



ONLINE SAFETY POLICY

Reviewed:	December 2024
By:	Sarah Hayde-Salter
Next Review Date:	December 2025

This Policy links to:

Keeping Children Safe in Education 2024

BRS Safeguarding Policy

Anti-Bullying Policy



CONTENTS

- a. Introduction
- b. Risks
- c. Roles and Responsibilities
- d. Communication
- e. Handling Incidents
- f. Learning
- g. IT Management
- h. Data Security
- i. Equipment and Digital Content

a. INTRODUCTION

The purpose of this policy is to:

- Set out the key principles expected to all members of staff, students and visitors with respect to the use of IT-based technologies.
- Safeguard and protect the students and staff
- Assist staff working with children and young people to work safely and responsibly with the Internet and other IT 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 for the whole school.
- Have clear structures to deal with online abuse such as online bullying, in line with BRS Safeguarding and Anti-Bullying Policies.
- Ensure that all members of staff and students 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.



b. RISKS

There are many potential risks, the main areas of risk for the BRS are;

- **CONTENT**
 - Exposure to inappropriate content
 - Lifestyle websites promoting harmful behaviours
 - Hate content
 - Content validation: how to check authenticity and accuracy of online content
- **CONTACT**
 - Grooming (sexual exploitation, radicalisation, gambling etc.)
 - Online bullying in all forms, especially via social media
 - Social or commercial identity theft, including passwords
- **CONDUCT**
 - Aggressive behaviours (bullying)
 - Privacy issues, including disclosure of personal information
 - Digital footprint and online reputation
 - Health and well-being (amount of time spent online, gambling, body image)
 - Sexting
 - Copyright (little care or consideration for intellectual property and ownership)

c. ROLES AND RESPONSIBILITIES

Role	Key Responsibilities
Senior Management Team	<ul style="list-style-type: none">• Must be adequately trained in off-line and online safeguarding, in line with statutory guidance and relevant Suffolk Safeguarding Partnership guidance• To lead a “safeguarding” culture, ensuring that online safety is fully integrated with whole school safeguarding.• To take overall responsibility for online safety provision• To take overall responsibility for data management and information security ensuring school’s provision follows best practice in information handling• To ensure the school uses appropriate IT systems and services including, filtered internet services• To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles• To be aware of procedures to be followed in the event of a serious online safety incident• Ensure suitable “risk assessments” undertaken so to meet the needs of students, including risk of children being radicalised• To receive regular monitoring reports from the Safeguarding Team.• To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures• To ensure Trustees are regularly updated on the nature and effectiveness of the school’s arrangements for online safety• To ensure the school’s website includes relevant information.



<p>Designated Safeguarding Lead (DSL) and Deputies</p>	<ul style="list-style-type: none">• Take a day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents• Promote awareness and commitment to online safety throughout the school• Ensure that online safety education is embedded within the students learning environment• Liaise with school technical staff where appropriate• To communicate regularly with the SMT and the designated Trustee/Committee to discuss current issues and review incidents• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident• To ensure that online safety incidents are logged as a safeguarding incident• Facilitate training and advice for all staff• Oversee any student surveys / feedback on online safety issues• Liaise with the Local Authority and relevant agencies• Is regularly updated in online safety issues and legislation and be aware of the potential for serious child protection concerns.• Ensure this Policy is reviewed annually or when any significant changes occur with regard to the technologies in use within the school
<p>Trustees / Safeguarding Trustee (including online safety)</p>	<ul style="list-style-type: none">• To ensure that the school has in place policies and practices to keep the children and staff safe online• To approve the Online Safety Policy and review the effectiveness of the policy
<p>IT Lead (Duncan Gregory)</p>	<ul style="list-style-type: none">• To report online safety related issues that come to their attention, to the DSL• To manage the school's computer systems, ensuring<ul style="list-style-type: none">- school password policy is strictly adhered to- systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date)- access controls/encryption exist to protect personal and sensitive information held on school owned devices- the school's policy on web filtering is applied and updated on a regular basis• Keeps up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant• That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the DSL• To ensure appropriate backup procedures and disaster recovery plans are in place
<p>Data Manager (Andrew Braithwaite)</p>	<ul style="list-style-type: none">• To ensure that the data they manage is accurate and up-to-date• Ensure best practice in information management, i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements• The school must be registered with Information Commissioner's Office (ICO)



Instructional Staff	<ul style="list-style-type: none">• To embed online safety in the students learning• To supervise and guide students carefully when engaged in learning activities involving online technology• To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All Staff	<ul style="list-style-type: none">• To read and adhere to the school's Online Safety Policy• To report any suspected misuse or problem to the DSL• Maintain an awareness of current online safety issues and guidance e.g. through CPD• To model safe, responsible and professional behaviours in their own use of technology <p>On Leaving Employment:</p> <ul style="list-style-type: none">• At the end of the period of employment to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with Line Manager and IT Manager on the last day to log in and allow a factory reset.
Students	<ul style="list-style-type: none">• To be aware of and have access to the BRS Online Safety 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 understand the importance of adopting safe behaviours and good online safety practice when using digital technologies• To contribute to student surveys / feedback that gathers information on their online experiences• To note, learn and apply all training provided covering Online Safety
Parents / Carers	<ul style="list-style-type: none">• To be aware of and have access to the BRS Online Safety Policy via BRS website• To support the BRS in promoting online safety• To consult with the school if they have any concerns about their child or young person's use of technology
External Groups	<ul style="list-style-type: none">• Any external individual/organisation to be aware of and adhere to the BRS Online Safety Policy as displayed on the website• To support the BRS in promoting online safety• To model safe, responsible and positive behaviours in their own use of technology

