DUDLEY ACADEMIES TRUST

E-Safety Policy

Issue number:	002
Responsible:	Compliance & Safeguarding Officer
Approved by:	Chief Executive
Date:	April 2020
Review date:	April 2021

Contents

Aims

Dudley Academy Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and local advisory committee members.
- 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.

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 academies on preventing and tackling bullying 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 pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum In England Computing Programmes of Study.

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

Roles and Responsibilities

The Board of Trustees

The Trust Board has overall responsibility for monitoring this policy and holding the Chief Executive (CE) and Headteachers to account for its implementation.

The Trust board, through the CE, will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All Trustees and Local Advisory Committee members will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the trust's IT systems and the internet (appendix 2).

The Chief Executive

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

The Headteacher

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

The Designated Safeguarding Lead (DSL)

Details of the trust's DSL are set out in our Child Protection and Safeguarding policy.

The DSL takes lead responsibility for online safety in their individual academy, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy.
- Working with the Headteacher and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged (see appendix 4) 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 trust's Behaviour Policy.
- 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 to the Headteacher and/or Local Advisory Committee.

This list is not intended to be exhaustive.

Managed Service Provider

The managed service provider is responsible for helping the trust to ensure that it meets E-Safety technical requirements. The managed service provides a number of tools to the trust including:

- 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, including terrorist and extremist material.
- Ensuring that the trust's IT 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 trust's IT systems on a regular 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 4) and dealt with appropriately in line with this policy.

This list is not intended to be exhaustive.

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 trust's IT systems and the internet (appendix 2), and ensuring that pupils follow the trust's terms on acceptable use (appendix 1).

- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy.

This list is not intended to be exhaustive.

Parents/Carers

Parents/carers 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 trust's IT 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-centre/parents/carers-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents/carers-and-carers/hot-topics
- Parent factsheet, Childnet International: https://www.childnet.com/ufiles/parents-factsheet-11-16.pdf

Visitors and Members of the Community

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

Use of Social Media

Staff are not permitted to access social media websites from the trust's computers or other trust device at any time unless authorised to do so by a member of the senior leadership team. However, staff may use their own devices to access social media websites while they are in school, outside of lessons or other structured sessions. Excessive use of social media, which could be considered to interfere with productivity, will be considered a disciplinary matter.

Staff should assume that anything they write (regardless of their privacy settings) could become public so should ensure that they are professional, maintaining a clear distinction between their personal and professional lives.

Any use of social media made in a professional capacity must not:

- Bring the school into disrepute.
- Breach confidentiality.
- Breach copyrights of any kind.
- Bully, harass or be discriminatory in any way.
- Be defamatory or derogatory.

The Trust appreciates that staff may make use of social media in a personal capacity. However, staff must be aware that if they are recognised from their profile as being associated with the trust, opinions they express could be considered to reflect the trust's opinions and so could damage the reputation of the trust. For this reason, staff should avoid mentioning the trust or their academy by name, or any member of staff by name or position. Opinions should follow the guidelines above so as not to bring the trust into disrepute, breach confidentiality or copyright, or bully, harass or discriminate in any way.

General Considerations

When using social media staff and others should:

- Never share work log-in details or passwords.
- Keep personal phone numbers private.
- Never give personal email addresses to pupils or parents/carers.
- Restrict access to certain groups of people on their social media sites and pages.

Those working with children have a duty of care and are therefore expected to adopt high standards of behaviour to retain the confidence and respect of colleagues and pupils both within and outside of the trust. They should maintain appropriate boundaries and manage personal information effectively so that it cannot be misused by third parties for 'cyber-bullying', for example, or identity theft.

Staff should not make 'friends' of pupils because this could potentially be construed as 'grooming', nor should they accept invitations to become a 'friend' of any pupils.

Staff should also carefully consider contact with a pupil's family members because this may give rise to concerns over objectivity and/or impartiality.

Staff should keep any communications with pupils transparent and professional and should only use the trust's systems for communications.

If there is any doubt about whether communication between a pupil/parent/carer and member of staff is acceptable and appropriate a member of the senior leadership team should be informed so that they can decide how to deal with the situation.

