`

e-Safety Policy

Contents

1. Aims

Our Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, trustees and governors.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Trust Community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying, cyber-bullying: advice for headteachers and school staff and 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 students' 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.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Trust Board

The Trust Board has overall responsibility for monitoring this policy and holding the CEO and headteachers to account for its implementation. The Board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support our schools in meeting the standards.

The Governing Body will make sure all staff undergo online safety and cyber-security training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

All Governors/ Trustees will:

- Ensure that they have read and understood this policy

- Agree and adhere to the terms on acceptable use of the schools' ICT systems and the internet (Appendix 2)

3.2 The Headteacher / Head of School

The Headteacher / Head of School 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 Designated Safeguarding Lead (DSL) and deputies are set out in our Child Protection and Safeguarding Policy.

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

- Supporting the Headteacher / Head of School in ensuring that staff understand this policy and that it is being implemented consistently throughout the School
- Working with the Headteacher / Head of School, network team and manager and other staff, as necessary, to address any online safety issues or incidents
- Working with the ICT manager to make sure the appropriate systems and processes are in place and are reviewed on a regular basis – at least annually.
- 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's behaviour policies
- Updating and delivering staff training on online safety (Appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher / Head of School and/or Governing Body/ Trust Board

This list is not intended to be exhaustive.

3.4 The Trust's IT technical support team leader

The ICT Team leader is responsible for:

- Reviewing the DfE's filtering and monitoring standards, discussing with IT staff and service providers what needs to be done to support our schools in meeting the standards and providing reports to the CEO and Audit & Risk Committee as required and at least annually
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and for keeping students 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 ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online potential safety incidents the Team is aware of are logged and passed on to the DSL in the relevant school.
- Ensuring that any incidents of potential cyber-bullying the Team is aware of are logged and passed on to senior pastoral staff in the relevant school.

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
- Agreeing and adhering to the terms on acceptable use of ICT systems and the internet (Appendix 2), and ensuring that students follow the terms on acceptable use (Appendix 1)

- Working with the DSLs 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
- Ensure any incorrectly categorised sites are reported to the IT Service Desk so that they can be blocked/unblocked as necessary.

This list is not intended to be exhaustive.

3.6 Parents / carers

Parents / carers are expected to:

- Notify a member of staff or the Headteacher / Head of School of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the ICT systems and internet (Appendix 1)

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice https://www.legislation.gov.uk/ukpga/2010/15/contentscentre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the schools' ICT systems or internet will be made aware of this policy, when relevant, and are expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

Primary schools

In **Key Stage 1**, students will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Students in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing

Secondary schools

In **Key Stage 3**, students 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

Students in **Key Stage 4** may 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

All schools

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

The School will use assemblies and the support and guidance programme 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 /carers about online safety

The schools will raise parents' awareness of internet safety in letters or other communications home and in information via school websites. This policy will also be shared with parents / carers.

Online safety may also be covered during parents' evenings or other information evenings.

If parents / carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher / Head of School and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher / Head of School.

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.

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 schools will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers and form teachers will discuss cyberbullying with their tutor 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 cyberbullying. This includes personal, social, health and economic (PSHE) education, SMSC days, and other subjects where appropriate.

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

The schools also send and/or make available information/leaflets on cyber-bullying to parents / carers so that they are aware of the signs, how to report it and how they can support students who may be affected.

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

The DSLs 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 students' 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.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Synergy Multi Academy Trust recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Our schools will treat any use of AI to bully pupils very seriously, in line with local behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the School and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

Any use of Artificial Intelligence should be carried out in accordance with our AI Usage Policy.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers, trustees and governors are expected to sign an agreement regarding the acceptable use of the schools' ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the terms on acceptable use if relevant.

Use of the schools' 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, trustees, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in Section 11 and Appendix 1.

8. Pupils using mobile devices in school

Secondary pupils may bring mobile devices into school. However, such devices must not be used at any time during the school day, unless a class teacher has explicitly asked pupils to use their 'phones for a specific classroom purpose. Otherwise, 'phones that are seen or heard by a member of staff will be confiscated and only returned to the pupil's parents.

Primary pupils cannot bring mobile devices to school unless there is a specific SEND need and arrangement or is given express permission at the discretion of the Headteacher.

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. To keep data secure and to protect themselves, members of staff are strongly recommended to access sensitive data through the cloud. If a USB device must be used to take data home data relating to the School, it must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Synergy IT Support Team

Work devices must be used solely for work activities and PIN protection must be used on mobile devices.

10. New Software Installation and Data Connections

- Staff and students must **not install software or extensions** on Trust-issued devices except those available in the Software Centre (staff only).
- All software installation requests must be submitted by staff via the **Service Desk**.
- Staff must **not sign up for, trial, or authorise any new software or data connections** (including MIS or Azure integrations) without prior checks for:
    - **GDPR compliance** (Trust GDPR Coordinator)
    - **System compatibility** (Head of IT Systems and Services)
    - **Budget approval** (Trust Finance Team)
- This applies to **all software and data connections**, including Wonde or similar platforms, web apps, and mobile apps that store staff or student personal data.
- The Trust may refuse requests if similar software already exists, to ensure best value and avoid duplication.
- Failure to follow this process may result in withdrawal of the software or data connection.

11. How the school will respond to issues of misuse

Pupils

Where a pupil misuses the ICT systems or internet as set out in Appendix 1 below, we will follow the procedures set out in the School's Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Staff

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

When using the School's ICT Systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the School's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the School's Network using someone else's details

I will 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 my role.

I agree that the School will monitor the websites I visit, and my school device will be monitored for suspicious activity and safeguarding purposes.

I will 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 (GDPR) Policy.

I will let the Designated Safeguarding Lead (DSL) and Network/ ICT manager know if a student informs me s/he has found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the School's ICT Systems and internet responsibly and ensure that students in my care do so too.

I will adhere to established cybersecurity protocols and policies to ensure ongoing compliance with regulatory requirements and to protect the integrity, confidentiality, and availability of our systems and data.

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

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

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/ Trustees 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.

13. Monitoring arrangements

The school pastoral leaders in conjunction with the DSL will log behaviour and safeguarding issues related to online safety.

This policy will be reviewed every 3 years.

14. Links with other policies

This online safety policy is linked to our:

- Artificial Intelligence (AI) Policy
- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Disciplinary Procedures
- Data Protection (GDPR) Policy and Privacy Notices
- Complaints Procedure
- Staff Code of Conduct

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms or access programmes which may have chat-room elements within them
- 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
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone (Secondary and College only) or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors, trustees and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	