Tadcaster Grammar School
e-Safety policy

Contents

Approved by Headteacher: November 2019
Approved by Governing Body: January 2020
Next Review Date: January 2022
SEP/22: POLICY CURRENTLY UNDER REVIEW BY STARMAT

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Tadcaster Grammar School with respect to the use of ICT-based technologies
- Safeguard and protect the children and staff of Tadcaster Grammar School
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use
- Have clear structures to deal with online abuse such as cyber-bullying which are cross referenced with other school policies
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Minimise the risk of misplaced or malicious allegations made against adults who work with students

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites and those which promote extremist views
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming and inappropriate communication
- 'Sexting' (sending and receiving of personally intimate images), and other forms of inappropriate communication
- 'Upskirting' and any similar taking of images without consent
- Cyber-bullying in all forms
- Identity theft and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information or publishing of images/video without consent
- Digital footprint and online reputation
- Health and well-being (amount of time spent online)
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of Tadcaster Grammar School community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the school 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 school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the relevant policies.
The school 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

Key Responsibilities

This school

- Plans Internet and mobile technology use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Will remind all members of the school community about their responsibilities through this e-Safety policy, and an Acceptable Use Agreement which every member will sign
- Provides, as part of the induction process, all new staff (including those on university/college placement and work experience) with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies
- Ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons
- Runs a rolling programme of advice and guidance, including:
    - Information leaflets; in school newsletters; on the school website
    - Demonstrations, practical sessions held at school
    - Suggestions for safe Internet use at home
    - Provision of information about national support sites for parents

Headteacher

- Takes overall responsibility for e-safety provision
- Takes overall responsibility for data and data security
- Ensures the school uses an approved, filtered Internet Service, which complies with current statutory requirements
- Has responsibility for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant
- Is aware of procedures to be followed in the event of a serious e-safety incident.
- Receives regular monitoring reports from the E-Safety Coordinator
- Ensures that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager)

E-Safety Coordinator

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Promotes an awareness and commitment to e-safeguarding throughout the school community
- Ensures that e-safety education is embedded across the curriculum
- Liaises with school ICT technical staff
- Communicates regularly with SLT and the designated Safeguarding Governor to discuss current issues, review incident logs and internet filtering systems
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- Ensures that an e-safety incident log is kept up to date
- Facilitates training and advice for all staff
- Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection 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 and use of social media

Safeguarding Governor

- Ensures that the school follows all current e-safety advice to keep the children and staff safe
- Approves the e-Safety Policy and reviews the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.
- Supports the school in encouraging parents and the wider community to become engaged in e-safety activities

Computing Curriculum Leader

- Oversees the delivery of the e-safety element of the Computing curriculum
- Liaises with the e-safety coordinator regularly

Network Manager

- Will report any e-safety related issues that arise, to the e-safety coordinator.
- Ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which usernames and passwords are unique to each user, regularly changed, and are distributed to users securely
- Ensures that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date
- Ensures the security of the school ICT system, and that the storage of all data will conform to UK data protection requirements, and comply with GDPR (General Data Protection Regulations)
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems
- Ensures that access controls / encryption exists to protect personal and sensitive information held on school-owned devices and that any computer, laptop or mobile device loaned to staff by the school is used solely to support their professional responsibilities
- Ensures that he / she keeps up to date with the school's e-safety policy and technical information in order to carry out their e-safety role and to inform and update others as relevant
- Ensures that the use of the school's network is regularly monitored in order that any misuse / attempted misuse can be reported to the e-Safety Coordinator for investigation / action / sanction
- Ensures appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- Keeps up-to-date documentation of the school's e-security and technical procedures
- Ensures that there is a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. and that this is applied and updated on a regular basis.

e-Development Manager

- Ensures that all data held on students on the School's VLE and Google G-Suite for Education applications is adequately protected
- Ensures that the use of the school's G-Suite and all its applications are regularly monitored in order that any misuse / attempted misuse can be reported to the e-Safety Coordinator for investigation / action / sanction

Teachers

- Embed e-safety issues in all aspects of the curriculum and other school activities
- Supervise and guide students carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant)
- Ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

Students

- should read, understand, sign and adhere to the Student Acceptable Use Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials
- know what action to take if they or someone they know feels worried or vulnerable when using online technology
- know and understand school policy on the taking / use of images and on cyber-bullying.
- take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- know and understand school policy on the use of mobile phones and handheld devices understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school

