Spencer Alliance for Leadership and Teaching: Online Safety Policy 2023-2024

Date of Adoption: 29.08.2023
Date of Review: 29.08.2024
Policy Owner: Tammy Elward, Director of SALT
Approved: Sarah Mcananey, Director of Inclusion and Safeguarding

The Spencer Alliance of Leadership and Teaching wish to ensure that every person, from course participants to leaders and assessors, engaged with our programmes and course delivery, is treated fairly and equitably at all times. This includes all arms of work:

Spencer Teaching School Hub, including all CPD courses
Spencer Teaching School Hub AB Services
George Spencer Academy SCITT
Spencer Apprenticeships
The Derby Research School at Wyndham Primary Academy
Maths Hub East Midlands West

This policy sits alongside the wider umbrella of the Spencer Academies Trust policies which sits here.

Definitions

The term 'learners' is used here to cover apprentices, SCITT trainees and participants on programmes and engaging with our AB Services as part of the Teaching School Hub. This reflects the broad scope of our engagement with young and adult learners.

Contents

Reporting Safeguarding, Prevent and E-Safety Concerns

SPENCER ALLIANCE for Leadership & Teaching

Safeguarding and Prevent

SALT Team Roles and Responsibility

Caroline Arnold
SALT Team Designated Safeguarding Lead
ITT Director and TSH Assistant Director
carnold@george-spencer.notts.sch.uk

Vicki Ilic
Mental Health and Wellbeing First Aider
SCITT Coordinator
vilic@george-spencer.notts.sch.uk

Tammy Elward
Prevent Lead and LGBTQ+ Trusted Link
SALT Director
tammyelward@satrust.com

Safeguarding is everyone's responsibility

Designated Safeguarding Lead: Caroline Arnold
carnold@george-spencer.notts.sch.uk

SALT Prevent Lead: Tammy Elward
tammyelward@satrust.com

Reporting Concerns within the SALT Team – My Concern
https://myconcern.thesafeguardingcompany.com/Concern/New

Reporting Concerns beyond the SALT Team – SALT Team Log
Please share your concerns here on our log form

East Midlands Regional Prevent Coordinator: Sam Slack
sam.slack@education.gov.uk
07384452156

Aims

Our organisation aims to:

- Have robust processes in place to ensure the online safety of learners, staff, volunteers and governors to deliver an effective approach to online safety, which empowers us to protect and educate the whole community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools and organisations on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting learners from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. The policy also takes into account the National Curriculum computing programmes of study.

Roles and responsibilities

The Spencer Academies Trust Executive Leadership Team

The Trust Executive Leadership Team, including the Trust Safeguarding Lead, has overall responsibility for monitoring this policy and holding the SALT Director to account for its implementation. The Trust Safeguarding Lead will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs (as recorded on My Concern) as provided by the senior designated safeguarding lead (DSL). The SALT Team also adhere to annual audit checks conducted by the Trust Safeguarding Lead.

The Director of SALT

The Director is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the organisation.

The SALT Designated Safeguarding Lead

Details of the organisation's DSL and other key colleagues are set out at the top of this policy and in our safeguarding policy. The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the director in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the director, ICT faculty support and other staff, as necessary, to address any online safety issues or incidents

- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the organisation's safeguarding policy

- Updating and delivering staff training on online safety

- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

The ICT faculty support team

The ICT faculty support team is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep learners safe from potentially harmful and inappropriate content and contact online while training with the organisation, including terrorist and extremist material
- Ensuring that the organisation's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly/fortnightly/monthly basis (as required for specific checks)
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see 'Reporting Safeguarding Prevent and E-Safety Concerns' section) and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

Learners and Parents

Learners and parents (where learners are below the age of 18) are expected to:

- Notify a member of staff of any concerns or queries regarding this policy
- Ensure they have read, understood and agreed to the terms on acceptable use of the organisation's ICT systems and internet (appendices 1 and 2)

Learners and parents can seek further guidance on online safety from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

Visitors, Facilitators, Guest Speakers and Members of the Community

Visitors, facilitators, guest speakers and members of the community who use the organisation's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it (appendix 1).

