Tadcaster Grammar School

1557

Tadcaster
Grammar School

Toulston, Tadcaster,
North Yorkshire. LS24 9NB

e-Safety

POLICY STATEMENT

Written by Mike Dunphy - September 2015
Discussed with Senior Leadership Team - September 2015
Endorsed by Governors – 07/10/15
Issued to Staff - published to website 08/10/15
Revised by MDU 19/10/17
Revised by MDU 07/09/18

Contents

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
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- 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)
- Sexting (sending and receiving of personally intimate images)
- 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 published Behaviour Management Policy.

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

Role	Key Responsibilities
Head of School	• 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 Co-ordinator • 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 Co-ordinator	• 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 / committee to discuss current issues, review incident logs and filtering / change control logs
	• 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
	• Liaises with the Local Authority and relevant agencies
	• 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

Role	Key Responsibilities
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 • The role of the Safeguarding Governor will include regular review with the e-Safety Co-ordinator including e-safety incident logs, filtering and introduction of new e-Learning initiatives
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 arises, 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 user names 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 • Ensures that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • Ensures that the school's policy on web filtering is applied and updated on a regular basis • Ensure that he / she keeps up to date with the school's e-safety policy and technical information in order to effectively 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 Co-ordinator 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 all data held on students on the school office machines have appropriate access controls in place
e-Development Manager	• Ensures that all data held on students on the School's VLE is adequately protected • Ensures that use of the school's email and Google Applications are regularly monitored in order that any misuse / attempted misuse can be reported to the e-Safety Co-ordinator 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

Role	Key Responsibilities
All staff	• To read, understand and promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To 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 • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To 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.
Students	• Read, understand, sign and adhere to the Student Acceptable Use Policy • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To 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 • to know and understand school policy on the use of mobile phones and hand held devices. • To 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
Parents/carers	• to 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 • to read, sign and understand the school Student Acceptable Use Agreement and promote it with their children • to access the school website / VLE / e-Portal pupil records in accordance with the relevant school Acceptable Use Agreement. • to consult with the school if they have any concerns about their children's use of technology

Communication

The policy will be communicated to staff/students/community in the following ways:

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with Students at the start of each year
- Acceptable use agreements to be issued to whole school community, usually on entry to the school

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 local authority 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 Head of School
    - 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 LA / Police

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

- 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

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 annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose
- 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

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 – such as music 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

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Will remind students about their responsibilities through an Acceptable Use Policy which every student will sign
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons
- Ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights
- 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

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection
- Makes regular training available to staff on e-safety issues and the school's e-safety education programme
- 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

Parent awareness and training

This school

- Runs a rolling programme of advice and guidance for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
    - Information leaflets; in school newsletters; on the school web site
    - Demonstrations, practical sessions held at school
    - Suggestions for safe Internet use at home
    - Provision of information about national support sites for parents

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- should 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
- will be expected to know and understand school policies on the use of mobile phones and other hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, laptops, hand held devices and other new technologies

Students

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In this school:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively
- Support is actively sought from other agencies as needed in dealing with e-safety issues
- Monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA as necessary
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

Procedures for Handling and Reporting Incidents

Many incidents of misbehaviour involving ICT do not lead to actual or potential significant offence, harm or distress. These should be dealt with by our normal discipline procedures. Where the member of staff involved believes the event to be an e-safety incident, they will follow this procedure:

- Log the incident via email to the safety coordinator. This fulfils the duty to inform the e-safety coordinator
- If the incident constituted misbehaviour the member of staff must add a negative comment to e-Portal
- The e-safety co-ordinator investigates and decides whether further action should be taken
- Further action may include sanctions and may involve parents. In extreme cases, it may be necessary to involve outside agencies such as the police or the local authority
- The e-safety co-ordinator will inform other staff as appropriate

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity through the Local Authority
- Uses the NYCC filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved web management status
- Ensures network is 'healthy' through use of anti-virus software and network set-up so staff and students cannot download executable files
- Requires that sensitive/personal data is not sent through insecure or unencrypted email/internet systems
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform

- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons
- Is vigilant in its supervision of students' use at all times, as far as is reasonable, and uses strategies in learning resource areas where older pupils have more flexible access
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns
- Ensures pupils only publish within an appropriately secure environment : the school's Virtual learning environment (VLE), Google Classroom, or other 'cloud based' platform agreed by the e-safety coordinator
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of Google Classroom and the school's Virtual Learning Environment as a key way to direct students to age / subject appropriate web sites;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored
- Informs staff and students that that they must immediately report any failure of the filtering systems directly to the network manager
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for students, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities, including the local authority and the police

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful
- Ensures the Systems Administrator / network manager is up-to-date with NYCC services and policies / requires the Technical Support Provider to be up-to-date with NYCC services and policies
- Storage of all data within the school will conform to the UK data protection requirements, and comply with the EU GDPR (General Data Protection Regulations)

