David Ross Education Trust

Broadening Horizons

Online Safety Policy

Document Management Information

Applicable to:

Contents

1.16 Each academy must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

2. Policy Scope

2.1 This policy

2.4 The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of academy.

3. The Trust's Policy on Online Safety

3.1 Policy Statements

Education – students

3.1.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore the central part of the academy's online safety provision. Children and young people need the help and support of the academy to recognise and avoid online safety risks and build their resilience.

3.1.2 The online safety curriculum will cover the four areas of risk:

content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

3.1.3 Online Safety education will be provided in the following ways:

A planned Online Safety programme will be provided as part of the curriculum and should be regularly revisited – this will cover both the use of ICT and new technologies in academy and outside academy.

Key Online Safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.

Students will be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.

Students should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside academy.

Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Rules for use of IT systems / internet will be displayed on log-on screens.

3.1.4 Staff should act as good role models in their use of ICT, the internet and mobile devices.

3.1.13 There will be regular reviews and audits of the safety and security of academy IT systems as part of the day to day operation of the IT Service.

3.1.14 Servers, wireless systems and cabling must be securely located and physical access restricted.

3.1.15 Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.

3.1.16 All users will have clearly defined access rights to academy IT systems. Details of the access rights available to groups of users will be recorded by the Trust IT Team.

3.1.17 The Trust processes for setting and managing passwords as set out in the IT Handbook will be adhered to.

3.1.18 Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security to their line manager.

3.1.19 If anyone is to be given unfiltered access at any time, this must be recorded in writing and agreed by the Online Safety Officer or Principal in agreement with the Head of IT & Data or a delegated IT Lead. The purpose and duration of the arrangement must be made clear. At the end of the planned period filtering must be restored to previous levels.

3.1.20 Any filtering issues should be reported immediately to the broadband provider or filtering provider by the IT Service staff working at the site, the contracted technical staff of the e Safety Officer.

3.1.30 Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of IT across the curriculum.

3.1.31 In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

3.1.32 External speakers can be useful as a catalyst to a discussion or to reinforce learning but are unlikely to be successful if they are the sole source of education or sanctions; in some cases, this approach can undermine settings ability to develop internal capacity to respond to concerns.

3.1.33

Students must not take, use, share, publish or distribute images of others without their permission.

Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

Students' / Pupils' full names will not be used anywhere on a website or social media, when in association with photographs.

Data Protection

3.1.39 The David Ross Education Trust collects and uses certain types of personal information about staff, students, parents, governors and other individuals who come into contact with the Trust in order to provide education and associated functions.

3.1.40 The Trust aims to ensure that all personal data is collected, stored and processed in accordance with General Data Protection Regulations (UK GDPR) and the provisions of the Data Protection Act 2018.

3.1.41 When processing personal data all staff and students will adhere to relevant policies and procedures, this ensures that personal data of staff, students, parents, governors and other individuals is processed fairly and lawfully, and in compliance with the data protection principles.

3.1.42 With regards to IT, IT is seen as beneficial to all members of the Trust in supporting learning, teaching, research, administration, and approved business activities of the Trust. The academy's IT Facilities provide a number of integral services and, therefore, any attempt to misuse a computer system could cause significant disruption to other users in the Trust. This could also lead to a breach of the data protection rights of individuals, resulting in harm to that individual and the Trust.

3.1.43 In accordance with the suite of Acceptable Use Polices, all users agree not to upload, download, post, email or otherwise transmit or store anything that:

is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libellous, invasive of anyone's privacy, hateful or racially, ethically or otherwise objectionable.

the user does not have the right to transmit.

infringes any patent, trademark, trade secret, copyright or other proprietary rights of any party.

is unsolicited or unauthorised(e)-356 (t)-2@ (ro)-6.( )T.5tro lawful,otn6 (t)-3 4[lib)2.2 (e)-3T: (e a)2.7 (n)

3.1.46 DSLs should be aware of national and local policy and procedures regarding responding to concerns relating to radicalisation.

3.1.47 The Government has also launched a website called ‘Educate Against Hate’, which is designed to equip school and college leaders, teachers and parents with the information, tools and resources they need to recognise and address extremism and radicalisation in young people, and this includes online issues.

Communications

3.1.48 The official academy email service may be regarded as safe and secure and is monitored. Staff (m)-6.3 (0 T(i

Use of video broadcasting e.g. YouTube

Responding to Incidents of Misuse

3.1.59 It is hoped that all members of the academy community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

3.1.60 If any apparent or actual misuse appears to involve illegal activity i.e.

example when developing curriculum approaches or making technical decisions. However, 4.10 **Online Safety Coordinator / Officer**

Takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the academy Online Safety documents.

Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.

Provides training and advice for staff.

Liaises with the Local Authority and Trust staff.

Liaises with Trust IT service staff.

Receives reports of online safety incidents and creates a log of incidents to inform future Online Safety developments.

4.11. **IT Service Staff**

The senior IT service staff member for the Academy is responsible for ensuring:

That the academy's IT infrastructure is secure and is not open to misuse or malicious attack.

Should be careful that "over blocking" does not lead to unreasonable restrictions as to what Sa[6 . - 0 a[eleieh 7 (an(e)-.1 p 6 (v5-1(.6 n) (u)2.r

x en6 (3)8c91O3 (a

S

Many academies will choose to combine the role of Child Protection Officer and Online Safety Officer

4.14. Students

Are responsible for using the academy IT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to academy systems. (NB. at KS1 it would be expected that parents / carers would sign on behalf of the pupils).

Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

N

Monitoring logs of internet activity (including sites visited) by the IT team and safeguarding staff at each academy,

Communication with Parents / carers,

Communication with Staff.

6. Related Policies

6.1. This policy is related to the following other Trust policies:

Safeguarding and Child Protection Policy

Acceptable Use Policy

Data Protection Policy

Social Media Policy

Anti-Bullying Policy

-