DJANOGLY CITY ACADEMY

E-Safety Policy

Author	J Amps
Last Reviewed	April 2017
Review Date	September 2018

E-Safety Policy

Creating a safe and well-structured e-learning environment

Djanogly City Academy

1: Background to our policy

a. What is e-Safety?

Children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis on a multitude of platforms and experience a wide range of opportunities, attitudes and situations. These opportunities can greatly enhance our way of sourcing information and learning about the world around us, but can occasionally place children, young people and adults in danger.

Some examples of this are:

- Bullying via social media or email
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

As an academy it is our 'duty of care' alongside that of parents and other members of the community to protect our children from these dangers.

The purpose of this e-safety policy is to outline what measures the academy takes to ensure that students can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate way.

b. Audience

This document is intended for public consumption as well as that of academy members, parents and local community and is a clear outward statement on the academy e-safety practices.

We at Djanogly City Academy must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. We are aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Our students should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good E-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role. (See Appropriate Use of IT Policy).

Breaches of an E-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, students and members of the wider school community across the country. We as a school are aware of our legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit primarily with the Principal and the Governing body.

2. General policy statement

Objectives

Here at Djanogly City Academy we aim to provide a safe, caring and friendly environment for all our students to allow them to learn effectively, improve their life chances and help them maximise their potential.

We take the safety of our students and staff very seriously. We believe that all students and staff have the right to be and feel safe whilst at school or on a school-run activity.

This policy should be read in conjunction with our behaviour and safeguarding policies. The academy will endeavour to ensure the e-safety of all academy members. It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this.

3. Whole academy responsibilities for e-safety

At Djanogly City Academy all members of staff and students are responsible for e-safety, responsibilities for each group include:

Students

- Participating in and gaining an understanding of e-safety issues and the safe responses from e-safety training sessions delivered through assembly and tutor sessions.
- Reporting any e-safety issue to the teacher, staff member or parent.
- Take responsibility for their own actions using the internet and communications technologies and adhere at all times to other ICT policies that outline acceptable and proper use of ICT facilities.
- Students are not permitted to use mobile phones on the school site

All Staff

- Have read and understood the DLT Acceptable Use Policy
- Have a clear understanding of e-safety issues and the required actions from e-safety training sessions delivered through INSET and CPD sessions.
- Reporting any e-safety issues to line managers as soon as the issue is identified.

- Take responsibility for their own actions using the internet and communications technologies and adhere always to other ICT policies that outline acceptable and proper use of ICT facilities.

Teaching Staff

- Educating students on e-safety through specific e-safety training sessions and re-enforcing this training in the day to day use of ICT in the classroom.

Network and ICT staff working within the academy

- Ensure that appropriate technological solutions are in place to ensure e-safety as well as possible whilst still enabling students to use the internet effectively in their learning.
- Ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored safely. In addition, securing and preserving evidence of any e-safety breach.
- Checks and audits all systems to ensure that no inappropriate data is stored or is accessible.
- Support the review of this and other policies to ensure that the academy continues to protect all parties through continuous reflection.
- Monitors the technology systems which track student internet use to detect e-safety breaches.
- Assists in the resolution of e-safety issues.

4. How the academy ensures e-safety in the classroom

a. Educating students on e-Safety

A clear objective of the academy is to educate students in safe use of ICT and the internet. We feel this is one of the best ways to minimise the potential for any e-safety issues to occur.

Students have and will receive specific e-safety lessons aimed at ensuring that:

- Students know the e-safety risks that exists and how to identify when they are at risk.
- Students know how to minimise e-safety risks by using e-safe practices when online.
- Students know when, how and to whom to report instances when their e-safety may have been compromised.
- Students know that they are in an environment that encourages them to report e-safety issues without risk of reprimand, humiliation or embarrassment.

As we continue to develop our e-safety provision the academy may use resources such as the Think U Know programme produced by the governments Child Exploitation and Online Protection (CEOP) centre as one of the primary education tools.

This can currently be found at: https://www.thinkuknow.co.uk/teachers/

In addition to this specific training all members of staff will have a duty to reinforce e-safety practices wherever possible and will offer students advice and support in the classroom where minor e-safety incidents have occurred.

b. How e-safety is monitored

- The ICT support team will actively monitor the students ICT activity using a monitoring system which can flag potential e-safety issues.
- The ICT team will periodically review internet access logs to track any websites which could potentially present an issue.
- The ICT team will periodically review internet and network logs to track trends and use the information to look at ways of improving e-safety.
- Teaching staff will directly monitor the students ICT and internet use in the classroom and flag concerns to the ICT team and work with them to record and action and concerns

c. How technology helps

The academy employs many different technologies to help to ensure e-safety for all the academy members;

- The academy will use internet filtering to block inappropriate content and in addition block websites which are irrelevant to the student's programme of study and are considered time wasting or counterproductive to the learning environment.
- The academy will use a system which can track all student activity on the academy's computers. This system will help flag potential e-safety issues which will be monitored and then can be investigated by senior staff.
- The academy will restrict which activities the students can perform using ICT and the internet through systems security policy and access controls to the networks we operate.

