drb Ignite Multi Academy Trust

Cyberbullying Policy

Trust Vision

The drb Ignite Multi Academy Trust has been established through a shared belief that lives can be transformed by what goes on in schools. We believe that the process of teaching and learning shapes futures.

All pupils achieve the highest standard of educational outcomes regardless of circumstance or background.

Introduction

The Trust believes that any bullying incident should be treated as a child protection concern when there is reasonable cause to believe that a child is suffering or likely to suffer significant harm.

Therefore, this Policy should be read in conjunction with a number of other Trust policies:

- Anti-bullying Policy
- Behaviour Policy
- Safeguarding and Child Protection Policy and Procedures
- Staff Code of Conduct
- Data Protection (GDPR) Policy.

Definition of cyberbullying

The Trust defines cyberbullying as:

> *the use of electronic communication, particularly mobile phones and the internet, to bully a person, typically by sending messages of an intimidating or threatening nature*

It can take a number of different forms:

- threats and intimidation
- harassment
- *cyber-stalking* e.g. repeatedly sending unwanted texts or instant messages
- sexting e.g. sending and receiving sexually explicit messages, primarily between mobile phones
- vilification/defamation
- exclusion/peer rejection
- impersonation
- unauthorised publication of private information/images
- *trolling* i.e., abusing the internet to provoke or offend others online

Children and adults may be reluctant to admit to being the victim of cyberbullying. It can be an extension of face-to-face bullying, with technology providing the bully with a further route to harass their target.

It differs from other forms of bullying in several significant ways. It:

- facilitates a far more extreme invasion of personal space. Cyberbullying can take place at any time
- intrudes into spaces previously regarded as safe and personal
- has potential for anonymity on the part of the bully. This can be extremely distressing for the victim
- has potential for the bully to play to a larger audience, so the scale and scope of cyberbullying can be greater than for other forms of bullying
- can disproportionately amplify the negative effect on the victim through knowledge that data is in the world-wide domain, even though the bully may feel his/her actual actions had been no worse than conventional forms of bullying
- can quickly draw in others as accessories due to the difficulty of controlling electronically circulated messages e.g. by passing on a humiliating picture or message a bystander becomes an accessory to the bullying.
- can take place between peers and across generations. Teachers can be victims and age and size are not important.

Cyberbullying and the law

Bullying in whatever form is **never** acceptable. The Trust recognises its duty to safeguard all pupils and staff and to provide a safe, healthy environment for everyone.

In education law

- The Education and Inspections Act 2006 (EIA 2006) outlines some legal powers which relate more directly to cyberbullying. Headteachers have the power to *such an extent as is reasonable* to regulate the conduct of pupils when they are off the school site.
- The Act also provides a defence for staff in confiscating items such as mobile phones from pupils.

In civil and criminal law

- There is not a specific law which makes cyberbullying illegal, but it can be considered a criminal offence under several different acts including Protection from Harassment Act (1997), Malicious Communications Act (1988), Communications Act (2003) Obscene Publications Act (1959) and Computer Misuse Act (1990).

Preventing cyberbullying

As with all forms of bullying, the Trust believes the best way to deal with cyberbullying is to prevent it happening in the first place. There is no single solution to the problem of cyberbullying, but the Trust will do the following to impose a comprehensive and effective prevention strategy.

Trust schools will:

- ensure that all pupils are given clear guidance on the use of technology safely and positively both in school and beyond including how to manage their personal data and how to report abuse and bullying online.
- provide annual training for parents/carers on online safety and the positive use of technology
- ensure the Trust's Acceptable Use Policy and associated guidelines are reviewed annually
- provide annual training for staff on associated policies and procedures
- plan and deliver a curriculum on online safety which builds resilience in pupils to protect themselves and others whilst online.

In Trust schools **the Designated Safeguarding Lead** will take overall responsibility for the co-ordination and implementation of cyberbullying prevention and response strategies.

The Designated Safeguarding Lead will:

- ensure that all incidents of cyberbullying, both inside and outside school, are dealt with immediately and will be managed and/or escalated in line with the procedures set out in the Trust's Anti-bullying Policy and Safeguarding and Child Protection Policy/Procedures.
- ensure that all staff know that they need to report any issues concerning cyberbullying to the Designated Safeguarding Lead.
- ensure that all staff are aware of the Prevent Duties.
- provide training so that staff feel confident to identify pupils at risk of being drawn into serious situations like terrorism in order for them to challenge extremist ideas and to know how to make a referral when a pupil maybe at risk.
- ensure that parents/carers are informed, and attention is drawn annually, to the Cyberbullying Policy as part of the school's responsibilities relating to safeguarding pupils and their welfare.
- ensure that all staff are aware of their responsibilities by providing clear guidance for staff on the use of technology within school and beyond. All staff should sign to say they have read and understood the Staff Code of Conduct which relates to bullying.

