Isle of Wight
Education Federation

The Governing Board of the Isle of Wight Education Federation

E-Safety Policy

Author	Mark Overy Josh Collins
Approved by	Full Governing Board
Approval date	January 2023
Review frequency	Bi-Annually
Next review	January 2025

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

Contents

1. Introduction

The development and expansion of the use of ICT, and particularly of the Internet, has transformed learning in education in recent years. Students at the Isle of Wight Education Federation need to develop high-level ICT 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 ICT can bring to teaching and learning. The Federation 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, each school will, through this E-Safety Policy, 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 will also form part of the school's protection from legal challenge, relating to the use of ICT. The content within this policy is based on the Department for Education's (DfE) guidance for Keeping Children Safe in Education.

The Colleges will:

- Ensure the Executive Headteacher delegates responsibility for E-Safety to a suitably trained senior member of staff (E-Safety Coordinator) and Governor (E-Safety Governor)
- Establish an E-Safety group consisting of key staff members including the E-Safety Coordinator, E-Safety Governor, Director of Facilities and ICT along with representatives from teaching staff, support staff, student council and parent voice
- Establish, maintain and review password, filtering and email procedures alongside the E-Safety Policy and procedure documents in line with Cyber Security Policy
- Ensure E-Safety issues are embedded in all aspects of the curriculum and staff CPD and that all users understand and follow the school E-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 E-Safety understanding through parents' evenings, newsletters, letters and websites
- Ensure that all information communication technology devices, equipment, software and services are fit-for-purpose in accordance with the E-Safety procedures and monitored in order that any misuse or attempted misuse is recorded and appropriate action taken through the appropriate sanctions
- Ensure that all individuals comply with the procedure in regard to 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/guardians/carers
- Ensure review of the effectiveness of E-Safety policy and procedures through participation in E-Safety meetings, monitoring of incident logs, filtering and change control logs

2. Scope of the Policy

This policy applies to all members of the Federation community (including staff, students, Governors, volunteers, parents / carers, visitors and community users) who have access to and are users of the college and wider Federation ICT 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, or other E-Safety incidents covered by this procedure, which may take place out of college, but is linked to membership of the college. The college will deal with such incidents within this procedure 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 college.

3. General Policy Statement

The Federation 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 of others. Safe and acceptable use refers to both school and personal equipment when at work or when accessing education related software. In the special circumstances of a College it is also important 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 to the school. We require all staff to comply fully with this policy. In addition we will ensure that all students, visitors and contractors are provided with the information they require to enable them to comply with this policy. The policy will be reviewed annually and revised where necessary.

4. Roles and Responsibilities

The Senior Leadership Team will:

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

The Safeguarding Lead will:

- Have overall responsibility for ensuring the safety (including online safety) of all staff, volunteers and members of the Federation
- 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 (see flowchart on dealing with online safety incidents, section 10)

The E-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 that need to be followed in the event of an online safety incident taking place.
- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies / documents
- Offer advice and support for all users
- Keep up to date with developments in online safety
- Understand and know where to obtain additional support and where to report issues
- Ensure provision of advice is there for staff and volunteers
- Monitors incident logs
- Reports regularly to the Safeguarding Leader

The E-Safety Officer will be trained in up to date online safety issues and be aware of the potential for serious child protection issues. (Nb. it is important to emphasise that these are child protection issues, not technical issues; simply that the technology provides additional means for child protection issues to develop).

The ICT Department will:

- Ensure appropriate solutions are put in place for online web activity monitoring, blocking and reporting
- Follow the Federation's Cyber Security Policy to ensure systems used by staff/students/volunteers are safe, secure and at minimal risk from potentially harmful or inappropriate content
- Routinely audit blocked/allowed site URLs to ensure their authenticity
- Further information about the overview of Internet Filtering and this facility is referenced in Section 11

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 relevant person (E-Safety Officer) – particularly where it is believed that a child's welfare is at risk
- Use digital communications with children and young people on a professional level and where possible only carried out using the official systems of the group.
- Ensure young people in their care are aware of online safety
- Be aware of online safety issues particularly those related to the use of mobile phones, cameras, gaming consoles and mobile devices and that they monitor their use and implement policies with regard to these devices

Parents/ Carers will:

- Ensure that their children understand the need to use the internet / mobile devices in an appropriate way
- Endorse (by signature) the Acceptable Use Policy for Young People which is included as part of the student handbook.
- Sign the relevant permission forms on the taking and use of digital and video images