Teaching staff will work with the ICT team to use control mechanisms to attempt to limit the applications and web sites which the students can visit whilst using ICT within a lesson.

5. How the Academy will respond to issues of misuse

The following are provided for example only. Whenever a student infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Principal and Governing Body.

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to sending electronic messages to friends
- Use of unauthorised instant messaging / social networking sites

Possible Sanctions: Confiscation of the device /referred to tutor, head of year or senior staff /contact with parent/ removal of Internet access rights for a period in school /detention

Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned and device confiscated during the school day
- Accidentally accessing offensive material and not notifying a member of staff of it

Possible Sanctions: Confiscation of the device /referred to tutor, head of year or senior staff /contact with parent/ removal of Internet access rights for an extended period of time/ exclusion

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

Possible Sanctions: Confiscation of the device /referred to tutor, head of year or senior staff including the Principal /contact with parent/ removal of Internet access rights for an extended period/ exclusion /referral to police

Category D infringements

- Continued sending of emails or electronic messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

Possible Sanctions: Confiscation of the device /referral to senior staff or Principal /contact with parent/ removal of Internet access rights for an extended period of time/ exclusion /referral to police

How will students be informed of these procedures?

- Students will be instructed about responsible and acceptable use and given strategies to develop 'safe behaviours'.
- The school's e-safety policy along with other whole school policies is available to parents through the school website and will be brought to their attention when they join.
- Further information can also be found on our school website at: http://www.djanogly.notts.sch.uk/page.php?p=esafety

6. Working with parents and the community

It should be clear from this policy document that Djanogly City Academy believes that the use of information and communication technologies in schools brings great benefits across the curriculum. Clearly many academy students will also have access to ICT and the internet at home, often without some of the safeguards that are presents within the academy environment. Therefore parents/carers/guardians must often be extra vigilant about their child's e-safety at home.

Highlighting E-Safety issues and setting out our plans to ensure appropriate, effective and safer use of electronic communications for our students aims to support a safe and structured learning experience for our students.

One of the goals of the academy is to support parent's role in providing an e-safe environment for their children to work in outside the academy.

The academy will do this in two ways;

- Raise awareness through student sessions in school
- Provide information to parents on e-safety and the importance of and how to monitor ICT use in the home through information published on our website at: http://www.djanogly.notts.sch.uk/page.php?p=esafety

Useful e–Safety programmes include:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Orange Education: www.orange.co.uk/education
- Safe: www.safesocialnetworking.org

Schools e-Safety Audit

This self-audit has been completed by the member of the Senior Leadership Team (SLT). Staff that could contribute to the audit include: Designated Child Protection Coordinator, SENCO, ICT Network Team and Principal.

Has the school an e-Safety Policy?		Yes
Date of latest update:		April 2017
Date of future review:		Sept 2018
The school e-safety policy was agreed by governors on:		
The policy is available for staff to access at:	http://www.djanogly.notts.sch.uk/page.php?p=policies	
The policy is available for parents/carers at:	http://www.djanogly.notts.sch.uk/page.php?p=policies	
The responsible member of the Senior Leadership Team is: J. Amps		
The governor responsible for E-Safety is: Chair of Governors		
The Designated Child Protection Coordinator is: See safeguarding policy		
Are all stakeholders (e.g. students, staff and parents/carers) able to make recommendations and will they be consulted with when updating the school e-safety policy?		
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)		
Do all members of staff sign an Acceptable Use Policy on appointment?		
Are all staff made aware of the schools expectation around safe and professional online behaviour?		
Is there a clear procedure for staff, students and parents/carer to follow when responding to or reporting an e-Safety incident of concern?		
Have e-safety materials from CEOP, Childnet and UKCCIS etc. been obtained?		
Is e-Safety training provided for all students		
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all students?		
Are staff, students, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?		
Is personal data collected, stored and used according to the principles of the Data Protection Act?		
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)?		
Has the school filtering been designed to reflect educational objectives and been approved by SLT?		
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?		
Does the school log and record all e-Safety incidents, including any action taken?		
Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?		

E-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

EiS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com