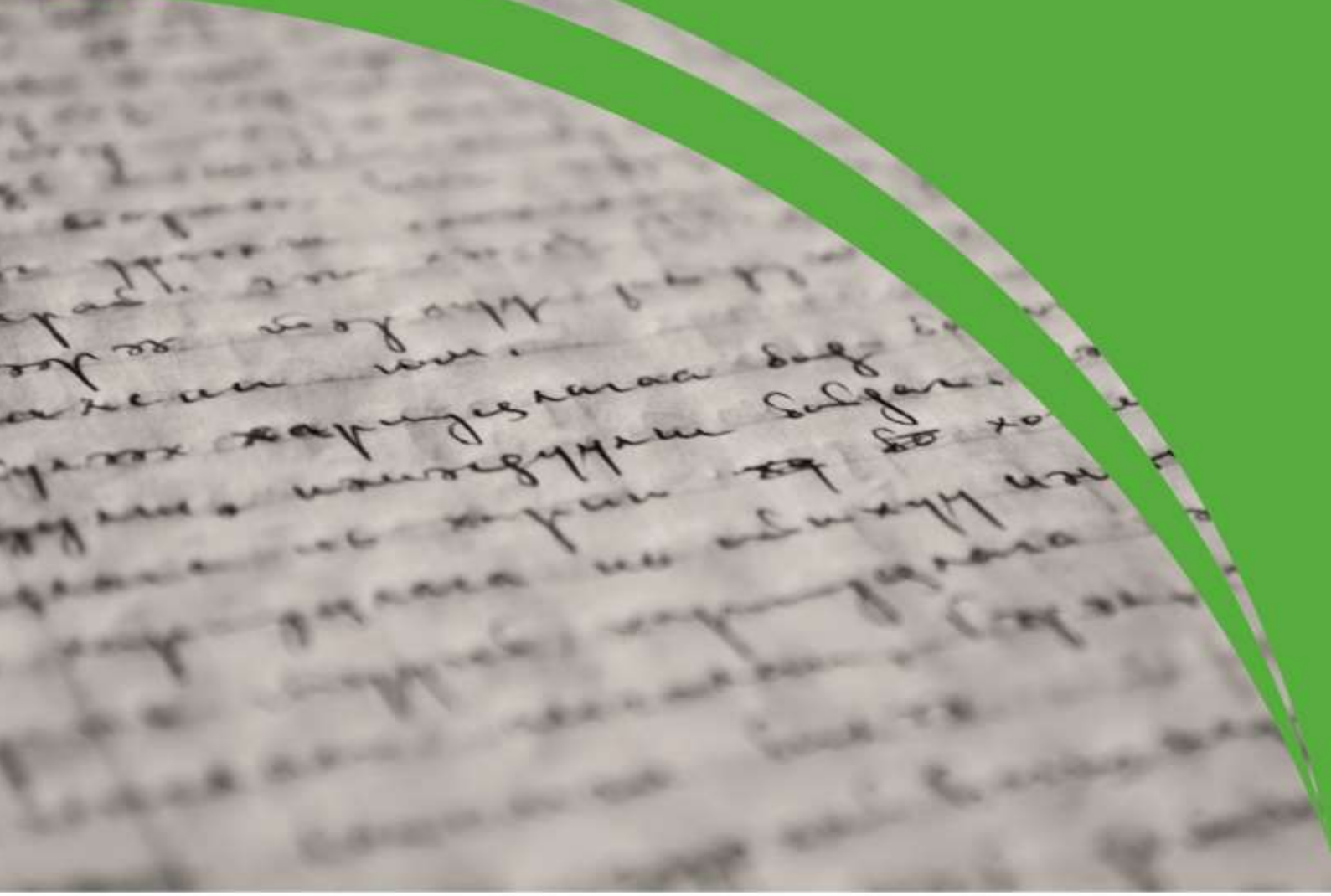


IT Misuse of ICT Policy

Key Document Details

School Name:	The White Horse Federation – all schools		
Version no:	1	Ratified date:	February 2020
Author:	M Weller	Interim review date	n/a
Owner:	M Weller	Next review date:	February 2021
Approved by:	CEO		

1. Introduction

1.1. Statement

Technology is constantly changing and will continue to do so, which means that it is of paramount importance for all service users of technology, be it pupils, teachers, staff members or another other member of the White Horse Federation, follow secure systems and process in order to maintain our safety and professional standing.