Students will:

- Abide by the Acceptable Use Policy / Rules, which they may be expected to sign before being given access to the organisation's systems and devices
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should demonstrate positive online behaviour Policy Statements

5. Educating children and young people to stay safe online

Whilst regulation and technical solutions are very important, their use should be balanced by making children and young people aware of the need to take a responsible approach to online safety. Children and young people need help and support to recognise and avoid online safety risks and build their resilience. Online safety awareness will be provided in the following ways:

- Key online safety messages should be reinforced as part of all relevant planned programmes of study for students particularly through the PSHE curriculum
- Online safety issues should be discussed / highlighted, when possible, in informal conversations with young people
- Young people should be made aware of the need to respect copyright when using material accessed on the internet and, if applicable, acknowledge the source of information used
- Staff and volunteers should 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, Federation website
- During meetings with parents / carers (formal and informal)
- 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

This information applies to any adult, but particularly those working with children and young people (paid or unpaid) within the school. Consideration should be given to how your online behaviour may affect your own safety and reputation and that of the school.

Communication between adults and between children/young people and adults, by whatever method, should take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, emails, digital cameras, videos, webcams, websites and blogs.

When using digital communications, staff and volunteers should:

- Only make contact with students for professional reasons via Federation allocated resources i.e. email, Google Classroom or Google Meet
- Not request, or respond to, any personal information from the child / young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm
- Ensure that all communications are transparent and open to scrutiny
- Be careful in their communications with children so as to avoid any possible misinterpretation
- Ensure that if they have a personal social networking profile, details are not shared with children and young people in their care
- Not add students as “friends” on any social network
- Not post information online that could bring the Federation into disrepute
- Any communications outside the agreed protocols (above) may lead to disciplinary and/or criminal investigations

When using communication technologies the school considers the following as good practice:

- The school’s official email service may be regarded as safe and secure and is monitored
- Users must immediately report, to a nominated person (E-Safety Officer) – in accordance with the school’s policy, the receipt of any communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such communication
- Any communication between staff / volunteers and the children / young people or their parents / carers must be professional in tone and content. These communications should, where possible, only take place on official (monitored) systems
- Young people should be taught about online safety issues, such as the risks attached to the use of personal details. They should also be informed of strategies to deal with inappropriate communications
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

8. Use of digital and video images

The development of digital imaging technologies has created significant benefits, allowing users instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will raise awareness about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should raise awareness among students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognize the risks attached to publishing their own images on the internet eg on social networking sites
- Written permission from parents or carers will be obtained to allow images to be taken of their children and also allowing their use for legitimate activities or for publicity that reasonably celebrates success and promotes the work of the school
- Staff and volunteers are allowed to take digital / video images, where appropriate, but must follow the school policies concerning the sharing, distribution and publication of those images. Those images should be taken, where possible, on the organisation’s equipment, not the personal equipment of staff. If photos are taken, their storage and use must not cause risk or embarrassment
- The full names of young people will not be used anywhere on a website, blog, or published article, particularly in association with photographs. Consideration should be given to media coverage and journalists should be made aware of this policy

