



---

# E-Safety Policy

Sir William Burrough Primary School

September 2024



|                                |                    |
|--------------------------------|--------------------|
| <b>Title:</b>                  | E-Safety Policy    |
| <b>Procedure Code:</b>         | X                  |
| <b>Source:</b>                 | X                  |
| <b>Document Owner:</b>         | Deputy Headteacher |
| <b>Review &amp; Update By:</b> | X                  |
| <b>Advisory Committee:</b>     | School Committee   |
| <b>Approval Committee:</b>     | X                  |
| <b>Date Approved:</b>          | X                  |
| <b>Date of Publication:</b>    | X                  |
| <b>Date of Next Review:</b>    | X                  |
| <b>Required on Website:</b>    | No                 |



## 0. Document Control

The table below contains the changes made between the different final editions of this document set for approval. This is to help provide information to those reviewing and approving the document of the changes being made.

| Document Edition | Section | Details of change |
|------------------|---------|-------------------|
|                  |         |                   |
|                  |         |                   |



## Contents

|                                                                        |    |
|------------------------------------------------------------------------|----|
| 0. Document Control .....                                              | 3  |
| 1. Definitions.....                                                    | 5  |
| 2. Scope of the Policy .....                                           | 6  |
| 3. Policy Aims and Ethos .....                                         | 6  |
| 4. Links to Legislation and Guidance Documents .....                   | 6  |
| 5. Roles and Responsibilities .....                                    | 7  |
| 6. Educating Pupils about Online Safety .....                          | 8  |
| 7. Educating Parents about Online Safety.....                          | 9  |
| 8. Personal Development/Online Safety Curriculum Content Overview..... | 9  |
| 9. Issues Affecting Online Safety .....                                | 9  |
| 10. Acceptable Use of the Internet in School .....                     | 10 |
| 11. Pupil Use of Mobile Devices in School .....                        | 10 |
| 12. Staff Using Work Devices Outside of School .....                   | 10 |
| 13. How the School Will Respond to Issues of Misuse .....              | 10 |
| 14. Training.....                                                      | 10 |
| 15. Monitoring Arrangement.....                                        | 11 |
| 16. Approval Signature .....                                           | 11 |
| 17. Appendix 1 – Key Members of Staff Referenced.....                  | 11 |
| 18. Appendix 2 – Links to Legislation & Guidance Documents .....       | 11 |
| 19. Appendix 3 – Procedures and Processes.....                         | 12 |



# 1. Definitions

The "Trust" refers to the company known as the University Schools Trust, East London and all Trustees, Governors and Staff who work within it.

A "School" refers to an individual academy within the Trust, as denoted by their Unique Reference Number. As such a 'school' may span one or several phases of education to the individual academies within the Trust. Depending on the context the term "School" may refer to a singular academy or to all of the academies within the Trust but as separate entities.

"Staff" refers to any individual who is employed by the Trust or who operates on the Trust's behalf, e.g. Trustees and Governors.

A "Parent" includes the natural or adoptive parent of a pupil as well as any non-parent / carer who has parental responsibility including being involved in the day-to-day care of a pupil.

A "Pupil" includes any incoming or current pupil at any School within the Trust. It also includes any individual who was previously a pupil at any School within the Trust and who has left within the appropriate timeframe for consideration as necessary, e.g. complaints. The term pupil is used as standard by the UST in its policy documents but can be replaced with the term "student" or "child" with no change of definition.

The "Headteacher" is defined as the individual who has ultimate responsibility for a school in line with UST strategy, approach, ethos and values. Individual schools may have alternative titles for this position such as Executive Headteacher or Principal.



## 2. Scope of the Policy

This policy applies to all relevant adults who are defined as:

- Trust staff, including any agency workers and contractors;
- Teacher trainees and other trainees/apprentices;
- Volunteers and any other individuals who work for or provide services on behalf of or for the school to include, but not limited to, all those detailed in the single central record (as amended);
- Trustees and governors
- Parents/carers

## 3. Policy Aims and Ethos

At Sir William Burrough Primary School, we aim 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.

## 4. Links to Legislation and Guidance Documents

### 4.1. Relevant Internal Policies

This policy should be read in conjunction with the following policies:

- Anti-Bullying Policy
- Behavioural Policy
- Child Protection and Safeguarding Policy
- Complaints Procedures Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Health and Safety Policy
- Mobile Phone Policy



## 4.2. Relevant External Documents

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. 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, the Equality Act 2010 and the Online Safety Act 2023. 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 and complies with our funding agreement and articles of association.

## 5. Roles and Responsibilities

### 5.1. Governors

The Governing Board will approve this policy and hold the Executive Headteacher/Headteacher to account for its implementation. Additionally, all governors will ensure that they have read and understand this policy.

### 5.2. Executive Headteacher/Headteacher

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

### 5.3. Deputy Headteacher (Curriculum), Pastoral Leader and ICT Curriculum Leader

The Deputy Headteacher (Curriculum), Pastoral Leader and Curriculum Leader are responsible for:

- Supporting the Executive Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Executive Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are 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.

