



GREENWOOD ACADEMIES TRUST

Online Safety Policy Statement

Version: 8.0 Approval Status: Approved

Document Owner:	Director of Safeguarding
Last Reviewed Date:	January 2023

Table of Contents

1. Policy Introduction and Aims 3

2. Policy Scope 3

3. Roles and Responsibilities 4

4. Management of the technical environment 6

5. Actions and sanctions 6

1. Policy Introduction and Aims

At the Greenwood Academies Trust we recognise that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. However, these technologies have created a landscape of challenges and dangers that is constantly changing. In order to ensure that all Trust environments provide a safe place for learning, we adhere to the following principles:

- Online safety is an essential part of safeguarding and the Trust has a duty to ensure that all pupils and colleagues are protected from potential harm online
- Online safety education is important to both our pupils and our staff. Pupils should be empowered to build resilience and to develop strategies to prevent, manage and respond to risk online

The purpose of the online safety policy is to:

- Safeguard and protect all members of the Trust's community¹ online
- Identify approaches to educate and raise awareness of online safety throughout the community
- Enable all colleagues to work safely and responsibly, to model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns.

The breadth of issues classified within online safety are considerable and ever evolving, but can be broadly categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content; for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, unsolicited and inappropriate commercial advertising and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other gain
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example: making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes or semi-nudes and/or pornography, sharing other explicit images and online bullying)
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and pupils need to be aware of the risks associated with publishing digital images on the internet.

Children must be made aware that such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

It is also common practice for employers to carry out internet searches for information about potential and existing employees as part of Safer Recruitment procedures.

2. Policy Scope

This policy applies to all colleagues including teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the Trust (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers. It applies to access to Trust systems and the internet. It also applies to the use of technology, using devices provided by the Trust or personal devices.

¹ The use of the word community throughout this document refers to pupils and staff

The policy also applies to online behaviour which may take place outside the Trust, but is linked to membership of our academies such as online bullying. Academies will deal with such behaviour using this policy and associated behaviour and discipline policies.

3. Roles and Responsibilities

The following section outlines roles and responsibilities of individuals and groups within the Trust and individual academies in relation to online safety. The Trust recognises that *all* members of the community have important roles and responsibilities to play with regard to online safety:

3.1 The Trust Board

The Trust Board is responsible for monitoring the overall effectiveness of this policy. The Board will receive regular information about online safety issues via the relevant committee.

3.2 The Executive Leadership Team (ELT)

ELT are responsible for ensuring effective implementation and review of this policy. ELT will ensure that the Trust Board receive regular information about online safety issues via the relevant committee. ELT will set expectations regarding Trust Quality Assurance.

3.3 Principals:

The Principal will be accountable for the following although, they may delegate day-to-day leadership responsibilities to other members of the academy leadership team and:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with Trust expectations as described in this policy and national recommendations and requirements
- Ensure the academy follows Trust policies and practices regarding online safety, information security and data protection
- Ensure that online safety is embedded within the whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety
- Support the DSL by ensuring they have sufficient training, time, support and resources to fulfil their responsibilities
- Ensure that all staff complete regular, up to date and appropriate online safety training²
- Be aware of what to do in the event of a serious online safety incident, and ensure the use of Trust reporting channels for online safety concerns
- Receive regular reports from the DSL on online safety to ensure appropriate action is being taken in their academy

3.3 Designated Safeguarding Leads (DSLs) will:

- Take day to day responsibility for online safety
- Promote an awareness of and commitment to online safety throughout the academy community
- Ensure there is an identified online safety co-ordinator who facilitates training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the academy community, as appropriate
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident

² Details of online safety resources and support networks are available in Keeping Children Safe in Education 2022 p.110

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1101454/Keeping_children_safe_in_education_2022.pdf

- Respond in a timely way to reported concerns regarding pupil internet usage, taking relevant action where required

3.4 Online Safety Co-ordinators will:

- Ensure they keep up to date with national, local and Trust updates regarding online safety³
- Facilitate training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the academy community, as appropriate
- Act as the named point of contact on all online safety issues, and liaise with other members of staff or other agencies, as appropriate
- Keep the online safety component of the curriculum under review, in order to ensure that it remains up to date and relevant to pupils

3.5 All staff will:

- Read, adhere to and help promote the Trust Online Safety policy, Acceptable Use Policy, Social Media Policy, Staff Code of Conduct, Managing Allegations against an Adult Working Within the Trust Policy and any other relevant Trust policies and guidance
- Take responsibility for the security of Trust/Academy systems and the data they use, or have access to
- Model safe, responsible and professional behaviours in their own use of technology
- Have an up to date awareness of a range of online safety issues and how they may be experienced by pupils through ensuring their training is up to date
- Know when and how to escalate online safety issues

3.6 Pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) will:

- Have an up to date awareness of a range of online safety issues and how they may be experienced by pupils through the Academy curriculum offer
- Read and adhere to relevant academy online safety documents
- Take responsibility for keeping themselves and others safe online
- Report to a trusted adult, if there is a concern online

3.7 Parents and carers:

We believe that our work in the area of online safety will be greatly enhanced if we have the engagement and support of all our parents and carers, it is therefore recommended that they are aware of the importance of:

- Encouraging their children to adhere to academy online safety documents
- Supporting the school in online safety approaches by discussing online safety issues with their children and reinforcing appropriate, safe online behaviours at home
- Modelling safe and appropriate use of technology and social media, including seeking permission before taking and sharing digital images of pupils other than their own children
- Identifying changes in behaviour that could indicate that their child is at risk of harm online
- Seeking help and support from their child's individual academy, or other appropriate agencies, if they or their child encounter risk or concerns online

³ Further resources can be found here <https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools>

- Using school systems, such as learning platforms, and other network resources, safely and appropriately
- Taking responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

3.8 External groups:

- Any external individual/organisation will be expected to read, understand and implement all relevant online safety documentation and expectations prior to being given individual access to any Trust network and ensure they adhere to these at all times

4. Management of the technical environment

The Trust commissions the services of Our Learning Cloud (OLC) to ensure the Trust and individual academies' technical infrastructure is secure, is not open to misuse or malicious attack and has all the necessary controls in place, such as web filtering and password protection to reduce the risk of online safety issues arising. OLC also maintain the Trust internet filtering system to ensure ongoing monitoring of staff and pupil use of the internet.

5. Actions and sanctions

Online activity of all staff and pupils across the Trust is monitored by the Safeguarding Directorate via the Trust Internet monitoring system maintained by OLC.

DSLs within academies are informed of incidents of misuse by pupils as reported via the Online Filtering System. Any incidents of this type should be dealt with through normal behaviour and disciplinary procedures with consideration given to safeguarding concerns in every incident.

Identified concerns relating to the online activity of Trust staff will be followed up through the relevant Directorate.

If you witness/become aware of any online safety issues you must refer this to the Academy DSL or your line manager.