All Users must:

- read, understand and promote the school's e-safety policies and guidance
- ead, understand, sign and adhere to the school's Acceptable Use Agreement / Policy
- be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- understand the importance of misuse or access to inappropriate materials and are aware of the consequence
- report any suspected misuse or problem to the e-safety coordinator
- maintain an awareness of current e-safety issues and guidance e.g. through CPD
- model safe, responsible and professional behaviours in their own use of technology
- ensure that any digital communications with students should be on a professional level and only through school based systems, never through personal mechanisms, e.g. personal email, text, mobile phones, Social networking etc.
- understand the importance of adopting good e-safety practice when using digital technologies outside of school, and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school
- know how to securely send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection
- ensure that no sensitive data is stored on School Laptops or other devices unless the device has had its hard disk encrypted
- be aware that It is the individual user who has responsibility to inform ICT Support that their laptop or storage device requires encrypting.
- be aware that USB Sticks (or any other physical external storage) must not be used on any school device without explicit permission from the Network Manager.

Parents/carers

- support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes student use of the Internet and the school's use of photographic and video images
- read, sign and understand the school Student Acceptable Use Agreement and promote it with their children
- access the school website / VLE / MIS student records in accordance with the relevant school Acceptable Use Agreement.
- consult with the school if they have any concerns about their children's use of technology

2. Education and Curriculum

Student e-safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / Life Skills curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including
  - to STOP and THINK before they CLICK
  - to develop a range of strategies to evaluate and verify information before accepting its accuracy
  - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
  - to understand how search engines work and to understand that this affects the results they see at the top of the listings
  - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
  - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
  - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
  - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
  - to understand why they must not post pictures or videos of others without their permission
  - to know not to download any files without permission
  - to have strategies for dealing with receipt of inappropriate materials
  - to understand why and how some people will 'groom' young people for sexual reasons;
  - to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
  - to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button

3. Social networks and mobile applications

- School staff are instructed not to establish social network sites for student use on a personal basis or to open up their own social network profiles to their students, but to use the schools' preferred systems for such communications
- We expect staff using school approved Twitter feeds or other Social Media applications to password protect them, associate them with a school based email account, and link them to the school website
- A policy which outlines the acceptable use of a 'Twitter' account for educational purposes is available from ICT support staff if required
- The school's preferred systems for social networking will be maintained in adherence with the school's policy

School staff will ensure that in private use:

- No reference should be made on social media to students, parents / carers or school staff
- No images of students may be taken or shared on personal devices
- They do not engage in online discussions on personal matters relating to members of the school community, or 'friend' any student currently on role. It is also advisable NOT to 'friend' students who have recently left the school, as they can gain access to staff personal Facebook posts through 'Friends of Friends' or similar access. This will be seen as the responsibility of the member of staff.
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- No posts / images / comments bring the school into disrepute, or are deemed to breach the STAR Multi Academy Trust 'Staff Code of Conduct'

4. Personal mobile phones and other mobile devices

Students' use of personal devices

- Mobile phones brought into school are entirely at the student's own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school
- Mobile phones which are brought into school should be turned off throughout the school day, and remain in their school bag, unless required as part of an approved and directed curriculum-based activity with consent from a member of staff
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place. Mobile phones and devices will be released to parents or carers in accordance with the school policy
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned. The recording, taking and sharing of images, video and audio on any mobile device is not allowed, except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded.
- All mobile phone use is to be open to scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time if it is deemed necessary
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office

Review and Monitoring

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates
- The e-safety policy will be reviewed regularly and when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff

Handling complaints

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Academy Trust can accept liability for material accessed, or any consequences of Internet access.

- Staff and students are given information about infringements in use and possible sanctions. Sanctions and support procedures available include:
    - Interview/counselling by tutor / House Leader/ e-Safety Coordinator / Senior Leadership Team or Headteacher
    - Informing parents or carers
    - Removal of internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework)
    - School based sanctions, up to and including permanent exclusion
    - Referral to the police

- Our e-Safety Coordinator acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the school's safeguarding and child protection procedures and safeguarding policy

Tadcaster Grammar School e-safety policy

Version:	V7
Date:	13/05/2020
Headteacher	Andrew Parkinson
e-safety coordinator	Mike Dunphy
Network Manager:	Steve South
Governor with responsibility for Safeguarding:	Christine Burt