GEORGE SPENCER ACADEMY

ETHOS OF EXCELLENCE

Online safety policy

The local governing body were notified of this policy on (DATE)

The policy will be reviewed on (DATE)

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

  deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. 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 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 children 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. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the senior designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Read and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The Principal

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

3.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, 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 school behaviour 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.

3.4 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 pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school'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
- 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 appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

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

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

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

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum (predominantly covered in the 'Computing' and 'Pesonal Development' curriculum)

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, they will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- 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
- How information and data is generated, collected, shared and used online
- 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

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE) [Google Classroom]. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's Director of Learning or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 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.)

6.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Learning managers will discuss cyber-bullying with their form groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Personal Development, and other subjects where appropriate.

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

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children 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 pupils, the school 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.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

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

8. Pupils using mobile devices in school

Pupils are not permitted to use their mobile devices in on school site. If mobile devices are brought into school pupils are aware that they will be confiscated by members of staff if they are seen or heard on school site.

9. 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 school's terms of acceptable use, as set out in appendix 2.

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.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. 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 school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

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

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 and deputies 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.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This policy will be reviewed every [2 years] by the Assistant Principal for Pupil Development and Well Being]. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Staff expectations and code of conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use code of conduct

Appendix 1: Acceptable use code of conduct (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: CODE OF CONDUCT FOR PUPILS AND PARENTS/CARERS

Pupils and parents/carers will read and follow the rules in the acceptable use code of conduct as outlined below.

When pupils and parents/carers the school's ICT systems (like computers) and get onto the internet in school they will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep their username and passwords safe and not share with others
- Keep private information safe at all times and not give their name, address or telephone number to anyone without the permission of the teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if they find any material which might cause them or others upset, distress or harm
- Always log off or shut down a computer when they have finished working on it.

They will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites.
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

Pupils will be aware that the school will monitor the websites they visit and that there will be consequences if they don't follow the rules.

Parents/carers will support the school in ensuring their child understands and adheres to these conditions.

Appendix 2: acceptable use code of conduct (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: CODE OF CONDUCT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

When using the school's ICT systems and accessing the internet in school, or outside school on a work device 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 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 the 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 the 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.

Appendix 3: Remote learning guiding principles

During the COVID-19 pandemic the vast majority of students had to access their education via remote learning. The following appendix sets out the academy's guiding principles where remote learning needs to be implemented.

Online Safety and Providing Off Site Teaching

All staff who interact with children and young people, including online, will continue to look out for signs a child may be at risk. Online teaching should follow usual principles for safe and acceptable use of technology. This includes, but is not limited to:

- Acceptable use of technologies
- Staff pupil/student online relationships
- Communication, including the use of social media
- Minimum expectations
- Online safety
- Essential rules for remote teaching

Communication

The academy will communicate basic information to parents where online learning platforms are being used which has included:

- Confirmation of online tools and or sites that the school will be using/if using (the platform currently being used is Google Classroom)
- Confirmation of what the child may be asked to do online
- Confirmation as to who their child will be interacting with online
- Confirmation as to whether other pupils will be able to access their child via the online platform
- Allowing the parent or carer the opportunity to voice any concerns
- The importance of not leaving the child alone during screen time
- Monitoring the search history
- Maintaining open communication with the child about online safety
- How to report a concern

The school website has an 'online safety' section providing Parents and carers provided with details/links to support services e.g. Internet Matters, LGFL, Net-aware, ThinkUKnow, Safer Internet Centre, and National Online Safety Website.

Learning Platform Guidance.

Google Classroom is the online learning platform that is used by the academy. This platform allows work to be set, completed and marked effectively whilst minimizing any online safeguarding risk. In line with the academy's acceptable use code of conduct (appendix 1) and safeguarding policy, online communication with students is done through regulated platforms (school email, google classroom). Staff will receive basic training in how to use google classroom.

Based on their knowledge of each individual group, teachers will consider the following when overseeing google classroom remote learning lessons and activities;

- Whether to allow pupils to post and comment in the communication 'Stream', or disable this function for them. (If pupil comments are disabled in the 'Stream', pupils will still be able to respond to feedback from their teacher on work they've handed in – they just won't be able to post on the 'Stream' page.)
- What students can talk about in posts and comments, (if allowed to)
- Whether to allow pupils to comment. Where comments are permitted, students will be informed that only relevant school work can be discussed in the 'Stream' and that they will be 'muted' if they post anything that's inappropriate or bullying in nature. (In addition, the teacher will follow the academy's behaviour policy protocols)

Video Conferencing

In certain, rare circumstances staff may need to utilize video conferencing. In these circumstances, permission must be granted by the Senior Leadership Team who will also provide support and guidance. The following principles must be followed where permission has been granted;

- Where possible, more than one member of staff is present
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background.
- Where possible, the conference/lesson/webinar etc should be recorded and backed up, so that if any issues were to arise, the video can be reviewed.
- Language must be professional and appropriate, including any family members in the background

The school recognizes that not all children will have access to a computer or internet facilities in the home, and has ensured that age appropriate resources have been provided for any child who needs them.