Online Safety Policy 2024/26

The Link Academy Trust is a company limited by guarantee and an exempt charity, regulated by the Education & Skills Funding Agency (ESFA). 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
- 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
- Limbtec 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 Limbtec.
- 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 (by signature) the 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 Agreements. 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 at 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. The HR Officer will also hold that information securely.
- All users will be provided with a username and password. Two form authentication will be implemented.

- 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 and 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 Limbtec.
- 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. This is applicable to pupils in Key Stage 2, many of whom 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. Photographs may be used in classrooms.

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 a 2-yearly cycle 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

Appendices

Appendix 1: Technical Security Policy

Appendix 2: Pupil Acceptable Use Agreement

Appendix 3: Staff Acceptable Use Agreement

Appendix 4: Child Protection Policy (including the Internet Safety Protocol)

Appendix 5: Anti Bullying Policy

Appendix 1

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 is 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 in order 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 are able to 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.

Learner passwords:
Schools need to take a risk-based approach to the allocation of learner usernames and passwords. Schools should be able to identify individuals accessing their systems and an individual logon is the recommended approach. For younger children and those with special educational needs, the DfE guidance states that schools could:

- Consider using authentication methods other than passwords.
- Consider using a separate account accessed by the teacher rather than the student.
- Segment the network so such accounts cannot reach sensitive data.
- Consider if the data or service being accessed requires authentication.

Policy Statements

- For younger children and those with special educational needs, learner usernames and passwords can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. Password complexity for these users could be reduced (for example 6-character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.

- Learners are encouraged to set passwords with an increasing level of complexity. Passwords using 3 three random words and with a length of over 12 characters are considered good practice.
- Users will be required to change their password if it is compromised. (Note: passwords should not be regularly changed but should be secure and unique to each account.)
- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important. The Project EVOLVE Privacy and Security strand should help you with this.

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 • completing actions following concerns or checks to systems	LIMBTEC
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

This is reviewed and signed on an annual basis. One copy is returned and placed in the pupil file and the other is retained by the parents or carers.

We allow you to use our Academy ICT Network and equipment that has different programs and apps for you to use. It also allows you to go onto the Internet. We trust you to use these programs, apps and the internet safely and sensibly but if you break the rules on purpose, we will stop you having the use of internet or learning resources, including pupil files, until we are sure that you can do so safely and respectfully. Here are the rules you must follow:

- Your folders belong to the school and staff will look at the files in there. They are not private to you.
- Staff can see what you are doing on a computer at any time and can track what you have been doing after you finish.
- The use of the internet is provided for your learning. All the sites and apps you visit are recorded.
- We expect you to behave sensibly and safely whilst using ICT equipment.
- Treat any computer or technology equipment with respect so that it does not get damaged. You should not move any equipment unless a member of staff asks you to. The Trust reserves the right to seek remuneration from parents of pupils who cause malicious damage to ICT equipment.
- Do not use another person's password or tell anyone else what your password is. If you think someone is using your password, then tell a member of staff.
- We try very hard to prevent you seeing websites that have nasty images on them or are about violence or that have things that are not appropriate for children to read. If one of these websites gets through our protection system, you should put the lid of laptop down / turn off the monitor / put the tablet face down and tell a member of staff immediately. Do not close the website – this is so a member of staff can get the website blocked. You must not show it to another pupil.
- Individual emailing outside the school system is not allowed. Going onto internet sites such as messenger and emailing are strictly forbidden.

If you do any of the following things in school, on purpose, you will be reported to the Executive/ Academy Head, and we will prevent you from using the internet unassisted and contact your parents:

- Visiting internet sites without permission or visiting sites that are not part of the topic you've been asked to look at.
- Using someone else's password and going into their personal folder
- Emailing anyone from an Internet site or sending messages to other pupils
- Using a social networking site such as Facebook
- Downloading plugins or games

I agree to abide by the rules of the Pupil Acceptable Use Agreement for (**INSERT ACADEMY)**

Pupil Name: Class: Signature:

Parent's Name: Signature: Date:

Appendix 3

Staff Acceptable Use Agreement (and Volunteer use)

This policy is reviewed annually, or as new information becomes available.

