DJANOGLY CITY ACADEMY

E-Safety Policy

2025-26

DJANOGLY CITY ACADEMY

E-Safety Policy 2025-26

Background to our Policy 3

General Policy Statement 4

Whole Academy Responsibilities for E-Safety 4

How the Academy Ensures E-Safety in the Classroom 5

How the Academy Will Respond to Issues of Misuse 7

Generative AI 8

Cyber Attack 9

Working with Parents and the Community 9

E-Safety Contacts and References 10

Background to our Policy

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.

- Content – Scholars may see inappropriate, harmful or illegal content online such as radicalisation, misogyny or self-harm.
- Contact – There are risks posed when interacting with others online such as child-on-child pressure, interacting with adults who pose as children or grooming.
- Conduct - Online behaviour that will cause harm such as cyberbullying or the sharing of semi-nude/nude images.
- Commerce – Scholars may be exposed to online gambling, phishing or inappropriate advertising.

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 scholars can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate way.

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 scholars 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 scholars 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, scholars and members of the wider school community across the country. We as an academy 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.

General Policy Statement

Objectives

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

We take the safety of our scholars and staff very seriously. We believe that all scholars and staff have the right to be and feel safe whilst at the academy or on an academy-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.

Whole Academy Responsibilities for E-Safety

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

Scholars

- Participating in and gaining an understanding of e-safety issues and the safe responses from e-safety training sessions delivered through assembly and values 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.
- Not being permitted to use mobile phones on the academy site.

All staff

- Have read and understood the DLT IT 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 scholars 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 scholars 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.
- Monitors the technology systems which track scholar internet use to detect e-safety breaches.
- Assists in the resolution of e-safety issues.

Designated Safeguarding Lead

- Takes responsibility for understanding the filtering and monitoring systems and processes in place.
- Regularly reviews the system in place and responds to any safeguarding concerns that are identified through ICT misuse.
- Raising awareness of the 4Cs of online safety: Content, Contact, Conduct and Commerce.

How the Academy Ensures E-Safety in the Classroom

Educating scholars on e-safety

A clear objective of the academy is to educate scholars 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.

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

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

All members of staff will have a duty to reinforce e-safety practices wherever possible and will offer scholars advice and support in the classroom where minor e-safety incidents have occurred.

How e-safety is monitored

- The ICT support team will actively monitor the scholars ICT activity using LGFL and SENSO as our filtering monitoring systems 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 scholars ICT and internet use in the classroom and flag concerns to the ICT team and work with them to record and action any concerns

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 scholars programme of study and are considered time wasting or counterproductive to the learning environment.
- The academy will use a monitoring system which can track all scholar 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 the DSL.
- The academy will restrict which activities the scholars 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 scholars can visit whilst using ICT within a lesson.

How the Academy Will Respond to Issues of Misuse

The following are provided for example only. Whenever a scholar infringes the e-Safety policy, the final decision on the level of sanction will be at the discretion of the Principal.

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 send electronic messages to friends
- Use of unauthorised instant messaging / social networking sites

Possible sanctions:

Confiscation of the device /referred to values teacher, achievement lead or senior staff /contact with parent/ removal of Internet access rights for a period in the academy /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 academy day
- Accidentally accessing offensive material and not notifying a member of staff of it

Possible sanctions:

Confiscation of the device /referred to values teacher, achievement lead 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 values teacher, achievement lead 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 academy 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 scholars be informed of these procedures?

- Scholars will be instructed about responsible and acceptable use and given strategies to develop 'safe behaviours' in their ICT/Computer Science lessons and through the SRE programme.
- The academy's e-safety policy along with other whole academy policies is available to parents through the academy website and will be brought to their attention when they join.
- Further information can also be found on our academy website at:

http://www.djanogly.notts.sch.uk/E-Safety/

Generative AI

Generative AI tools are now widespread and easy to access. Staff, scholars and parents/carers may be familiar with generative AI such as ChatGPT.

DCA recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

DCA will treat any use of AI to bully scholars very seriously, in line with our school's behaviour policy.

Scholars are prohibited from using and accessing AI while studying at DCA.

Staff must be aware of the risks of using AI tools and should ensure a DPIA has been completed before using any new tools with an understanding of the Large Language Model (LLM) that is processing the data.

Individuals must not enter personal details including names into any form of AI tool.

Cyber-attack

Where a cyber-attack may compromise any processing of data/information in school.

The Djanogly Learning Trust (DLT) have a Cyber Response Plan Implemented to mitigate the impact of a Cyber Security incident.

In the event of a cyber-attack, DCA will:

- Act swiftly and decisively with the Head of IT at the Trust, to mitigate the impact.

The Djanogly Learning Trust will:

- Isolate affected systems to prevent the spread of the attack
- Network Manager/IT department to back up data
- Ensure the backups are held offline
- Systems for restoring services and recovering data from the backups are tested and reliable
- Contact the National Cyber Security Centre (NCSC)
- Contact the local law enforcement and Action Fraud
- Inform the DfE by emailing: securityenquiries@education.gov.uk

For exams and assessments, any work completed in an exam situation is stored in a secure location which is not accessible from outside the Academy and only by designated staff members internally.

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 the academy brings great benefits across the curriculum. Clearly many academy scholars will also have access to ICT and the internet at home, often without some of the safeguards that are present 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 scholars aims to support a safe and structured learning experience for our scholars.

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 scholar sessions in the academy
- 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:

Djanogly City Academy - E-Safety

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

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

Date revised: This policy was last reviewed and revised in December 2024

Review date: October 2025