access restricted.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- Appropriate security measures (including updates) are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data, including operating systems.
- The school's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats.
- Responsibilities for the management of technical security are clearly assigned to the Trust's CSC.
- All users will have clearly defined access rights to school technical systems and accounts are deleted when the user leaves. Details of the access rights available to groups of users will be recorded by the CSC and will be reviewed, at least annually, by the online safety group.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security (see Access control policy)
- The CSC, in partnership with Trustees/SMT/SLT/DSL, regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.

- Users should report any actual/potential technical incident to the E/AH and CSC as expediently as possible.
- The CSC are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Guest users are provided with appropriate access to school systems based on an identified risk profile.
- By default, users do not have administrator access to any school-owned device.

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform). Further details can be found at the National Cyber Security Centre and SWGfL "Why password security is important".

Policy Statements:

- The password policy and procedures reflect NCSC and DfE advice/guidance.
- The use of passwords is reduced wherever possible, for example, using Multi-Factor Authentication (MFA) or (Single Sign On) SSO.
- Security measures are in place to reduce brute-force attacks and common passwords are blocked.
- School networks and system will be protected by secure passwords.
- Passwords are encrypted by the system to prevent theft.
- Passwords do not expire, and the use of password managers is encouraged.
- Complexity requirements (e.g. capital letter, lower case, number, special character) are not used.
- Users can reset their password themselves.
- All passwords are at least 12 characters long and users are encouraged to use 3 random words.
- Passwords are immediately changed in the event of a suspected or confirmed compromise.
- No default passwords are in use. All passwords provided "out of the box" are changed to a unique password by the CSC.
- All accounts with access to sensitive or personal data are protected by Multi-Factor Authentication methods.
- A copy of administrator passwords is kept in a secure location.
- All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.

Filtering and Monitoring

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, as online content changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

The filtering system will apply to all:

- Users, including guest accounts.
- school owned devices
- Devices using the school broadband connection.

The filtering system will:

- Filter all internet feeds, including any backup connections.
- Be age and ability appropriate for the users and be suitable for educational settings.

- Handle multilingual web content, images, common misspellings and abbreviations.
- Identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them.
- Provide alerts when any web content has been blocked.

Mobile and app content is often presented in a different way to web browser content. If users access content in this way, the Trust will obtain confirmation from the filtering provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

Introduction to Monitoring

Monitoring user activity on school devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring will allow us to review user activity on school devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

The monitoring strategy is informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

Filtering and Monitoring Responsibilities

DfE Filtering Standards require that schools identify and assign roles and responsibilities to manage your filtering and monitoring systems, and include:

Role	Responsibility	Name / Position
Responsible Trustee	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	D Course
Senior Leadership	Team Member Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	DCEO
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems	Director of Safeguarding
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports	Baytek

	• completing actions following concerns or checks to systems	
All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:	• they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs • there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material	

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the filtering provider by actively employing the Internet Watch Foundation URL list and other illegal content lists. Filter content lists are regularly updated, and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- There is a filtering and monitoring system in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content.
- There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.
- Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.
- The filtering and monitoring provision is reviewed at least annually and checked regularly.
- There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change.
- Mobile devices that access the school's internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.

Changes to Filtering and Monitoring Systems

All requests for changes to the filtering and monitoring systems must be made in accordance with the Change Control policy.

Filtering and Monitoring Review and Checks

To understand and evaluate the changing needs and potential risks of the school, the filtering and monitoring provision will be reviewed at least annually. The review will be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the CSC. Additional checks to filtering and monitoring will be informed by the review process so that governors have assurance that systems are working effectively and meeting safeguarding obligations.

Reviewing the filtering and monitoring provision

A review of filtering and monitoring will be carried out to identify the current provision, any gaps, and the specific needs of learners and staff.

The review will take account of:

- the risk profile of learners, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what the filtering system currently blocks or allows and why

- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of learners
- teaching requirements, for example, the RHSE and PSHE curriculum
- the specific use of chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies are in place
- what checks are currently taking place and how resulting actions are handled

To make the filtering and monitoring provision effective, the review will inform:
- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review will be carried out as a minimum annually, or when:
- a safeguarding risk is identified
- there is a change in working practice, e.g. remote access or BYOD
- new technology is introduced

Checking the filtering and monitoring systems
Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

When filtering and monitoring systems are checked this should include further checks to verify that the system setup has not changed or been deactivated. Checks are performed on a range of:
- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

Logs of checks are kept so they can be reviewed. These record:
- when the checks took place
- who did the check
- what was tested or checked
- resulting actions

Training/Awareness
It is a statutory requirement in England that staff receive training, at least annually, about safeguarding, child protection, online safety and filtering and monitoring. Furthermore, in order to protect personal and sensitive data, governors, senior leaders, staff and learners should receive training about information security and data protection, at least annually.

