THE FITZROY ACADEMY

Online Safety Policy 2022.23

NEWREFLEXIONS
Where every child matters

Aims

The Fitzroy Academy aims to:

- Have robust processes in place to ensure the online safety of all pupils and staff;
- 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.

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 on files of pupils' electronic devices where they believe there is a "good reason" to do so.

Roles and responsibilities

<u>The Head Teacher</u>

The Head Teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

<u>The Head Teacher/designated safeguarding lead</u>

The Head Teacher, as Designated Safeguarding Lead, takes lead responsibility for online safety in school, in particular:

- in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- working with the IT manager and other staff, as necessary, to address any online safety issues or incidents;
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately;
- updating and delivering staff training in online safety;
- liaising with other agencies and/or external services if necessary.

This list is not intended to be exhaustive.

<u>The IT manager</u>

The IT manager 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 school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- conducting regular security and firewall checks and monitoring the school's ICT systems;

- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
- ensuring that any incidents of cyberbullying are dealt with appropriately in line with the school Behaviour Policy.

This list is not intended to be exhaustive.

All staff

All staff, including agency staff, are responsible for:

- maintaining an understanding of this policy;
- implementing this policy consistently;
- agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet;
- working with the Head Teacher to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy;
- ensuring that any incidents of cyber-bullying are dealt with appropriately.

This list is not intended to be exhaustive.

Educating pupils about online safety

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

- identify where to go for help and support when they have concerns about content or contact on the Internet or other online technologies;
- recognise acceptable and unacceptable behaviour;
- identify a range of ways to report concerns about content and contact
- 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;
- understand how changes in technology affect safety;
- know how to report a range of concerns.

Within the context of The Fitzroy Academy provision and the related SEN of the learners, the above outlines will need to be personalised and adapted to the needs of the learners and reflective of their independence and ability to apply and process information.

Cyber-Bullying 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.

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.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread amongst pupils, the school 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.

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.

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.

Acceptable use of the internet in school

All staff are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet.

Use of the school's internet must be for educational purposes only, or for the purposes of fulfilling the duties of an individual's role.

The school will monitor the websites visited by pupils and staff to ensure they comply with the above.

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but staff will monitor their use closely at all times. Ideally it is best if pupils do not bring these into school.

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 that would violate the school's terms of acceptable use.

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 school.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

How the school will respond to issues of misuse

Where a staff member misuses the school'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 school will consider whether incidents, which involve illegal activity or content, or otherwise serious incidents, should be reported to the Police.

Training

All new staff members will receive training, as part of their induction, on online safeguarding issues including cyberbullying 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 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.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Procedure

Reviewed: August 2022
Next Review due: August 2023