DOVE HOUSE SCHOOL ACADEMY TRUST

Online Safety Policy

<table>
<tr><td colspan="3"><b>Policy Title</b></td><td colspan="3">Online Safety Policy</td></tr>
<tr><td colspan="3"><b>Author / Reviewer</b></td><td colspan="3">Data Protection Lead/ Senior Leadership Team</td></tr>
<tr><td colspan="3"><b>Governor Committee</b></td><td colspan="3">Delegated to Headteacher</td></tr>
<tr><td colspan="3"><b>Signed by Tom Pegler (Headteacher)</b></td><td colspan="3"></td></tr>
<tr><td><b>Reviewed</b></td><td>June 2020</td><td><b>Approved</b></td><td>July 2020</td><td><b>Next Review</b></td><td>July 2022</td></tr>
</table>

1. Aims

Dove House School Academy (DHSA) aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers 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 statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools 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 computing programmes of study.

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

3. Roles and responsibilities

3.1 The Board of Trustees

The Board of Trustees has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

All trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms of the Acceptable Use Policy by signing the Acceptable Use Agreement, if they use school equipment

3.2 The Headteacher

The Headteacher 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 (DSL)

Details of the school's DSL and Designated Safeguarding Deputies are set out in our Child Protection Policy.

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, IT 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's Anti-Bullying 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 school to the Headteacher and/or the Board of Trustees

This list is not intended to be exhaustive.

3.4 The IT Manager/ School's IT Provider

The IT manager in conjunction with the school's IT provider is responsible for:

- Ensuring appropriate filtering and monitoring systems are in place, which are updated on a regular basis, to 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 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 school's IT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors, agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms of the Acceptable Use Policy via the Acceptable Use Agreement
- Ensuring that any online safety incidents are logged via CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged via CPOM and dealt with appropriately in line with the school's Anti-Bullying policy.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to notify a member of staff or the 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

3.7 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. If appropriate, they will be expected to agree to the terms of the Acceptable Use Policy via the Acceptable Use Agreement.

4. Educating pupils about online safety

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

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 school 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 school will raise parents' awareness of internet safety in the following ways:

- Acceptable Use Agreements for pupils and employees
- Information included in letters, newsletters and our website
- Parents evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Social Media Policy

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 is defined as 'an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself.'

By cyber-bullying, we mean bullying by electronic media e.g.:

- Bullying by texts or messages or calls on mobile 'phones
- The use of mobile 'phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in on-line forums

6.2 Preventing and addressing cyber-bullying

Central to the school's anti-bullying policy is the principle that '*bullying is always unacceptable'* and that '*all pupils have a right not to be bullied*'.

The school also recognises that it must take note of bullying perpetrated outside school which spills over into the school; therefore once aware we will respond to any cyber-bullying we become aware of carried out by pupils when they are away from the site.

All staff have a responsibility to log any incidents of cyber-bullying on CPOMs, and to ensure that it is dealt with appropriately in line with the school's Anti-Bullying Policy.

Cyber-bullying may be at a level where it is criminal in character. It is unlawful to disseminate defamatory information in any media including internet sites.

Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.

The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

If we become aware of any incidents of cyberbullying, we will need to consider each case individually as to any criminal act that may have been committed. The school will pass on information to the police if it feels that it is appropriate or is required 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 the school complaints procedure.

7. Acceptable use of the internet in school

All staff, volunteers, and visitors (where relevant) are expected to sign the Acceptable Use Agreement as per the Acceptable Use Policy.

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.

The school will monitor the websites visited by pupils, staff, volunteers and visitors (where relevant) to ensure they comply with the above.

More information is set out in the Acceptable Use Policy.

8. Pupils using mobile devices in school

The use of mobile phones and other personal technologies by pupils is prohibited as set out in the Pupil Acceptable Use Agreement.

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 Policy.

Staff 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 IT manager.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the Pupil Acceptable Use Agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where staff issues of misuse arise, it may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal. See the Acceptable Use Policy for more information.

The school 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, which is delivered by the DSL, or a Deputy DSL. They will ensure new staff understand all relevant policies. This induction may be covered within the annual training if this falls at the same time; otherwise it will be carried out separately during the initial starting period.

All staff members will receive refresher training at least once each academic year as part of safeguarding training. Any update in national or local guidance, as well as other relevant updates, while be shared with all staff during briefings, and also captured in the next whole school training as required.

The DSL and deputies will undertake training at least every other year to enable them to fulfil their role.

Trustees will receive training as part of their safeguarding training.

Volunteers will receive appropriate training and updates, as appropriate.

12. Monitoring arrangements

This policy will be monitored by the Headteacher. The policy will be reviewed every 2 years by the Data Protection Lead and Senior Leadership Team.

The policy will be approved by the Headteacher.

13. Links with other policies

This online safety policy is linked to our:

- Child Protection Policy
- Safeguarding policy
- Acceptable Use Policy
- Anti-Bullying Policy