Medina College and The Island VI Form

E-Safety Policy

Author	Josh Collins
Approved by	IEB
Approval date	11 May 2026
Review frequency	Bi-Annually
Next review	November 2026

Revision History

Revision	Change	Date
1.4	Updated pages	12/07/2013
1.5	Minor Amendments	17/03/2014
1.6	Minor Amendments	14/01/2015
1.7	Minor Amendments	14/10/2016
1.8	Minor Amendments	16/01/2018
1.9	Adjustment for IWEF and responsibilities	01/10/2019
2.0	Minor Amendments	19/01/2021
2.1	Minor Amendments	07/07/2022
2.2	Minor Amendments	22/09/2022
2.3	Amendments to AUP	06/12/2022
2.4	Major revision following Trust onboard	08/12/2025
2.5	Minor Amendments	06/05/2026

Contents

1. Introduction

The development and expansion of the use of IT, and particularly of the Internet, has transformed learning in education in recent years. Students at Medina College (including The Island VI Form) need to develop high-level IT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment.

There is a large body of evidence that recognises the benefits that IT can bring to teaching and learning. Medina College has made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks". However, through this Online Safety Policy, Medina College will ensure that they meet their statutory obligations to ensure that students are safe and protected from potential harm, both within and outside school.

The policy forms part of the school's protection from legal challenge relating to the use of IT. The content within this policy is based on the Department for Education's (DfE) most recent statutory guidance for *Keeping Children Safe in Education (KCSIE)*.

The Colleges will:

- Ensure the Executive Headteacher delegates responsibility for Online Safety to a suitably trained senior member of staff (Online Safety Coordinator) and Governor (Online Safety Governor).
- Establish an Online Safety group consisting of key staff members including the Online Safety Coordinator, Online Safety Governor, IT Manager, along with representatives from a range of stakeholders (teaching staff, support staff, student council, and parent voice).
- Establish, maintain, and review password, filtering, and email procedures alongside the Online Safety Policy and procedure documents in line with the Cyber Security Policy.
- Ensure Online Safety issues are embedded in all aspects of the curriculum and staff CPD, and that all users understand and follow the school Online Safety policy and procedure.
- Ensure that all users are aware of, understand, and agree to the Acceptable Use Policy (AUP) through signing and submitting the appropriate form prior to their initial engagement in any activities.
- Engage and help with parental or carer Online Safety understanding through parents' evenings, newsletters, letters, and websites.
- Ensure that all IT devices, equipment, software, and services are fit-for-purpose in accordance with the Online Safety procedures and monitored so that any misuse is recorded and appropriate action taken.
- Ensure that all individuals comply with the procedure regarding the use of digital images and video, ensuring appropriate permission alongside the media and medium.
- Provide or arrange awareness training and guidance for students, staff, governors, and parents/carers.
- Ensure review of the effectiveness of Online Safety policy and procedures through participation in Online Safety meetings, monitoring of incident logs, filtering, and change control logs.

2. Scope of the Policy

This policy applies to all members of the Medina College (including The Island VI Form) community (including staff, students, Governors, volunteers, parents/carers, visitors, and community users) who have access to and are users of the college and wider HISP Multi-Academy Trust IT systems, both on and offsite.

The Education and Inspections Act 2006 empowers the Executive Headteacher, 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, inappropriate use of AI tools, or other Online Safety incidents covered by this procedure, which may take place out of college but are linked to membership of the college. The college will deal with such incidents within this procedure and associated behaviour policies and will inform parents/carers of inappropriate Online Safety behaviour taking place out of college.

3. General Policy Statement

Medina College believes that the online safety of individuals within the school is of paramount importance. The first requirement for maintaining high standards of safety is that everyone is vigilant and undertakes personal responsibility for their own safety and that of others. Safe and acceptable use refers to both school and personal equipment when at work or when accessing education-related software. It is vital that adults recognise their additional responsibility for modelling safe practice for young people.

We believe that health and safety standards will be maintained only with the cooperation of all staff, students, and visitors. We require all staff to comply fully with this policy and ensure all students, visitors, and contractors are provided with the information required to comply.

The College recognises the increasing availability and use of Artificial Intelligence (AI) tools in education and online environments. From an online safety perspective, some risks may include:

- Exposure to inappropriate or misleading information/content
- Collections or misuse of personal data
- Academic integrity concerns
- Over-reliance on automated decision making

The safe, ethical and curriculum-specific use of AI is addressed in Medina College's separate AI Policy. This current E-Safety policy focuses on safeguarding, supervision, filtering and acceptable use.

4. Roles and Responsibilities

The Senior Leadership Team will:

- Ensure the policy is regularly monitored.
- Ensure that all members of the school have appropriate Online Safety training.