### 5.4. Personal Development Lead (PD)

The PD lead is responsible for supporting the Deputy Headteacher Pastoral to update and deliver staff training for online safety and liaises with other agencies and/or external services if necessary.



## 5.5. Network Lead

The Network lead 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Renewing the software, which monitors staff and student online activities.

## 5.6. 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
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

## 5.7. Parents

Parents are expected to:

- Notify a member of staff or the Executive Headteacher of any concerns or queries regarding this policy
- Parents 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-centre/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>

## 5.8. 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.

## 6. Educating Pupils about Online Safety

At Sir William Burrough Primary School, pupils are taught about online safety as a part of the Computing curriculum. However, the safe use of social media and the internet is covered, where relevant, within other subjects. **Additionally, we deliver themed assemblies and wider**



curriculum enrichment to further raise pupils' awareness of the dangers that can be encountered online.

## 7. Educating Parents about Online Safety

At Sir William Burrough Primary School, parents are made aware of internet safety through parent workshops. Information about internet safety is shared via the school's website and parent forums, where relevant. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Phase Leaders.

## 8. Personal Development/Online Safety Curriculum Content Overview

In **Key Stage 1**, pupils are taught to:

- Use technology safely and respectfully, keep 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.

In **Key Stage 2**, pupils are taught to:

- Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

## 9. Issues Affecting Online Safety

### 9.1. Cyber-Bullying

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 the school's Anti-Bullying policy).

### 9.2. Preventing and Addressing Cyber-Bullying

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

As a part of student's personal development, teachers and student facing support staff are encouraged to actively discuss cyber-bullying with pupils where appropriate, explaining the reasons why it occurs, the forms it may take and what the consequences can be. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Anti-Bullying 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 Senior Leadership Team 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.

## 10. Acceptable Use of the Internet in School

Use of the school's internet must be for educational purposes only, or for fulfilling the duties of an individual's role, in line with the acceptable use of the internet policy. We monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

## 11. Pupil Use of Mobile Devices in School

The use of mobile phones by students is prohibited in the school. Any breach of this by pupils will result in confiscation of the mobile device as outlined line with the school's Mobile Phone policy.

## 12. Staff Using Work Devices Outside of 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 that 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. If staff have any concerns over the security of their device, they must seek advice from the ICT manager. Work devices must be used solely for work activities.

## 13. How the School Will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, action will be taken and will be proportionate depending on the individual circumstances, nature and seriousness of the specific incident. 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 staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## 14. 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).



## 15. Monitoring Arrangement

This policy will be reviewed by a member of the Senior Leadership Team. At every review, the policy will be shared with the governing board.

## 16. Approval Signature

Signature of (enter position e.g. Chair) \_\_\_\_\_

Print name \_\_\_\_\_

Date \_\_\_\_\_

## 17. Appendix 1 – Key Members of Staff Referenced

|                                     |                             |
|-------------------------------------|-----------------------------|
| Designated Safeguarding Lead        | Siobhan Fehim/Heather Coney |
| Deputy Designated Safeguarding Lead | David Hodges                |
| Executive Headteacher               | Siobhan Fehim               |
| Deputy Headteacher (Curriculum)     | Karyce Maitland             |
| ICT Curriculum Lead                 | Helen Green                 |
| Pastoral Leader                     | Heather Coney               |
| Personal Development Lead           | David Hodges                |
| Network Lead                        | Nathaniel Thompson (TQS)    |
| Chair of Governors                  |                             |
| Safeguarding Governor               |                             |

## 18. Appendix 2 – Links to Legislation & Guidance Documents

- [Keeping Children Safe in Education](#)
- [National Curriculum computing programmes of study](#)
- [Preventing and tackling bullying.](#)
- [Protecting children from radicalisation](#)
- [Online Safety Act](#)

### Additional Guidance Sources

- NSPCC: <http://www.nspcc.org.uk/>
- Childline: <http://www.childline.org.uk/pages/home.aspx>
- Anti-Bullying Alliance: <http://anti-bullyingalliance.org.uk/>
- Beat Bullying: <http://www.beatbullying.org/>



- Childnet International – making the internet a great and safe place for children. Includes resources for professionals and parents <http://www.childnet.com/>
- Thinkuknow (includes resources for professionals and parents) <https://www.thinkuknow.co.uk/>
- Safer Internet Centre <http://www.saferinternet.org.uk/>

## 19. Appendix 3 – Procedures and Processes

Appendix 3 should contain the procedures and processes associated with the policy if appropriate.

A common issue with policies is that the procedural detail tends to be contained within the policy leading to a merging of principles and application. The procedures and processes followed in implementing the policy should be separated out and located in the appendix or, if more appropriate, as an operational manual which can be reference in the Links to Legislation Guidance Documents section.