PolyMAT

E-SAFETY POLICY

Reviewed: May 2024

Approved: July 2024

Revision due: October 2025

Contents

1. AIMS

PolyMAT aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, Local Academy Committee members and trustees;
- 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 and filtering and monitoring.

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 Trust Board

The Trust Board has overall responsibility for monitoring this policy and holding the CEO and Headteachers to account for its implementation.

The Trust Board will appoint a Lead Trustee for Safeguarding, Attendance, Filtering and Monitoring, who takes responsibility for ensuring that the DfE's standards for Filtering & Monitoring[1] are being met across the Trust.

3.2 The Local Academy Committee

[1] Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Each school's Local Academy Committee will appoint a Link Academy Committee Member (ACM) for Safeguarding, Attendance, Filtering and Monitoring, who will take responsibility for ensuring that the DfE's standards for Filtering & Monitoring[2] are being met by the school, and report back to the Lead Trustee.

All Trustees and Local Academy Committee members will ensure that they have read and understand this policy and agree to adhere to the terms of PolyMAT's Acceptable Use of IT Systems Policy.

3.3 The Headteachers

Headteachers are responsible for ensuring that staff working in their schools understand this policy, and that it is being implemented consistently throughout their school.

3.4 The Designated Safeguarding Leads

Details of the school's DSL are set out in our child protection and safeguarding policy as well as 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 manager and other staff, as necessary, to address any online safety issues or incidents;
- 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 logged and dealt with appropriately in line with the school behaviour policy;
- Updating and delivering staff training on online safety (appendix 4 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 and/or Local Academy Committee.

This list is not intended to be exhaustive.

The Trust Safeguarding Lead will provide support and challenge to DSLs in their role of leading on online safety.

3.4 The ICT manager/ technicians

The school's ICT manager/ technicians are 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;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;

---

[2] Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

- 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;
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (see PolyMAT's Acceptable Use of IT Systems Policy).
- Working with the DSL to ensure that any online safety incidents are logged on sims 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

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 (see PolyMAT's Acceptable Use of IT Systems 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
- Hot topics - Childnet International
- Parent factsheet - Childnet International

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

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

- In **Key Stage 1**, pupils 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.
- In **Key Stage 2**, pupils 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**, they 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;
    - How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met;
    - How information and data is shared and used online;
    - What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context);
    - How to respond safely and appropriately to adult they may encounter (in all contexts, including online) whom they do not know.
- 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.

Schools 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

Schools will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and communication platforms. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings or other events.

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

Schools will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors or Class Teachers will discuss cyber-bullying with their class/ 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 cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, Local Academy Committee members, trustees 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).

Schools/ the Trust may also send information/leaflets on cyber-bullying to parents from time to time 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, schools will follow the processes set out in the school's behaviour policy. Where illegal, inappropriate or harmful material has

been spread among pupils, schools 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 PolyMAT's Complaints policy.

7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils, parents, staff, volunteers and Local Academy Committee members are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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, Local Academy Committee members and visitors (where relevant) to ensure they comply with the above.

More information is set out in PolyMAT's Acceptable Use of ICT Systems Policy.

8. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the school's ICT systems or internet, the school will follow the procedures set out in their policies on behaviour. 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 Trust's staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

9. 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 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.

Local Academy Committee members will receive training on safe internet use and online safeguarding issues as part of their annual safeguarding training.

More information about safeguarding training is set out in each school's child protection and safeguarding policy.

10. MONITORING ARRANGEMENTS

The DSL logs behaviour and safeguarding issues related to online safety for each school.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the Safeguarding & Standards Committee.

11. LINKS WITH OTHER POLICIES

This online safety policy is linked to:

- Each school's Child protection and safeguarding policy
- Each school's Behaviour policy
- PolyMAT's Staff disciplinary procedures
- PolyMAT's Data protection policy and privacy notices
- PolyMAT's Complaints procedure
- PolyMAT's Acceptable Use Of ICT Systems Policy

APPENDIX 1: ONLINE SAFETY TRAINING NEEDS – SELF AUDIT FOR STAFF

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
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, Local Academy Committee members, trustees and visitors? (see PolyMAT's Acceptable Use of ICT Systems Policy)	
Are you familiar with the school's acceptable use agreement for pupils and parents? (see PolyMAT's Acceptable Use of ICT Systems Policy)	
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?	