The Safeguarding Lead will:

- Have overall responsibility for ensuring the safety (including online safety) of all staff, volunteers, and members of Medina College.
- Be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff or volunteer.

The Online Safety Officer will:

- Ensure that staff/volunteers have an up-to-date awareness of the school's current online safety policy and practices.
- Ensure that all staff/volunteers are aware of the procedures for an online safety incident.
- Take day-to-day responsibility for online safety issues and lead in establishing and reviewing the online safety policies.
- Offer advice and support for all users.
- Keep up to date with developments in online safety, including emerging technologies like Artificial Intelligence.
- Monitor incident logs and report regularly to the Safeguarding Leader.

The IT Department will:

- Ensure appropriate solutions are in place for online web activity monitoring, blocking, and reporting, including emerging AI-driven services where possible
- Follow the Cyber Security Policy to ensure systems are safe, secure, and at minimal risk from harmful content
- Routinely audit blocked/allowed site URLs to ensure their authenticity

All staff will:

- Have an up-to-date awareness of the school's current online safety policy and practices.
- Have read and understood the Staff Acceptable Use Policy.
- Report any suspected misuse or problem to the Online Safety Officer.
- Use digital communications with young people on a professional level, exclusively using official school systems.
- Actively enforce the school's Mobile Phone Policy, ensuring personal devices do not compromise safeguarding.
- Monitor the use of mobile devices, gaming consoles, and web-based AI tools, intervening when necessary.

Parents/Carers will:

- Ensure that their children understand the need to use the internet and mobile devices appropriately.
- Endorse the Acceptable Use Policy for Young People.
- Sign the relevant permission forms on the taking and use of digital and video images.

Students will:

- Abide by the Acceptable Use Policy, which they must sign before being given access to systems.
- Understand the importance of reporting abuse, misuse, or access to inappropriate materials.
- Demonstrate positive online behaviour.
- Adhere strictly to the school's Mobile Phone Policy and academic integrity guidelines regarding the use of AI platforms as defined in the AI Policy

5. Educating Children and Young People to Stay Safe Online

Whilst regulation and technical solutions are very important, their use must be balanced by making young people aware of the need to take a responsible approach to online safety. Online safety awareness will be provided in the following ways:

- Key online safety messages will be reinforced as part of all relevant planned programmes of study, particularly through the PSHE curriculum.
- Online safety issues will be discussed in informal conversations with young people where appropriate.
- Young people will be educated on the ethical and safe use of Artificial Intelligence (AI) tools, including understanding misinformation, data privacy, and academic integrity.
- Young people will be made aware of the need to respect copyright when using internet material.
- Staff and volunteers will act as good role models in their use of online technologies.

6. Awareness Raising for Parents/Carers

The school will provide online safety information to parents and carers through:

- Letters, newsletters, and the Medina College and The Island VI Form websites.
- Formal and informal meetings with parents and carers.
- Sharing the group's policies with parents and carers.
- Engaging parents in the signing of acceptable usage policies.

7. Protecting the Professional Identity of Staff and Volunteers

Consideration must be given to how online behaviour may affect personal safety and the reputation of the school. Communication between adults and students must take place within clear and explicit boundaries. Official communication and learning platforms include managed Microsoft and Google environments provided by the college, as well as procured third-party services with active contracts managed by college staff. Personal accounts must not be used for professional or educational communication with students and parents.

When using digital communications, staff and volunteers must:

- Only make contact with students for professional reasons via allocated resources (e.g., official email, Google Classroom, or Google Meet).
- Never request or respond to personal information from a student unless appropriate to a professional role or in an emergency.
- Ensure all communications are transparent, open to scrutiny, and careful in tone to avoid misinterpretation.
- Never share personal social networking profile details with students.
- Never add students as "friends" on any personal social network.
- Never post information online that could bring Medina College or the Trust into disrepute.

Good Practice Guidelines:

- The school's official email service is monitored and regarded as safe.
- Users must immediately report the receipt of any offensive or threatening communication to the Online Safety Officer and must not respond.
- Personal information must not be posted on the school website; only official email addresses will be used to identify staff.

8. Use of Digital and Video Images

The development of digital imaging allows instant use and sharing of images. However, images may remain available on the internet forever and can cause harm or embarrassment.

- Staff must raise awareness among students about the risks associated with taking, sharing, and publishing images, particularly on social media.
- Written permission from parents or carers must be obtained to allow images to be taken of their children for legitimate activities or publicity.
- Staff and volunteers must use the organisation's equipment, not personal devices, to capture images of students.
- The full names of young people will not be used anywhere on a website, blog, or published article in association with photographs.