- I will only access the system with my own name and registered password, which I will keep secret and I will inform Limbtec as soon as possible if I know my password is no longer secret.
- I acknowledge that any devices provided for me to use remain the property of the Trust and should only be used for appropriate activities and tasks.
- I will not access the files of others or attempt to alter settings without permission.
- I will not alter, attempt to repair or interfere with the components, software or peripherals of any computer or device that is the property of the Trust.
- I will always log on using my password and log off the system when I have finished working.
- I understand that the Trust may, in line with DfE policy, check my computer files and e-mails and may monitor the internet sites I visit.
- I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of Limbtec.
- Any e-mail messages I send will not damage the reputation of the Academy or Trust.
- Any joke e-mails and attachments should be considered carefully before being forwarded to ensure that they do not contain any offensive, illegal or virus content. If in any doubt they should not be sent.
- I will report immediately, to the Executive/Academy Head, any unpleasant material or messages sent to me.
- I will adhere at all times to the policy on the taking of photographs.
- I understand that a criminal offence may be committed by deliberately accessing internet sites that contain certain illegal material.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Activity that threatens the integrity of the Trust's ICT systems, or activity that attacks or corrupts other systems are forbidden.
- I understand that I am responsible for the safety of sensitive Academy/Trust data that I use or access.
- In order to maintain the security of data I will take the following steps:
  - I will not save data files to a PC, laptop or device other than that provided by the Trust.
  - If I need to transfer data files to view off site, I will only do so using our secure Office 365
- I will not share or give out any passwords that I use to access Trust systems – if I have reason to believe that my password is no longer secure, I will seek to change it.

Sensitive data includes:

- Pupil reports ▪ SEN records ▪ Letters to parents ▪ Class based assessments ▪ Exam results Whole Academy data ▪ Medical information ▪ Information relating to staff, e.g., Appraisal Reviews. If you are in any doubt as to the sensitivity of data you are using, please consider these questions:
- Would it place anyone at risk? Would it cause embarrassment to an individual or the Academy? Would it divulge personal information? Would it have legal or financial implications? If the answer to any of these questions is yes, then please treat the data as sensitive.

Taking Photographs

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. Taking pictures of children with personal devices such as mobile phones is not permitted unless with the permission of the Executive/Academy Head. To share pictures with parents via Facebook and the academy website, it is permissible to use school iPads. However, no image may be taken that could, in any way, be construed as being of an inappropriate nature that compromises the dignity and safety of a child. It is also not permitted to take pictures of adults without their permission and sharing these in any way other than through academy-based activity is strictly forbidden. Images taken in school must never be used for personal reasons nor shared with unauthorised persons and should be deleted from the iPad as soon as it is no longer necessary for it to remain on the device.

Staff Conduct in the use of Social Networking

In general terms, the Trust expects that the conduct of its employees is such that no justifiable complaint can be made by parents, pupils, colleagues, Governors, other bodies or agencies or members of the community in relation to conduct and behaviour of Trust staff. This principle applies to the use of social networking sites.

The way in which Trust staff present and conduct themselves on social networking sites can have an impact on the public perception of the Trust and its academies and influence the way in which those staff members are perceived by pupils and parents. In their use of social networking sites, staff should be aware that that their online behaviour could affect their professional standing, dignity and perception of their integrity.

It is recommended that staff take adequate precautions when using social networking sites and applications, both in vetting material that could be connected to them (through their own profile and information added about them) and through the use of appropriate security settings.

It is forbidden for Trust employees to be “friends” with pupils on social networking sites as this could be viewed as a safeguarding issue.

It is recommended that Trust employees do not identify our Academies on social networking sites as this could directly link their behaviour outside of work with the reputation of the Trust and its academies.

Where pupils behave inappropriately online with staff this should be reported to the same colleagues and this will be dealt with through the Trust’s pupil disciplinary process. The following are examples of what the Trust considers to be gross misconduct:

- Conduct that is a serious abuse of position – e.g., entering into a personal relationship with a pupil.
- Criminal offences and other conduct outside employment could cause an employee’s position at the Trust to become untenable particularly in circumstances where the conduct or offence is unacceptable to colleagues, leadership or parents or where the conduct or offence has the potential to affect the reputation of the Trust and Academy.
- Making defamatory statements in the course of employment (e.g., making statements that are or could be slanderous or libellous) whether orally, written, or in electronic communication.
- Breach of these disciplinary rules in relation to social networking or any inappropriate use of social networking sites and applications by staff will be dealt with through the Trust’s Disciplinary Procedure.
- I understand that if I do not adhere to any of the rules outlined in this agreement, my network access may be suspended immediately, any Trust devices removed and that other disciplinary consequences may follow.