Before joining the trust, new staff should check any information they have posted on social media sites and remove any post that could cause embarrassment or offence.

Further Information

NASUWT, (2012). *Social networking – guidelines for members.*
https://www.nasuwt.org.uk/article-listing/using-social-media-safely.html

Educating Pupils About Online Safety

Pupils will be taught about online safety as part of the personal, social, health and economic curriculum (PSHE) to develop their knowledge and understanding of the digital world.

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.

The safe use of social media and the internet will also be covered in other subjects where relevant (see Social Media policy).

The trust's academies 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.

Educating Parents/Carers About Online Safety

The trust's academies will raise Parent's/Carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with Parents/Carers.

Online safety will also be covered during Parents/Carers' 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 and the DSL.

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

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.

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 trust's academies will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying 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 cyber-bullying. This includes PSHE education, and other subjects where appropriate.

All staff, local advisory committee members 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 trust's academies also send 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 children who may be affected.

In relation to a specific incident of cyber-bullying, the trust will follow the processes set out in the trust's Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the trust will use all reasonable endeavors 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.

Examining Electronic Devices

Dudley Academies 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.

The Trust can apply an appropriate disciplinary penalty to pupils who refuse to co-operate with such inspections.

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 trusts 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 trust 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 Searching, screening and confiscation at school.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the trust's Complaints Procedure.

Acceptable Use of the Internet in Academy

It is a requirement for all Pupils, Parents/Carers, staff, volunteers and local advisory committee members to agree to the 'Acceptable Use' policy before access is allowed. As a

user you will see a 'pop-up' message advising of your obligations related to acceptable use of the computerised or networked environments.

Use of the trust'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 advisory committee members and visitors (where relevant) to ensure they comply with the above.

Pupils Using Mobile Devices in Academies.

Pupils may bring mobile devices into their academy, but are not permitted to use them during:

- Lessons.
- Tutor group time.
- Clubs before or after school, or any other activities organised by their academy.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the trust's Behaviour Policy, which may result in the confiscation of their device.

Staff Using Work Devices Off-Site

Staff members using a work device outside of their academy must not install any unauthorised software on the device and must not use the device in any way which would violate the trust'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 off-site. Any USB devices containing data relating to the trust must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the IT manager.

Work devices must be used solely for work activities.

How The Trust Will Respond to Issues of Misuse

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

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 Advisory Committee members 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.

Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

Appendix 1: Acceptable Use Agreement (Pupils and Parents/Carers)

Acceptable use of the trust's IT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the trust's IT systems and accessing the internet, whilst on trust premises, 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. – 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 trust'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 or other personal electronic device onto trust premises: – I will not use it during lessons, tutor group time, exams, clubs or other activities organised by the trust, without a member of staff'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 trust 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 trust's IT systems and internet responsibly.	
Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the trust's IT systems and internet when appropriately supervised by a member of trust staff. I agree to the conditions set out above for pupils using the trust's IT 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: Acceptable Use Agreement (Staff, Local Advisory Committee Members, Volunteers and Visitors)

Acceptable use of the trust's IT systems and the internet: agreement for staff, local advisory committee members, volunteers and visitors	
Name of staff member/local advisory committee member/volunteer/visitor:	
When using the trust's IT systems and accessing the internet, whilst on trust premises or outside of trust premises, 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 trust'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 trust's network using someone else's details	
I will only use the trust's IT systems and access the internet on trust premises, or outside trust premises on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the trust will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside of trust premises, and keep all data securely stored in accordance with this policy and the trust's Data Protection policy. I will let the designated safeguarding lead (DSL) and IT manager know if a pupil informs me they have 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 trust's IT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date**:

Appendix 3: 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 the trust?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the trust's Acceptable Use Agreement for staff, volunteers, local advisory committee members and visitors?	
Are you familiar with the trust's Acceptable Use Agreement for pupils and parents/carers?	
Do you regularly change your password for accessing the trust's IT systems?	
Are you familiar with the trust'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.	

Appendix 4: Online Safety Incident Report Log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**