9. Data Security

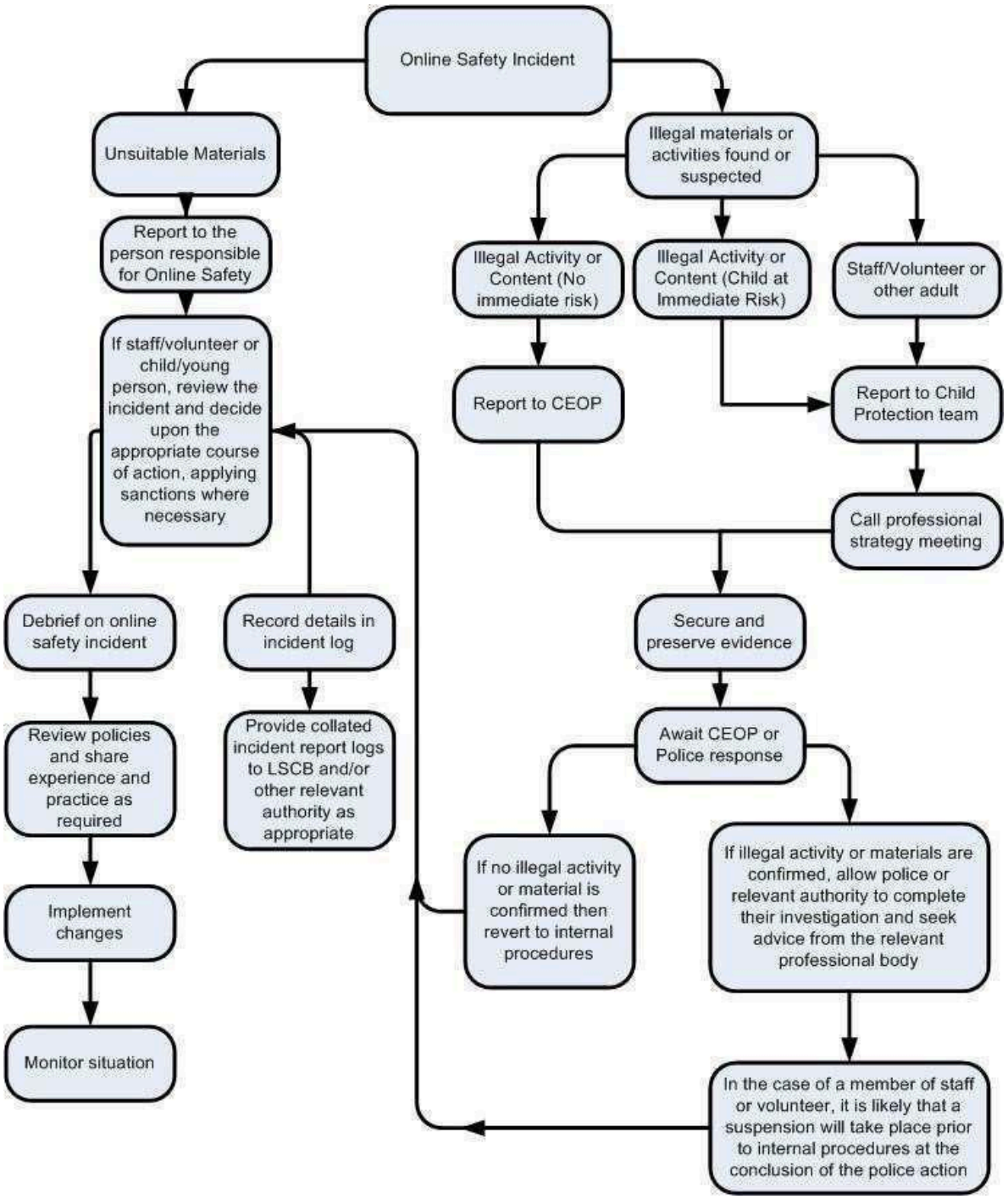
Personal data will be recorded, processed, transferred, and made available according to UK GDPR & the Data Protection Act 2018. Personal data must be:

- Used fairly, lawfully, and transparently.
- Used for specified, explicit purposes.
- Adequate, relevant, and limited to only what is necessary.
- Accurate and kept up to date.
- Kept for no longer than is necessary.
- Handled in a way that ensures appropriate security against unlawful processing, loss, or damage.

Medina College has a specific policy for Data Protection reviewed by the Data and Administration Team.

10. Flowchart for Responding to Online Safety Incidents

Note: Please refer to the separately maintained visual flowchart document detailing the step-by-step response to online safety incidents, including escalation paths to the Safeguarding Lead and local authorities.