Name

Signature Date

Executive/Academy Head Authorisation:

Appendix 4

Child Protection and 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 Executive/Academy Head 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 Executive/Academy Head.

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 Limbtec. Limbtec 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 Limbtec. They will then go into the pupil's work area and retrieve then delete the image. This will be reported to the Executive/Academy Head 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 Executive/Academy Head so the use can be logged.

Staff need to know who to report to. Any incident or issue must be reported to the Executive/ Academy Head 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

Anti-Bullying Policy

This Policy applies to all academies within the Link Academy Trust.

Introduction

The Link Academy Trust always strives to promote positive behaviour and encourage good relationships between pupils in its schools. In spite of this, it is accepted that some bullying incidents will still occur. Bullying can be:

- Physical: pushing, kicking, hitting, pinching, any form of violence, threats.
- Verbal: name-calling, sarcasm, spreading rumours, persistent teasing.
- Emotional: tormenting, threatening ridicule, humiliation, exclusion from groups or activities.
- Racist: racial taunts, graffiti, gestures.
- Sexual: unwanted physical contact, abusive comments.

It is the responsibility of the individual academy, and everyone associated with that academy to eradicate bullying by ensuring the development of a caring and supportive ethos.

This document provides details of the Trust's policy on dealing with such incidents of bullying.

Aims

The aims in managing incidents of bullying are:

- To provide a secure environment in which pupils can report incidents confidently.
- To show all pupils and parents that bullying is taken seriously.
- To enable staff to respond calmly and consistently to bullying incidents.
- To reassure pupils that the academy will protect and support all parties whilst the issues are resolved.
- to provide long term and positive programmes of personal development where it is required

Definition of Bullying

There is no legal definition of bullying, but it is generally considered to be when an individual or a group of people with more power, repeatedly and intentionally cause hurt or harm to another person or group of people who feel helpless to respond. Bullying can continue over time, is often hidden from adults, and will probably continue if no action is taken.

It is usually defined as behaviour that is:

- repeated
- Intended to hurt someone either physically or emotionally.
- often aimed at certain groups, for example because of race, religion, gender or sexual orientation

What bullying is not:

- single episodes of social rejection or dislike
- single episode acts of nastiness or spite.
- random acts of aggression or intimidation
- mutual arguments, disagreements or fights.

These actions can cause great distress. However, they do not fit the definition of bullying, and they're not examples of bullying unless someone is deliberately and repeatedly doing them.

Implementation of the Policy

Each academy will regularly emphasise to pupils that bullying is not acceptable and that all incidents will be taken seriously.

Pupils will also be encouraged to report incidents of bullying to a member of staff or their parents. Parents should raise any concerns they have with the class teacher or Executive/Academy Head at the earliest opportunity.

All incidents of bullying will be taken seriously, investigated and appropriate action taken. Incidents will be dealt with speedily, fairly and positively. A written record will be kept of all incidents where further investigation is considered necessary – this record will include detail of the incident(s), the investigation and outcome.

Parents will be informed at the earliest opportunity where an incident is considered serious enough to warrant further investigation or where there are repeated incidents of a minor nature.

Parents will be made aware of the Trust's complaints procedure. Any complaints made through that procedure will be taken seriously and dealt with accordingly.

Advice and support will be offered to the bullied individual.

The bully will be supported in recognising their unsociable behaviour and offered support to modify that behaviour. Staff will also ensure that, where necessary, action is taken to prevent further incidents.

Such action may include:

- imposition of sanctions
- obtaining an apology
- informing parents of both bully and bullied
- provision of mentor support for both victim and bully

All staff, teaching and non-teaching will be vigilant and deal with all observed incidents of bullying even where the bullied individual has not reported the incident.

All teaching staff, non-teaching staff and parents will be made aware of the contents of this policy.

Evaluation and Review

All staff will be asked to ensure that they are familiar with the contents of this policy and will be encouraged to provide feedback on its effectiveness on an ongoing basis.

This policy will be brought to the attention of all parents and will be freely available to any parent wishing to see a copy.