Educating Learners about Online Safety

Learners will be taught about online safety as part of their training curriculum (predominantly covered in the 'Personal Development' curriculum, but also in terms of E-Safety for Pupils they are working with)

Personal Development Curriculum

During the programmes of study, learners will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of conduct apply in all contexts and the implications for them professionally (e.g Teacher Standards – Professional Expectations), including online
- About online risks, including the difficulty of removing potentially compromising material placed online or shared with others, and the implications professionally relating to pre-employment checks (KCSIE September 2022)
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties

including jail, and school-based mitigations for employees to safeguard staff and pupils

- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

Cyber-Bullying

Definition: Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that learners understand what it is and what to do if they become aware of it happening to them or others. We will ensure that learners know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The organisation will actively discuss cyber-bullying with learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Learning managers in the SCITT and Apprenticeships (including mentors, trainers etc) will discuss cyber-bullying in mentor meetings and in training sessions, and the issue will be addressed in the monthly Safeguarding Newsletter.

Staff encouraged to find opportunities to embed cyberbullying and e-safety into other learning opportunities.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support learners, as part of safeguarding training (see section 11 for more detail).

The organisation also sends information/leaflets on cyber-bullying to learners so that they are aware of the signs, how to report it and how they can support other learners who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among learners, the organisation will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Acceptable Use of the Internet in Schools

All learners, staff, volunteers and facilitators will be informed of the terms set out in the '**Acceptable Use Code of Conduct**' as outlined in appendices 1 and 2. Use of all schools' internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. The organisation monitors the websites visited by learners, staff, pupils, volunteers, facilitators and visitors (where relevant) to ensure they comply with the above.

Online Filtering & Monitoring:

All staff receive appropriate safeguarding and child protection training, including online safety which includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring. They understand that the designated safeguarding lead takes lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place.

Our online filtering and monitoring services are operated centrally by AIT and in constant review by the Trust. The system constantly filters out and monitors what children and adults can and can't access on academy devices.

Staff, learners and facilitators must report to the DSL if:

- They see or suspect learners are accessing unacceptable content;
- They know that unacceptable content can be accessed;
- They are teaching content that could cause a spike in logs;
- They are aware of failure or abuse of the system;
- They perceive there to be unreasonable restrictions;
- They become aware of abbreviations/misspellings that allow access to unacceptable content.

Learners using Mobile Devices in Schools

Learners are not permitted to use their mobile devices on school site beside in designated recreation areas, e.g. staffroom or where approved by the principal of the school under local guidance.

Staff using Work Devices outside School

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the organisation's terms of acceptable use, as set out in appendix 1. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT faculty support team. Work devices must be used solely for work activities.

How the organisation will respond to issues of misuse

Where a learner misuses the organisation's or a school's ICT systems or internet, we will assess the seriousness of the incident and the action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

The organisation will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police. Advice of the Trust Safeguarding Lead will be sought.

Training

All new staff members receive training, as part of the organisation's holistic safeguarding induction training, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation encompassed within.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Where appropriate, governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers, guest speakers and facilitators will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our Safeguarding Policy.

Monitoring Arrangements

The DSL and SALT Team logs behaviour and safeguarding issues related to online safety on MyConcern. This policy will be reviewed every year by the Director of SALT.

Appendix 1: ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: CODE OF CONDUCT FOR LEARNERS, VISITORS and STAFF

Learners, visitors and staff will read and follow the rules in the acceptable use code of conduct as outlined below.

When using a school's ICT systems and accessing the internet in school, or outside school on a work device learners, visitors and staff will:

- Not access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)

- Not use them in any way which could harm the school's reputation

- Not use any improper language when communicating online, including in emails or other messaging services

- Not install any unauthorised software, or connect unauthorised hardware or devices to the school's network

- Not share passwords with others or log in to the school's network using someone else's details

- Not leave a device unlocked when not directly near it

- Not take photographs of pupils without checking with their line manager first

- Not share confidential information about the school, its pupils or staff, or other members of the community

- Not access, modify or share data they are not authorised to access, modify or share

- Not promote private businesses, unless that business is directly related to the school

- Only use a school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of their role

- Be aware that the school will monitor the websites they visit and their use of a school's ICT facilities and systems.

- Take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

- Let the designated safeguarding lead (DSL) and ICT faculty support team know if a pupil informs them they have found any material which might upset, distress or harm them or others. Staff will also take the same steps if they themselves find any material which might upset, distress or harm them or others.

- Always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Processes for 2023-24: All learners, visitors and staff will be required to complete the google form.