1.2. Aim and purpose

This policy outlines how allegations of ICT misuse will be handled. The term ICT includes, but is not limited to:

- Any computer, tablet or laptop
- Any device that has access, whether fixed or mobile, to chatrooms, social media, podcasts, instant message services, location tracking technologies and/or GPS.
- Wireless and broadband devices and access
- Mobile phones
- Consoles and gaming devices
- The downloading and broadcasting of music
- Streaming services
- Digital cameras
- Display devices such as whiteboards
- Printers or Photocopiers
- Software used for business or education purposes

1.3. Who it applies to

This policy applies to all staff, students, community users or anyone who has access or uses any aspect of IT within any federation establishment.

2. Policy

2.1. Description

Any allegation about the misuse of ICT must be dealt with in a prompt, fair and sensitive manner. The key priority must be to ensure the safety and well-being of children and young people at all times.

The school will deal with any incidents on an individual case by case basis, using a set of sanctions that are proportionate to any behaviours demonstrated. The school will take into account:

- The context
- The intention
- The impact of any incident before determining the response and actions to be taken

The school will allow a degree of flexibility in the application of actions e.g. a series of low level incidents would likely to be treated differentially from persistent and more serious incidents.

Media attention

If an incident attracts intense media interest and speculation, every attempt will be made to protect and support members of the school community. Statements will only be given by an authorised member of the school or organisation. All incidences will take into account the safeguarding and welfare of the children, young people and their families. Advice from the investigating body will be taken before communicating with the media.

2.2. Permissive/ non permissive

This policy must be followed.

2.3. Compliance

If any individual doesn't apply to this policy appropriate action will be taken as outlined below.

3. Key steps in the process

3.1. Roles and responsibilities

All staff are responsible for reporting incidents of misuse to the senior designated person for safeguarding at the school/setting. The designated safeguarding person for your school/setting can be found on the E-Safety and Online Safeguarding policy.

3.2. Procedures

Reporting of all incidents

The incident should be reported to the **senior designated person for safeguarding** at the school/setting. A written record should be made and the situation monitored. Alternatively, if it was felt that a conflict of interest could occur, then the member of staff must follow the "Whistle Blowing" Policy.

The context, intention and impact of any misuse must be considered in order to determine the seriousness of the misuse. If the incident relates to an inadvertent access to an inappropriate website, then the website details should be added to the filtered list. It is important that staff report any inadvertent breaches of the policy to avoid a non-reported event being escalated.

If an allegation of misuse is made against a child or young person, then parents and carers must be informed and should be advised of the actions the school takes.

The context, intention and impact of any misuse must be considered. All details should be accurately recorded with a reason for any decision noted.

If it is suspected that at any stage, a child or young person may have been, or is considered to be subject to abuse - the school <u>will</u> follow their safeguarding policy and procedures immediately.

These procedures should also be followed if an allegation of abuse is made against any employee, volunteer, manager, student or member of the school community. The school's safeguarding policies will take precedence over all others.

Reporting of serious incidents

Any serious incident must be dealt with and reported to the senior designated person for safeguarding at the school. The following incidents must always be reported to the Police, SWCPP, Children's Social Care, Local Authority Designated Officer and Ofsted.

- Discovery of indecent images of children and young people
- Behaviour considered to be grooming
- Sending of obscene materials

If not reported, then an offence may be committed. No attempt should be made to download, print or send any found as further offences could be committed by doing so.

No internal investigation or interview should be carried out in the event of any serious allegation, unless an explicit request has been made by an investigating body. The investigative bodies would be Children's Social Care, the Police and/or the Local Authority Designated Officer.

Any hardware implicated in any investigation should be secured to preserve evidence. This would include mobile phones, laptops, computers or any portable media device. In the case of potentially illegal material being found, then as far as is reasonably practicable, the equipment and materials should not be touched or switched off unless authorised by the Police. Individuals should be kept out of the immediate area. Where possible the monitor or screen should be turned off but the device left on.

Any internal disciplinary procedure should not be undertaken until any investigation by a relevant agency has been completed. Before an internal disciplinary procedure takes place, the school/setting should take advice from TWHF's Legal or Human Resources teams.

On the completion of both internal and external investigations, a review should be undertaken of policies and procedures, which would then be amended as necessary.

A report should also be made to the Internet Watch Foundation in the case of potentially illegal materials, including images of child abuse have been accessed online, giving details of the website address. If it is unclear whether the content is illegal, then the concern should be reported as a matter of caution.