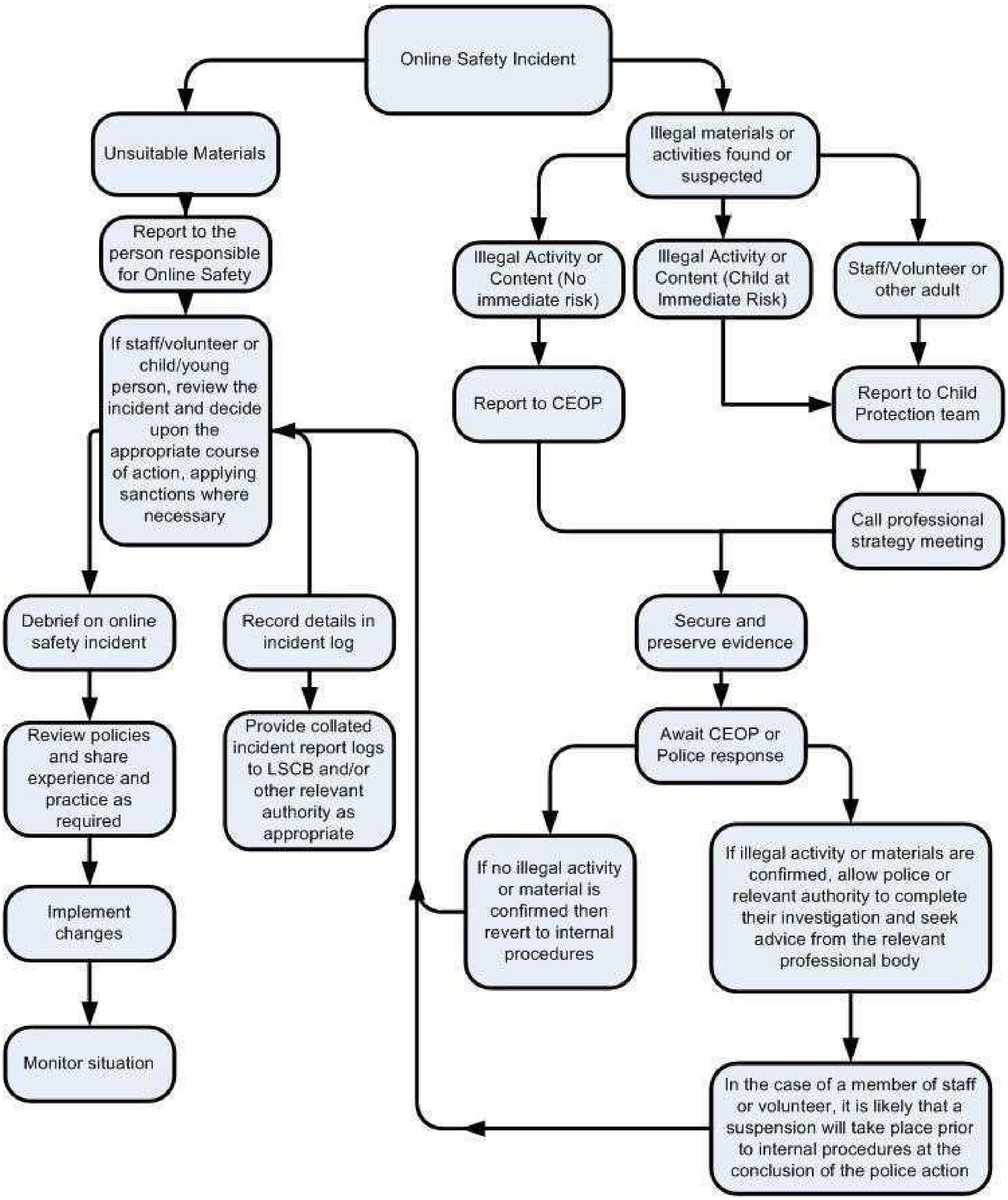
9. Data Security

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject’s rights
- Secure
- Only transferred to others with adequate protection

The Isle of Wight Education Federation has a specific policy for Data Protection which is routinely reviewed and updated by the Data and Administration Team and the Federation Governing Body. This policy is available either on request, via the Federation’s website (www.iwef.org.uk) or stored within the Shared Google Drives.

10. Flowchart for Responding to Online Safety Incidents


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

11. Internet Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the college has a filtering procedure to manage the associated risks and to provide preventative measures which are relevant to the situation in this college.

Responsibilities

The responsibility for the management of the college's internet filtering procedure will be held by the ICT Support Department. They will manage the college filtering system in line with this procedure and the Cyber Security Policy, and will keep records / logs of changes and of breaches of the filtering systems. To ensure that there is a system of checks and balances and to protect those responsible, changes to the college filtering service must:

- Be logged in change control logs
- Be authorised by a second responsible person
- Be reported to the E-Safety Committee

All users have a responsibility to report immediately to the IWEF Helpdesk any infringements of the college's filtering procedure of which they become aware or any sites that are accessed, which they believe should have been filtered. All users of the Federation's ICT System must not attempt to use any programmes or software that might allow them to bypass the filtering or security systems in place to prevent access to such materials. Further information regarding the installation or use of potentially malicious or harmful software/programs are detailed in the IWEF Cyber Security Policy.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the E-Safety education programme and the signing of the Student Acceptable Use Form. They will also be warned of the consequences of attempting to subvert the filtering system. Staff users will be made aware of the filtering systems through signing the staff user agreement form, induction training, staff meetings, briefings and Development Days. Parents will be informed of the college's filtering procedure through the Acceptable Use Agreement and through the college new starter pack.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access sites which they feel should be filtered should report this in the first instance to the ICT Support Helpdesk who will raise this with the ICT Management Team to decide whether to make changes to the college filtering system.