Trustees, Senior Leaders and staff are made aware of the expectations of them:
- at induction
- at whole-staff/trustee training
- through the awareness of policy requirements
- through the acceptable use agreements
- in regular updates throughout the year

Those with specific responsibilities for filtering and monitoring (Responsible Trustee, DSL, OSL or other relevant persons) will receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

Learners are made aware of the expectations of them:

- in lessons by way of completing the national ICT curriculum
- through the acceptable use agreements

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc.

Audit/Monitoring/Reporting/Review

Trustees/SLT/DSL/OSL will ensure that full records are kept of:

- Training provided
- User Ids and requests for password changes
- User logons
- Security incidents related to this policy
- Annual online safety reviews including filtering and monitoring
- Changes to the filtering system
- Checks on the filtering and monitoring systems

Further Guidance

Schools in England (and Wales) are required "*to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*". Furthermore, the DfE's statutory guidance 'Keeping Children Safe in Education' obliges schools in England to "*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness*" and they "*should be doing all that they reasonably can to limit children's exposure to the above risks from the school's IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."

Appendix 2:
Pupil Acceptable Use Agreement for KS2

Introduction
Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity, and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:
- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement
When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:
- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and password safe and secure and not share it with anyone else.
- I will be aware of "stranger danger" when I am online.
- I will not share personal information about myself or others when online.
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me.
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:
- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:
- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:
- I will hand my phone into the school office every morning and collect my phone at the end of the day. I will ensure my phone is switched off
- I will only use social media sites with permission and at the times that are allowed
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work**.**

I understand that I am responsible for my actions, both in and out of school:
- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include loss of access to the school network/internet, suspensions, parents/carers contacted and in the event of illegal activities involvement of the police.

Learner Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: Group/Class:

Signed: Date:

Parent/Carer Countersignature

Name of Parent:

Signed: Date:

Appendix 3:
Pupil Acceptable Use Agreement for KS1 and EYFS

This is how we stay safe when we use computers:

• I will ask a teacher or suitable adult if I want to use the computers/tablets.

• I will only use activities that a teacher or suitable adult has told or allowed me to use.

• I will take care of computers/tablets and other equipment.

• I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

• I will tell a teacher or suitable adult if I see something that upsets me on the screen.

• I know that if I break the rules, I might not be allowed to use a computer/tablet.

Signed (child):

(for younger children the signature of a parent/carer should be sufficient)

Name of parent/carer

Signed by parent/carer:

Appendix 4:
Staff (and Volunteer) Acceptable Use Agreement
School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I will refer to the School Mobile and Smart Technology Policy.
- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that only the Trust/academy devices to be used in school as these are protected by up to date virus software to protect any virus contamination.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- **I will be professional in my communications and actions when using school systems:**
    - I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
    - I will communicate with others in a professional manner, I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are

published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not use my personal email addresses/mobile phone/social networking sites to communicate with parents/careers.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened**.**

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

Appendix 5

Internet Safety Protocol across the Link Academy Trust

The most important and effective strategy to keep children safe is education, education, education! Through an embedded Online Safety curriculum, discussion, support and guidance by staff, and support to parents, we can equip pupils with the skills and attitudes to keep themselves safe and avoid risk taking behaviour. Educating children to keep themselves and others safe online is the most important task we undertake when considering Online Safety.

The internet in the Link Academy Trust has a range of filters and security devices. By logging onto the academy system pupils agree to abide by the Trust's Pupil Acceptable Use Agreement. However, some problems can still arise.

1. Pupils may access sites bypassing the Netsweeper proxy although we have measures in place to prevent this, such as group policies on laptops and restrictions on iPads. In this case the name of the student needs to be passed to the E/AH who will arrange for the pupil to be banned from using the Internet unassisted and for their parents to be informed. The device needs to be handed to the E/AH.

2. Pupils may try to access social media sites including web-based email and messenger Apps, e.g., WhatsApp. We have measures in place to block inappropriate age-related social media, which sometimes can contain unkind comments about other pupils and has the potential for cyberbullying. Any attempts to access inappropriate social media or web-based email or messaging will result in Internet independent use being suspended and parents being informed.

3. Pupils find inappropriate images and language on sites that they have found in the course of their work. In this case the teacher needs to:

- Record the name of the student and the web address and remove the machine they were on.
- Pass this information on to the Executive/Academy Head and Baytek. Baytek will block inappropriate sites on the Netsweeper filter and inform the CEO should the need arise.
- The DSL will assess the risk and contact the appropriate parties if this is deemed to be a child protection issue following our Online Safety incident reporting procedures.

If the teacher feels these images have been saved into the pupil's work area, they should inform Baytek. They will then go into the pupil's work area and retrieve then delete the image. This will be reported to the E/AH who will take appropriate action.

There may be instances when teachers need to do searches and accidentally go to web pages that may contain inappropriate images. If this happens, they must notify the E/AH so the use can be logged.

Staff need to know who to report to. Any incident or issue must be reported to the E/AH in the first instance.

Remember, if a child discloses an Online Safety issue to you, or you see or hear anything that concerns you, make sure you report it as soon as possible.

If you have a personal digital safety or cyberbullying concern, you can contact the Professionals Online Safety Helpline on 0844 381 4772 or helpline@saferinternet.org.uk