  Students and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password
- Ensures that staff's access to the schools' management information system is controlled through a separate password for data security purposes

- We provide students with an individual network log-in username. They are also expected to use a personal password
- All students have their own unique username and password which gives them access to the Internet, the Learning Platform and their own school approved email account
- Makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network
- Has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas
- Requires all users to always lock or log off when they have finished working or are leaving the computer unattended
- Has set-up the network so that users cannot download executable files / programmes
- Has blocked access to music/media download sites – except those approved for educational purposes
- Advises that all mobile equipment is scanned with anti-virus / spyware before it is connected to the network
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so
- Makes clear that staff are responsible for ensuring that any computer, laptop or mobile device loaned to them by the school, is used solely to support their professional responsibilities
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems
- 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
- Provides students and staff with access to content and resources through the approved Learning Platforms which staff and students access using their username and password
- Makes clear responsibilities for the daily back up of MIS and other important files
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data
- Ensures that all student data sent over the Internet is encrypted or only sent within an approved secure system
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
- Our wireless network has been secured to appropriate standards suitable for educational use
- All computer equipment is installed professionally and meets health and safety standards
- Reviews the school ICT systems regularly with regard to health and safety and security

Password policy

- This school makes it clear that staff and students must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use 'strong' passwords for access into our network, e-Portal, email and VLE
- We require staff to change their passwords into e-Portal on a regular basis.

E-mail

This school

- Provides staff with a Google email account for their professional use, and makes clear personal email should be through a separate account
- Will contact the Police if one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the police

Students:

- Students are introduced to, and use e-mail as part of the ICT/Computing scheme of Learning
- Students are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer
    - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe
    - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature
    - not to respond to malicious or threatening messages
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them
- Students sign the school ICT Acceptable Use Agreement (AUA) and confirm that they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with

Staff:

- Staff are expected to use only the school provided, Google based @tgsch email system for professional purposes
- Staff are expected never to use email to transfer staff or student personal data
- All staff sign to say they have read and understand both the ICT AUA and the e-safety policy, and we explain how any inappropriate use will be dealt with

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- The school web site complies with the statutory DfE guidelines for online publication;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the web site is the school address, telephone number and email addresses for key members of staff
- Photographs published on the web do not have full names attached without the permission of parents/carer
- We do not use students' names when saving images in the file names or in the tags when publishing to the school website

Virtual Learning Environment

- Uploading of information on the schools' Virtual Learning Environment (VLE) is shared between different staff members according to their responsibilities
- Photographs and videos uploaded to the schools VLE will only be accessible by members of the school community, unless permission has been given to publish them to a wider audience
- In school, students are only able to upload and publish within school approved and closed systems, such as the VLE or Google Classroom

Social networking

- Teachers 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 teachers using school approved Twitter feeds or blogs to password protect them, associate them with a school based e-mail 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 discussion on personal matters relating to members of the school community, or in the case of Facebook, do not 'friend' any student currently on role. It is also advisable NOT to 'friend' past students, as they can gain access to staff personal Facebook posts through 'Friends of Friends' 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

5. Equipment and Digital Content

Storage of sensitive data on fixed/mobile devices

- **Laptops:** No sensitive data should be stored on School Laptops unless the laptop has had its hard disk encrypted
- **USB Sticks (or any other physical external storage):** No sensitive data should be stored on such storage devices unless it has been fully encrypted

  It is the individual member of staff who has responsibility to inform ICT Support that their laptop or storage device requires encrypting.

- **Office and classroom Computers:** No sensitive data should be stored on the local drives of any office or classroom based computers
- **School Management System (MIS):** Any sensitive data printed out from the school's MIS system should be marked with the word PROTECT in the footer of each page

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 hand held device brought into school
- Mobile phones which are brought into school must 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 Head of School. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head of School is to be 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
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone or email system
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations
- 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
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences

Version Control

As part of the maintenance involved with ensuring your e-safety policy is updated, revisions will be made to the document. It is important that the document owner ensures the document contains the following information and that all revisions are stored centrally for audit purposes.

Title	Tadcaster Grammar School e-safety policy
Version	V3
Date	19/10/2017
Author	e-safety coordinator Mike Dunphy
Approved by head teacher	
Approved by Governing Body	
Next Review Date	October 2019

Modification History			
Version	Date	Description	Revision Author
V2 V3 V4	28/09/15 19/10/17 07/09/18	Additional wording (CMU consultation) Additional wording to reflect student/staff AUAs, and GDPR Head of School change (WWI)	e-safety coordinator e-safety coordinator e-safety coordinator e-safety coordinator

Role (September 2018)	Named individual
Head of School	Wendy Wilson
e-Safety co-ordinator	Mike Dunphy
Network Manager	Steve South
Computing Curriculum Leader	Jon Bell
e-Development Manager	Steve Smith
Governor with responsibility for Safeguarding	Christine Burt