Students who feel that a site should be unfiltered should report this to their teacher who can assess if the site is required. If the site is required the teacher must complete a website unblock request form on the students' behalf and submit it to the Helpdesk. If necessary the Helpdesk may refer the request to the Head of Department or Headteacher.

Staff who feel that a site should be unfiltered should complete a website unblock request form and submit it to the Helpdesk. If necessary the help desk may refer the request to the Head of Department or Headteacher.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The college will therefore monitor the activities of users on the college network and on college equipment as indicated in the College E-Safety Procedure and the Acceptable Use agreement.

Audit / Reporting

Routine reports will be circulated to the Safeguarding Leads of each College site and instantaneous alerts that trigger specific topic warnings, such as abuse/self-harm/drugs, will be sent immediately. Logs of filtering change controls and of filtering incidents will be made available to:

- E-Safety Committee
- Governors Committee

The filtering procedure will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

12. Personal Data Policy

Introduction

The College and individuals within the Federation have access to a wide range of personal information and data, held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about children / young people, members of staff / volunteers and parents and carers eg. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Professional records eg. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families

It is the responsibility of all staff and volunteers to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not have permission to access that data or does not need to have access to that data. Anyone who has access to personal data must know, understand and adhere to this policy.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow “good information handling principles”.

Guidance for organisations on the DPA is available on the Information Commissioner's Office website (https://ico.org.uk/) and the Federation’s own Data Protection and GDPR policies are available on the IWEF Website and also stored within the Shared Google Drives and Staff Handbook.

Policy Statements

The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed. Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

Responsibilities

The safeguarding officer will keep up to date with current legislation and guidance and will carry out risk assessments. We aim to follow guidance from the Information Commissioner’s Office, http://www.nationalarchives.gov.uk/information---management/ , this outlines the responsibilities of other appointed staff such as Senior Information Risk Officers.

Registration

Most Colleges that hold personal data must register as a Data Controller on the Data Protection Register held by the Information Commissioner.

Staff and volunteers will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Meetings / briefings / training for staff / volunteers
- Day to day support and guidance from faculty members

Risk Assessments

Information risk assessments will be carried out by staff / volunteers to establish key areas of the group where data might be at risk and how the risk could be reduced.

Storing personal data

Personal data must be held securely on the college's allocated cloud storage platforms and only accessed by those with permission to do so. Any personal data removed from the premises/cloud storage should have the appropriate level of protection to prevent loss of data. The College has a clear policy and procedures for the automatic backing up, accessing and restoring all data held on systems, including off-site backups, all of which is outlined in the Cyber Security Policy.

The College recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests ie. a written request to see all or a part of the personal data held.

Disposal of data

The Federation will comply with the requirements for the safe destruction of personal data when it is no longer required. Such data must be destroyed, rather than deleted and be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, and other (paper based) media must be shredded, incinerated or otherwise disintegrated.

Guidance for Reviewing Internet Sites (for suspected harassment and distress)

This guidance is intended for use when schools and Colleges need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the website(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police.

Please follow all steps in this procedure:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant)
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - Incidents of 'grooming' behaviour, or
    - sending of obscene materials to a child
- Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

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 □ Permanent

□ Carisbrooke □ Medina □ VI Form Campus

□ Staff □ 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

13. 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.	

14. Reporting Log

Date	Time	Incident	Action Taken	Name/Signed

15. Monitoring Log

Date	Monitored by	Issue Identified	Reported to	Signed

16. List of Responsible Persons

E-Safety Coordinator:

Mike Peake – Carisbrooke College
Michelle Barnes – Medina College
Dave Mumford – The Island VI Form

Designated Safeguarding Lead:

Mike Peake – Carisbrooke College
Michelle Barnes – Medina College
Dave Mumford – The Island VI Form

E-Safety Governor:

Clare Caddick

ICT Technical Staff:

Mark Overy - Director of Premises and ICT
Josh Collins - Operations Manager (Systems)
Mark Arnold - Operations Manager (Facilities)

Data Protection Officer (DPO):

Vanda Niemiec – IW Council Data Protection Adviser - 01983 821000

Information Asset Owners:

Debbie Williams – Medina College, Carisbrooke College & The Island VI Form

Information Commissioner's Office:

IW Council Legal Services - 01983 821000

Local Authority Designated Officer (LADO)

Child Protection Team - Telephone: 01962 876364