4. Responding to incidents of misuse

This flowchart in Appendix 1 should be followed by any staff member when responding to a suspected incident of misuse.

It is hoped that all members of The White Horse Federation community will be responsible users of digital technologies, who understand and follow policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

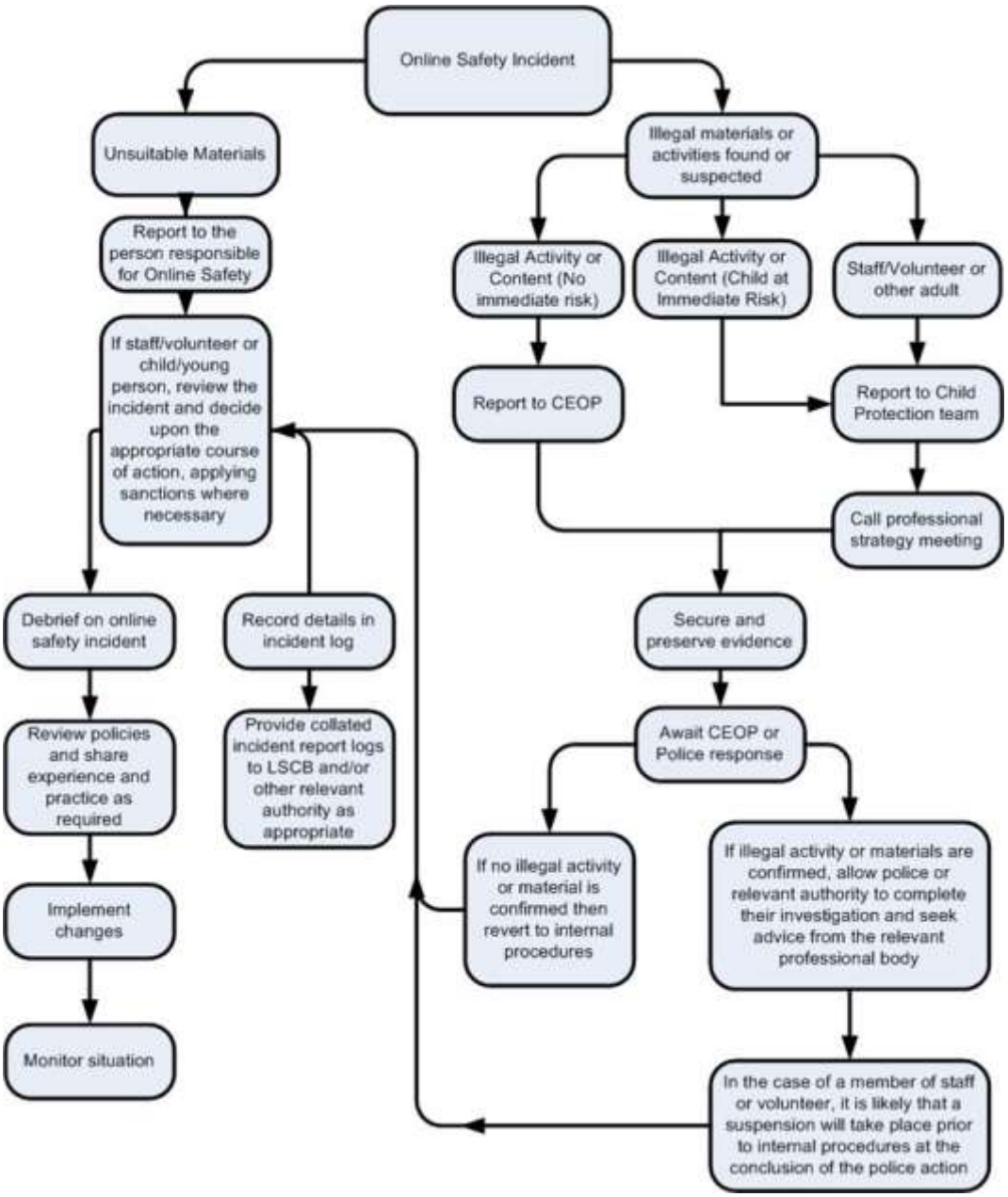
In the event of suspicion of misuse on a device, all steps in this procedure should be followed:

- Have more than one senior member of staff 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 then 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
  - 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
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials
- **Isolate the device in question as best you can. Any change to its state may hinder 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 / academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Appendix 1


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