drb Ignite Multi Academy Trust

Cyberbullying Policy

drb Ignite Multi Academy 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.

Vision

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

Background

The Trust and its schools recognise 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.

This policy should be read in conjunction with the Trust's Anti-bullying Policy, Behaviour Policy, Safeguarding and Child Protection Policy and Procedures, the Staff Code of Conduct and Data Protection (GDPR) Policy.

Cyberbullying

Cyberbullying is defined 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

Children and adults may be reluctant to admit to being the victim of cyberbullying. 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

It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target.

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

- by facilitating a far more extreme invasion of personal space. Cyberbullying can take place at any time
- intruding into spaces that have previously been 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 very rapidly to a larger audience so the scale and scope of cyberbullying can be greater than for other forms of bullying
- through knowledge that the data is in the world-wide domain, disproportionately amplifying the negative effect on the victim, even though the bully may feel his/her actual actions had been no worse than conventional forms of bullying
- difficulty in controlling electronically circulated messages means more people can get drawn in as accessories. By passing on a humiliating picture or message a bystander becomes an accessory to the bullying.
- the profile of the bully and target can be different to other forms of bullying as cyberbullying can take place between peers and across generations. Teachers can be victims and age and size are not important.
- many cyberbullying incidents can themselves act as evidence, so it is important the victim saves the information.

Cyberbullying and the law

Bullying is **never** acceptable, and the Trust fully recognises its duty to protect all pupils and staff and to provide a safe, healthy environment for everyone.

Education Law:

- The Education and Inspections Act 2006 (EIA 2006) outlines some legal powers which relate more directly to cyberbullying. Head teachers 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.

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 as a minimum to impose a comprehensive and effective prevention strategy.

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, Behaviour Policy and Safeguarding and Child Protection Policy/Procedures.
- ensure that all specific school policies relating to safeguarding, including cyberbullying are reviewed and updated regularly in line with Trust requirements
- 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 children at risk of being drawn into terrorism, to challenge extremist ideas and to know how to make a referral when a child is at risk.
- ensure that parents/carers are informed, and attention is drawn annually to the cyberbullying policy so that they are fully aware of the school’s responsibility 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.

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 school's Acceptable Use Policy, Guidelines for Staff when pupils are using Digital Devices, Pupil Use of Digital Devices and are reviewed annually
- provide annual training for staff on the above policies and procedures
- provide annual training for staff on online safety
- plan and deliver a curriculum on online safety which builds resilience in pupils to protect themselves and others online.

School IT Support Teams along with the Headteacher will:

- ensure adequate safeguards are in place to filter and monitor inappropriate content and alert the Designated Safeguarding Lead to safeguarding issues.
- ensure that visitors to the school 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 that any misuse of the system will result in access to the system being withdrawn.
- ensure all staff are familiar with and hence comply with the following GDPR compliant 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 new GDPR requirements. The Trust is aware of its duties under the Data Protection Act (1998) and new 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 the 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.

The Executive Governance Groups will:

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

Guidance for Staff

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

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

Mobile Phones

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

Computers

- Ask the pupil to get up 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 a member of the Senior Leadership team and pass them the information that you have
- Normal procedures to interview pupils and to take statements will then be followed particularly if a child protection issue is presented.

Use of Technology in School

All members of the school community are expected to take responsibility for using technology positively. As well as training, the following is in place:

- All staff are expected to sign to confirm they have read and understood the 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 taken through and understood Children's Use of Digital Devices

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 seen to be cyber-bullying. Parents/carers must play their role and take responsibility for monitoring their child's online life.

- Parents/carers can help by making sure their child understands the school's policy and, above all, how seriously the school takes incidents of cyber-bullying.
- Parents/carers should also explain to their children 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 the incident falls in the holidays the 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. Here are some parents/carers might like to try:

- 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	Headteachers DSLs
Links	Safeguarding Policy and Procedures Behaviour Policy Acceptable Use Policy
Staff responsible	Headteachers DSLs
Committee responsible	Trust Board
Date approved	**November 2018**
Reviewed	November 2018
Next review	November 2019
Sign off by Chair of Trust	Date: November 2018

*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