WEST GRANTHAM
Church of England Primary Academy

DIOCESE OF SOUTHWELL & NOTTINGHAM
MULTI ACADEMY TRUST

E-Safety Policy

Approved by the Board of Directors – 05 July 2022

Policy:	E Safety Policy
Approved by:	
Date:	May 2022
Review cycle:	Annual

VERSION CONTROL

VERSION	DATE	AUTHOR	CHANGES
2020	March 2020	DO – IT Director	No changes
2021	April 2021	DO – IT Director	No changes
2022	May 2022	BD & TTL	Changed I.T. Director to Trust Technical Lead (TTL) IT Technical Guidance and Cyber Security Policy added to Links with Other Policies Paragraphs numbered throughout the policy

E-Safety Policy

Introduction

1. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in academies are bound. Academies must, through their E-Safety Policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside the academy. The policy also forms part of the Trust's/academy's protection from legal challenge, relating to the use of digital technologies.

Scope

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

Rationale

3. The Education and Inspections Act 2006 empowers Principals/Headteachers to such extent as is reasonable, to regulate the behaviour of pupils/students 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 trust/academy. The 2011 Education Act increased these powers with regard to the searching for and 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. In addition the Counter Terrorism and Securities Act 2015 requires academies to ensure that children are safe from terrorist and extremist material on the internet.

4. 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.

Roles and Responsibilities

<u>Board of Directors</u>

5. The Board of Directors is accountable for the effective operation of the e-safety policy overall. Regular reports around safeguarding in the academies are received by the Board. These include reference to e-safety where appropriate.

<u>Local Governing Body</u>

6. The responsibility for the effective operation of the policy in the academy has been delegated to the Local Governing Body who will monitor and review its operation at the academy by receiving regular reports about e-safety incidents and monitoring

filtering and change control logs. It is suggested that the safeguarding governor includes the monitoring of e-safety within their remit.

Principal/Headteacher

7. The responsibility for the 'day to day' management and operation of the e-safety policy has been delegated to the Principal/Headteacher. The Principal/Headteacher is responsible for:
   - ensuring that all the staff have read and understand the policy;
   - ensuring training and advice is provided for staff;
   - ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

Staff

8. All 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;
   - they have read, understood and signed the Academy Acceptable Use Policy;
   - they report any suspected misuse or problem to the Principal/Headteacher;
   - online safety issues are embedded in all aspects of the curriculum and other activities;
   - pupils/students understand and follow the E-Safety Policy and Academy Acceptable Use Policy;
   - pupils/students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations appropriate to the age of the pupils/students;
   - they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
   - in lessons where internet use is pre-planned students/pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

The Designated Safeguarding Lead

9. Should be trained in E-Safety issues and be aware of the potential for serious child protection/ safeguarding issues to arise from:
   - sharing of personal data;
   - access to illegal / inappropriate materials;
   - inappropriate on-line contact with adults/strangers;
   - potential or actual incidents of grooming;
   - cyber-bullying.

Trust Technical Lead/Technical Staff/ICT Support Service

10. that the relevant people named in the above sections are effective in carrying out their e-safety responsibilities

Pupils/students

11. Pupils/Students are responsible for:

- using the academy digital technology systems in accordance with the Pupil/Student Acceptable Use Policy;
- having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations appropriate to their age;
- understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- knowing and understanding policies on the use of mobile devices and digital cameras, taking and the use of images and on cyber-bullying;
- understanding the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's E Safety Policy covers their actions out of school, if related to their membership of the academy.

Parents/Carers

12. Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way and will be encouraged to support the academy in promoting good online safety practice and following guidelines on the appropriate use of:
    - digital and video images taken at school events;
    - access to parents' sections of the website/Learning Platform and on-line pupil/student records;
    - their children's personal devices in the academy (where this is allowed).

Objectives

13. To educate pupils/students to take a responsible approach to e-safety;
14. To help and support children and young people to recognise and avoid online safety risk and build their resilience;
15. To reinforce e-safety messages and make e-safety a focus in all areas of the curriculum;
16. To provide information and awareness to parents to help them understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local online safety campaigns/literature;
17. To provide e-safety training and guidance for staff to ensure they understand their responsibilities;
18. To ensure that children are safe from terrorist and extremist material on the internet as required under the Counter Terrorism and Securities Act 2015.

Links with Other Policies

19. The E-Safety Policy must be read in conjunction with the other following policies:

ICT Policy
IT Technical Guidance
Cyber Security Policy
Bring Your Own Device (BYOD) Policy
Data Protection Policy
Social Media Policy
Policy for Child Protection to Safeguard the Welfare of Children

Guidance for Implementation

Curriculum

20. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:
    - A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited;
    - Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities;
    - Pupils/Students should be taught in all lessons to be critically aware of the materials/ content they access on-line and be guided to validate the accuracy of information;
    - Pupils/students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
    - Pupils/students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making;
    - Pupils/students should be helped to understand the need for the Pupil/student Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside the academy;
    - Staff should act as good role models in their use of digital technologies, the internet and mobile devices;
    - Pupils/students should be guided to sites checked as suitable for their use in lessons where internet use is pre-planned;
    - Processes should be in place for dealing with any unsuitable material that is found in internet searches;
    - Staff should be vigilant in monitoring the content of the websites the young people visit where Pupils/students are allowed to freely search the internet;
    - Pupils/students with special educational needs should be appropriately supported according to their specific needs and their personal understanding of the e-safety risks;

Parents/Carers

21. The academy should seek to provide information and awareness to parents and carers through:
    - Curriculum activities
    - Letters, newsletters, web site, Learning Platform
    - Parents / Carers evenings / sessions
    - High profile events / campaigns e.g. Safer Internet Day
    - Reference to the relevant web sites / publications

Staff

22. The academy should ensure that:
    - An audit of the e-safety training needs of all staff should be carried out and a planned programme of formal e-safety training made available to staff which is regularly updated and reinforced;
    - All new staff should receive online safety training as part of their induction programme including ensuring that they fully understand the trust E-Safety Policy and academy Acceptable Use Policy;
    - Staff identify e-safety as a training need within the performance management process where appropriate;

- The nominated person receives regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations;
- The E-Safety Policy and its updates are presented to and discussed by staff in staff meetings/INSET days;
- The nominated person provides advice/guidance/training to individuals as required.

Directors/Governors

23. The Trust/academy should ensure that:
    Directors/members of the Local Governing Body take part in e-safety training/awareness sessions, particularly those who are members of any subcommittee/group involved in technology/online safety/health and safety/safeguarding.

Monitoring of Internet Usage

24. Academy technical staff regularly monitor and record the activity of users on the academy technical systems and users are made aware of this in the Acceptable Use Policy.

Review

25. The application and outcomes of this policy will be monitored to ensure it is working effectively using:
    - Logs of reported incidents
    - Monitoring logs of internet activity (including sites visited) / filtering
    - Internal monitoring data for network activity
    - Surveys/questionnaires of Pupils/students, parents/carers and staff.

26. This policy is reviewed annually by the Trust in consultation with the recognised trade unions.