Senior leaders and IT support teams will:

- ensure adequate safeguards are in place to filter and monitor inappropriate content and alert the Designated Safeguarding Lead to any safeguarding concerns
- ensure that visitors are given clear guidance on the use of technology in school. This includes how to report any safeguarding issues to the Designated Safeguarding Lead. Visitors will be given highly restricted guest accounts which will not allow any access to personal data and are clear that misuse of the system will result in access to the system being withdrawn.
- ensure all staff are familiar with and comply with the following GDPR policies:
    - Data Protection Policy
    - Acceptable ICT Use Policy
    - Access Control Policy
    - Individual User Agreement
    - Information Security Policy
    - Password Policy

School Business Managers will:

- ensure the school manages personal data in line with statutory and GDPR requirements. The Trust is aware of its duties under the Data Protection Act (1998) and GDPR requirements. Careful consideration will be given when processing personal information so that the individual's privacy is respected where it needs protection. Access to personal information will only be given to those who need it. The principles of the Data Protection Act will be applied when processing, collecting, disclosing, retaining or disposing of information relating to a pupil or member of staff.

Trustees will:

- appoint a local member with responsibility for safeguarding who will work with the school Designated Safeguarding Lead to ensure that policies and practices relating to safeguarding including the prevention of cyberbullying are implemented effectively.

Guidance for Staff

Guidance on safe practice in the use of electronic communications and storage of images is contained in the Staff Code of Conduct. The Trust will deal with inappropriate use of technology in line with the Staff Code of Conduct. Inappropriate use will be taken seriously and could result in disciplinary procedures.

Reporting a concern

If a cyber-bullying incident is suspected or reported to you, the following protocol should be followed:

Mobile Phones

- Ask the pupil to show you the mobile phone
- Note clearly everything on the screen relating to any inappropriate text message or image, including the date, time and names
- Make a transcript of a spoken message, again recording date, times and names
- Tell the pupil to save the message/image
- Inform the Designated Safeguarding Lead immediately and pass them the information you have collected

Computers

- Ask the pupil to find on-screen the material in question
- Ask the pupil to save the material
- Print off the offending material straight away
- Make sure you have got all pages in the right order and that there are no omissions
- Inform the Designated Safeguarding Lead and pass them the information that you have
- Agreed procedures to interview pupils and to take statements will then be followed in line with the Trust's Safeguarding and Child Protection policy and procedures

Use of Technology in School

All members of the school community are expected to take responsibility for using technology positively.

- All staff are expected to sign to confirm they have read and understood the Trust's Acceptable Use Policy.
- All staff are expected to sign to confirm they have read and understood the Staff Code of Conduct
- All staff are expected to have read and understood *Guidelines for Staff when Children are using Digital Devices*
- All pupils are expected to have been taught to use digital devices safely and in age appropriate ways.

Guidance for Parents/Carers

It is vital that parents/carers and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be considered to be cyber-bullying. Parents/carers must play their role in taking responsibility for monitoring their child's online life.

- Parents/carers can help by making sure their child understands the Trust/school policy and, above all, how seriously the Trust/school takes incidents of cyber-bullying.
- Parents/carers should also explain to their children the legal issues relating to cyber-bullying.
- If parents/carers believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving the offensive text on their computer or on their child's mobile phone) and make sure they have all relevant information before deleting anything.
- Parents/carers should contact the school as soon as possible.
- If an incident falls in the holidays the Trust/school reserves the right to take action against bullying perpetrated outside the school both in and out of term time.

E-Safety at Home

Several sites offer helpful advice to parents/carers, particularly with respect to how they can best monitor their child's use of the computer at home. These are communicated to parents/carers.

- www.thinkyou.know.co.uk/parents
- www.saferinternet.org.uk
- Vodafonedigitalparenting.co.uk
- www.childnet.com
- www.anti-bullyingalliance.org.uk
- www.nspcc.org.uk
- www.cyberangels.org
- Digizen

Monitoring and review	Trust Board Headteachers DSLs
Links	Safeguarding Policy and Procedures Behaviour Policy Acceptable Use Policy
Staff responsible	Headteachers DSLs Trust Safeguarding Leads
Committee responsible	Trust Board
Date approved	**February 2020**
Reviewed	February 2020
Next review*	February 2022
Sign off by Chair of Trust	 Date: February 2020

*Please note that should there be any changes/further national guidance issued relevant to this Policy, it will be updated accordingly prior to the review date shown above and referred to the next Trust Board meeting.

Change Management

Issue No.:	Change date:	Change description:
1.0	July'18	Initial release
2.0	Sept'18	Rebranded
2.0	Nov'18	Signed off and released
3.0	Nov'19	Checked, no content changes, signed off
4.0	Feb' 20	Reviewed and signed off