Acceptable Use Policy (E-Safety)

The Diamond Learning Partnership Trust

Contents

1. Aims 3
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating pupils about online safety 6
5. Educating parents about online safety 7
6. Cyber-bullying 7
7. Acceptable use of the internet in Trust 9
8. Pupils using mobile devices in Trust 9
9. Staff using work devices outside Trust 10
10. How the Trust will respond to issues of misuse 10
11. Training 10
12. Monitoring arrangements 11
13. Links with other policies 11
Appendix 1: acceptable use agreement (pupils and parents/carers) 12
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors) 13
Appendix 3: online safety incident report log 14

ACCEPTABLE USE (E-SAFETY) POLICY

1. Aims

The Diamond Learning Partnership Trust 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 Trust 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 statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools and 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.

3. Roles and responsibilities

3.1 The CEO/Lead Executive Headteacher

The CEO/Lead Executive Headteacher is responsible for ensuring that this policy is being implemented throughout the Trust and that Headteachers and Local Governing Bodies (LGB's) understand this policy and are communicating it to all staff in their academies.

3.2 The Local Governing Body (LGB)

The LGB has overall responsibility for monitoring this policy and ensuring with the Headteacher that it is implemented.

The LGB 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 governors will:

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

3.3 The Headteacher

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

3.4 The Designated Safeguarding Lead

Details of the academies Designated Safeguarding Lead (DSL) and deputies are set out in each academies Child Protection and Safeguarding Policy.

The DSL takes lead responsibility for online safety in the 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 3) 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 Trusts' Behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in the academy to the Headteacher and/or LGB.

This list is not intended to be exhaustive.

3.5 ICT Service Provider

The ICT Service Provider who support the Trust ICT Services 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 Trust'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 Trust's ICT 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 3) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Trust behaviour policy.

This list is not intended to be exhaustive.

3.6 All staff and volunteers

All staff, (including agency staff), contractors 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 ICT 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.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Trust behaviour policy.

This list is not intended to be exhaustive.

3.7 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 Trust's ICT systems and internet (appendix 1).

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

3.8 Visitors and members of the community

Visitors and members of the community who use the Trust's ICT 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).

4. Educating pupils about online safety

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

In **Foundation Stage**, pupils will be taught to:

- Ask a teacher when they want to use the computers or iPad.
- Only use activities that a teacher has asked them to use.
- Take care of the computer.
- Ask for help from a teacher when they are not sure what to do.
- Tell a teacher if they see something on the screen that upsets them.
- Know that if they break the rules they might not be allowed to use a computer or iPad.

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.

Pupils 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.

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

Online safety will also be covered during parents' evenings.
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 should be raised with 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 Trust 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 Trust will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their pupils, 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, governors and volunteers (where appropriate) will 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 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 Trust will follow the processes set out in the Trust Behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the Trust 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

Trust 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 Trust 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 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 Trust complaints procedure.

7. Acceptable use of the internet in Trust

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the Trust's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the Trust's terms on acceptable use if relevant.
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, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices within Trust premises

Pupils may bring mobile devices into academies within the Trust, but are not permitted to use them during the school day. Pupils are required to submit their mobile device to the School Office at the start of the day and collect it at the end of the school day (each academy has their own arrangements for the collection and distribution of mobile phones at the start and the end of the school day – pupils must speak to their school office for further advice).

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 Trusts' Behavior policy, which may result in the confiscation of their device.

9. Staff using work devices outside of the Trust

Staff members using a work device outside of the Trust 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 outside of the Trust. 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 Trust ICT advisory and support service provider.

Work devices must be used solely for work activities.

10. How the Trust will respond to issues of misuse

Where a pupil misuses the Trust's ICT 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 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 Trust 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 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 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. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary policy
- Data protection policy and privacy notices
- Complaints procedure
- Electronic communication and information systems policy
- Monitoring policy

13. Review and monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 3.

This policy will be reviewed annually by the HR Office. This policy will remain in force until such time as a new one is formally agreed.

Adopted on: March 2021

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

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

Name of pupil:	
When using the Trust'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. • 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 into school: • I will not use it during lessons, tutor group time, clubs or other activities organised by the Trust/Academy. • I will not use my mobile phone during school time but instead submit the mobile phone to the school office upon arrival at school and collect it at the end of the school day. • 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 ICT systems and internet responsibly.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the Trust's ICT 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 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: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the Trust's ICT systems and the internet:

agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the Trust's ICT systems and accessing the internet in Trust, or outside Trust 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 ICT systems and access the internet in Trust, or outside Trust 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 Trust, 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 Headteacher 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 ICT 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 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**