Gastrells
Community Primary School

"a flying start to a
life of learning"

Gastrells Community Primary School

E-Safety Policy

MISSION STATEMENT

At Gastrells Community Primary School, our mission is to promote pupil success by inspiring and developing their knowledge, interests, physical and mental wellbeing, and a love of learning in a child-centered, inclusive and empowering environment.

Approved by Standards Committee

Last reviewed on: June 2024

Next review due by: June 2026

Contents

Introduction

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical building.

This policy document is drawn up to protect all parties – the students, the staff and the school – and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Aims

The aims of our Computing and E-Safety policies are:

- To provide a varied, enjoyable, and challenging Computing curriculum for all children at Gastrells, which meets the requirements of the National Curriculum programs of study for Computing.
- Have processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.

Roles and Responsibilities

The Governing Body

The Governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

All governors will:

- Ensure that they have read and understood this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (see Acceptable Useage Policy).

The Headteacher

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

The Designated Safeguarding Lead

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, computing team 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 in line with the school behaviour policy.

- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the governing board.

If any issues arise with the technology itself then staff should liase with Computing Leads (Kayleigh Grace-Fox & Chloe Woolls) and then the DSL.

<u>Educating pupils about online safety</u>

Pupils in KS1 & KS2 will be taught about online safety as part of the curriculum using 'Project Evolve'.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact. The safe use of social media and the internet will also be covered in other subjects where relevant.

<u>Educating parents about online safety</u>

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be available to parents. Where possible, the school will organise external speakers to provide presentations to parents to help keep them up to date with online safety.

<u>Staff</u>

All staff should be familiar with the school's policy including:

- Staff use of email
- Safe use of the internet including use of internet-based communication services such as instant messaging and social network
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs and use of websites
- e-bullying/cyberbullying procedures
- their role in providing e-safety education for pupils

<u>Types of risk</u>

Online safety means keeping children safe from 4 types of risk, known as the C's.

These are:

<u>Content</u>

Content is anything posted online - it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact

Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

Conduct

Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

Commerce

Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applies to staff.

Online safety often overlaps with other safeguarding issues. For example, children may show potential signs of being sexually abused online. Abuse can take place completely online, or online and physically.

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. (See also the school behaviour policy)

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.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

This issue will be addressed as part of online safety in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

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 among 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.

Person Responsible: Computing Subject Leader