11. Internet Filtering

Introduction The filtering of internet content aims to prevent users from accessing material that is illegal or inappropriate. No filtering system cannot provide a 100% guarantee. It is therefore important that the college has a filtering procedure to manage risks.

Responsibilities The IT Support Department manages the college filtering system in line with the Cyber Security Policy. Major changes to the college filtering service must:

- Be logged in change control logs via the authorised ticketing system
- Be authorised by a second responsible person
- Be reported to the Online Safety Committee

Users must not attempt to use any software to bypass the filtering or security systems.

Changes to the Filtering System

- Students: Report required unfiltered sites to a teacher. The teacher assesses the site and submits a website unblock request via the Self Service Portal if appropriate.
- Staff: Complete a website unblock request form and submit it via the Portal, including their Line Manager for vetting and approval.
- IT Staff: Process block/unblock requests made through the portal after confirming LM approval and vetting.

Audit and Reporting Routine reports are circulated to the Safeguarding Leads. Instantaneous alerts triggering specific topic warnings (abuse, self-harm, drugs) are sent immediately, with a daily and weekly round-up email to Safeguarding personnel.

12. Personal Data Policy

The College has access to a wide range of personal information (digital and paper). This includes personal details of students, staff records, and agency information.

Policy Statements and Responsibilities

- The school will hold the minimum personal information necessary.
- The safeguarding officer will keep up to date with current legislation and ICO guidance (available at https://ico.org.uk).
- Staff and volunteers will receive data protection training during induction and regular briefings.
- Information risk assessments will be carried out to establish key areas where data might be at risk.

Storing and Disposing of Data

- Personal data must be held securely on allocated cloud platforms.
- Any data removed from the premises must have appropriate protection to prevent loss.
- Data destruction must be safe and secure (e.g., electronic files securely overwritten, paper shredded/incinerated).

13. Guidance for Reviewing Internet Sites

This guidance is used when investigating incidents involving online services (cyber-bullying, harassment, deception).

> CRITICAL: Do not follow this procedure if you suspect the website contains child abuse images. Halt monitoring and report immediately to the police.

Procedure for Investigation:

- Have more than one senior member of staff involved to protect individuals from accusations.
- Use a designated computer that is not used by young people and can be taken off-site by the police if necessary.
- Record the URL of any site and describe the content. Record and store screenshots if necessary.
- If the concern has substance, initiate internal discipline procedures, or involve the Local Authority / Police.
- Isolate the computer in question; any changes to its state may affect a police investigation.

Website Unblock Request

Please fill out the following form to request for a website to be unblocked on the school system Please note that by requesting for a site to be unblocked you must be fully aware of and are responsible for the sites content Requests may be referred to the head teachers for authorisation if the website is categorised by the colleges filtering system as "Adult"_

Before returning this form, please ensure you have completed the following:
Make sure all applicable sections are fully completed with accurate information_

1 - Details

First Name

Last Name

E-mail Address

2 - Website Details

URL

Site Content

Reason For Unblock

Temporary Medina Staff

Permanent

Carisbrooke

VI Form Campus

Students

3 - Staff Signature

By signing this document you are showing that you understand and agree to all of the terms_ Signature

Date

4 - Department Head Signature

By signing this document you are showing that you understand and agree to all of the terms_ Signature

Date

5 - Head Teachers Signature (if required)

By signing this document you are showing that you understand and agree to all of the terms_

Signature

Date

FOR OFFICE USE ONLY: Date Received HT Review Completed Rejected

1. Record of Reviewing Internet Sites

College:	
Date:	
Reason for investigation:	

Details of first reviewing person

Name:	
Position:	
Signature:	

Details of second reviewing person

Name:	
Position:	
Signature:	

Name and location of computer used for review

Computer:	Location:

Web site(s) address Reason for concern

1.	
2.	
3.	
4.	
5.	
6.	
7.	

Conclusion and Action proposed or taken

1.	
2.	
3.	
4.	
5.	
6.	
7.	

2. Reporting Log

Date	Time	Incident	Action Taken	Name/Signed

3. Monitoring Log

Date	Monitored by	Issue Identified	Reported to	Signed

4. List of Responsible Persons

E-Safety Coordinator:

Anna Mursell – Medina College

Phil Pearce-Jones – The Island VI Form

Designated Safeguarding Lead:

Katie Sandiford – Medina College and The Island VI Form

E-Safety Governor:

xxx

IT Technical Staff:

Josh Collins - IT Manager

Data Protection Officer (DPO):

Shane Williams - Global Policing - shane@globalpolicing.co.uk

Information Asset Owners:

Kevin Thurlow-Criss - HISPMAT Executive Director of Operations

Anna Mursell – Medina College and The Island VI Form