



GREENWOOD ACADEMIES TRUST

E-Safety Policy Statement

Version: 7.0 Approval Status: Approved

Document Owner:	Graham Feek
Classification:	External
Review Date:	01/05/2017
Effective from:	14 May 2015

Table of Contents

1. Scope of the Policy	3
2. Roles and Responsibilities.....	3
3. Use of Digital and Video Images	4
4. Social Media – Protecting Professional Identity	4
5. Unsuitable or Inappropriate Activities/Responding to Incidents of Misuse	4
6. Academy Actions and Sanctions.....	4

Introduction

The Greenwood Academies Trust recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use.

Our approach is to implement appropriate safeguards within the Trust and its academies, while supporting staff and students to identify and manage risks independently and with confidence. Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the Trusts' e-safety provision. Children and young people need the help and support of the academy to recognise and avoid e-safety risks and build their resilience. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard students, we will do all that we can to make our students and staff stay e-safe and to satisfy our wider duty of care. E-safety will be a focus in all areas of the curriculum and staff should take active steps to reinforce e-safety messages across the curriculum.

This E-safety policy should be read alongside other relevant Trust policies, including Safeguarding, Acceptable Use, Anti Bullying and the Disciplinary procedure.

1. Scope of the Policy

This policy applies to all members of the Academy community (including staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of Academy ICT systems, both in and out of the Academy.

The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the Academy but are linked to membership of the Academy. The 2011 Education Act increased these powers with regard to the searching for and confiscation of electronic devices and the deletion of data. In the case of both Acts, action can only be taken over issues covered by the published Behaviour Policy.

The Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

2. Roles and Responsibilities

The following section outlines the broad e-safety roles and responsibilities of individuals and groups within the Academy. The E-safety Procedure Document sets out the detailed requirements of these roles.

THE TRUST BOARD

The Trust Board is responsible for the overall effectiveness of the policy. This will be carried out by the Trust Board receiving regular information about e-safety incidents and monitoring reports. A member of the Trust Board has the role of Safeguarding Champion, which includes e-safety.

THE PRINCIPAL AND SENIOR LEADERS

The Principal has a duty of care for ensuring the safety of members of the Academy community and therefore has overall responsibility for e-safety in the Academy.

E-SAFETY CO-ORDINATOR

The Principal delegates much of the day to day responsibility for e-safety to an E-Safety co-ordinator who may often also be the Designated Safeguarding Lead (DSL). The E-Safety Co-ordinator has a leading role in establishing, reviewing and implementing the Academy e-safety procedures, providing training and advice for staff and liaising with outside bodies in relation to e-safety issues.

PUPILS

Pupils should be aware of the significant risks of exposing themselves or others to personal harm or danger because of inappropriate use of IT and digital media and should manage their use of IT to minimise these risks.

Pupils are responsible for using the Academy IT systems in accordance with their Digital Citizen Contract (DCC) and generally understanding the importance of adopting good e-safety practice when using digital technologies in and out of the Academy.

PARENTS AND CARERS

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way.

The Academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the Academy website and information about national and local e-safety campaigns and literature.

STAFF

Staff are responsible for ensuring that they have an up to date awareness of e-safety matters and of the current Academy e-safety policy and practices and have read, understood and signed the staff Acceptable Use Policy (AUP). Staff that work directly with pupils are also responsible for helping them understand the importance of e-safety and how they can reduce exposing themselves to risk.

COMMUNITY USERS

Community Users who access Academy systems as part of the wider Academy provision, will be expected to sign a Community User AUP before being provided with access to the Academy systems.

IT DIRECTORATE

The IT Directorate is responsible for ensuring that the Academy's technical infrastructure is secure and 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 e-safety issues arising. The IT Directorate also monitor staff and pupil usage of the internet.

3. Use of Digital and Video Images

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. Such images may provide avenues for cyber 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 common for employers to carry out internet searches for information about potential and existing employees. The Academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

4. Social Media – Protecting Professional Identity

The staff AUP and pupil DCC set out the expectations about the appropriate use of social media by staff, pupils and parents/carers. This guidance must be followed in order to ensure that staff, pupils and parents/carers do not engage in any activity which may cause them to breach acceptable standards of conduct.

5. Unsuitable or Inappropriate Activities/Responding to Incidents of Misuse

The staff AUP and pupil DCC set out the requirements in relation to reporting unsuitable or inappropriate activities. Where such activities also raise a safeguarding concern, the Trust's Safeguarding Policy, and relevant procedures must be followed. The E-Safety Procedure Document sets out how any suspected illegal activity or images should be dealt with by the Academy.

6. Academy Actions and Sanctions

It is more likely that the Academy will need to deal with incidents that involve inappropriate rather than illegal misuse. Incidents will be dealt with as soon as possible in a proportionate manner and members of the Academy community will be made aware that incidents have been dealt with. Incidents of misuse will be dealt with through normal behaviour and disciplinary procedures.