d. COMMUNICATION

The policy will be communicated to staff/students/parents/carers/external groups

- Policy to be posted on the school website and relevant notice boards
- Policy to be part of school induction pack for new staff
- Regular updates and training on online safety for all staff



e. HANDLING INCIDENTS

- The school will take all reasonable precautions to ensure online safety
- Staff and students are given information about infringements in use and possible sanctions.
- Safeguarding Lead and / or deputies act as first point of contact for any incident
- Any suspected online risk or infringement is reported to the DSL that day
- Any concern about staff misuse is always referred directly to the Chief Executive, unless the concern is about the Chief Executive in which case the complaint is referred to the Chair of Trustees and the LADO (Local Authority's Designated Officer).

f. LEARNING

Students

The BRS:

- Has an e-Safety session included in the programme
- Plans online 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 the Online Safety Policy and use of posters and information boards
- Ensure staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- Ensures that staff and students understand the issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;

Staff

The BRS:

- Makes regular training available to staff on online safety issues
- Provides, as part of the induction process, all new staff with information and guidance on the Online Safety Policy

g. IT MANAGEMENT

Internet access, security (virus protection) and filtering

This school:

- Informs all users that Internet/email use is monitored;
- Has the educational filtered secure broadband connectivity
- Uses a filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming, gambling, alcohol and drugs). All changes to the filtering policy are logged and only available to staff with the approved web filtering management status
- Ensure network health through the use of anti-virus software



- Uses individual log-ins for all users
- Has regular back-up of school data
- Storage of all data within the school will conform to the EU and UK data protection requirements; storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.
- To ensure the network is used safely, ensure all staff are aware of the school's online safety policy. Following this, they are set-up with Internet, email access and network access.
- All users of the school's e-Portfolio system (OneFile) are issued with their own unique username and password and users are reminded to not give this information to another user.
- Ensure all users know to log off when they have finished working or leaving their computer or device unattended
- Ensure all equipment owned by the school and/or connected to the network has up to date virus protection
- Makes clear that staff are responsible for ensuring that any computer/laptop/device loaned to them by the school, is used primarily to support their professional responsibilities
- Maintains equipment to ensure Health and Safety is followed
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school approved systems
- Does not allow outside Agencies to access its network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems
- All IT and communication systems installed professionally and regularly reviewed to ensure they meet health and safety standards

Password policy

- This school makes it clear that staff and students must always keep their passwords private, must not share with others; if a password is compromised the school should be notified immediately
- All staff have their own unique username and private password to access school systems. Staff are responsible for keeping their password(s) private
- We require staff to use strong passwords
- We require staff to change their passwords into the MIS every year as directed

E-Mail

This school:

- Provides staff with an email account for their professional use
- 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

School Website

- The Chief Executive, supported by the Trustees, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- The school website complies with statutory DFE requirements



- 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;
- Photographs published on the web do not have full names attached. We do not use students' names when saving images in the file names or in the tags when publishing to the school website

e-Portfolio

- Uploading of information on the schools' e-Portfolio system is shared between different staff members according to their responsibilities
- Photographs and videos uploaded to the schools' e-Portfolio system will only be accessible by members of staff

Social Networking

- Staff are instructed to always keep professional and private communication separate
- Staff are not permitted to communicate with students via personal networking profiles
- Where necessary, staff may be required to communicate with students via a BRS networking page. "BRS" must be within their name and the password must be known to a member of the safeguarding team.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and students safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

Video Recording of Riding Lessons

- We use video recording equipment in riding lessons to assist with teaching, learning and assessment. These recordings may be uploaded to the e-Portfolio system but will not be shared outside of the BRS without gaining permission of the student and of those aged under 18 years, their parent/guardian.

h. DATA SECURITY

Strategic and operational practices

At this school:

- The Operations Director is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised
- Appropriate DBS checking of staff is carried out and records are held in a single central record.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out 10 minutes idle time.
- All servers are in lockable locations and managed by DBS checked staff
- Details of all school-owned hardware will be recorded in a hardware inventory



- Details of all school-owned software will be recorded in a software inventory
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. (Further information can be found on the Environment Agency website).
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

i. EQUIPMENT AND DIGITAL CONTENT

- Students must follow BRS procedures with regards to holding and using mobile devices in the yard areas and in all lectures.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting trainees, young people or their families within or outside of the setting.
- Staff will be issued with a phone or device where contact with students, parents or carers is required.
- Staff should not use personally-owned devices, such as a mobile phone, camera or device to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- We gain parental/carer permission for use of digital photographs or video involving their child as part of the Course Confirmation form when their daughter/son joins the school
- We do not identify students in online photographic materials or include the full names of students in the credits of any published school produced video materials/DVDs
- If specific student photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or student permission for its long term, high profile use
- Students are taught about how images can be manipulated in their e-Safety session and also taught how to consider how to publish for a wide range of audiences which might include trustees, parents or younger children as part of their daily activities.
- Students are advised to be very careful about placing any personal photos on any "social" online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.