

# Mr H Out of School Club



## Acceptable Usage/ E Safety Policy

August 2024

## **Context**

### **Development of this Policy**

Our e-Safety/Acceptable Use Policy has been written by the Club. It will be reviewed bi-annually. The e-Safety/Acceptable Use Policy relates to other policies, including Safeguarding.

### **Aims**

This policy is intended to help provide clarification on unacceptable behaviour, relating to any information and communications technology (ICT) owned by the Club, or personal technology used within the context of the Club (this includes off site visits, using Club systems at home etc).

It aims to cover all ICT including:-

- the use of computers on the Club network
- network and internet connectivity
- all mobile devices including laptops, mobile phones, desktop computers, tablets and audio/visual equipment
- all software, electronic communication and storage systems
- Our website including our Facebook page and Twitter

It applies to:-

- staff (teaching and non teaching)
- pupils
- parent helpers
- visitors
- Training students e.g. classroom assistant trainees
- Work experience students
- After Club club users

### **Teaching and Learning**

#### **Benefits of Information and Communications Technology**

- The Internet and other digital technologies are an essential element in 21st century life for education, business and social interaction. The Club has a duty to embrace such technologies and provide pupils with quality access and guidance, as part of their learning experience. Internet use will enhance learning so the Club access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Internal networks and electronic communications, portable storage devices, audio visual equipment, laptops and PCs have become an essential part of the educational environment, so the whole Club community needs to understand the appropriate and effective use of such technologies, to support teaching and learning.

#### **Risks associated with Information and Communications Technology**

There are unfortunately some risks associated with the positive educational and social benefits of using the internet and other digital technologies. Pupils will therefore be monitored closely while using the internet, by a member of teaching staff and through the local authority monitoring system.

## **Managing the Club Network and Internet Access**

### **Information systems security, filtering and monitoring.**

- Club ICT systems security will be reviewed regularly.
- The Club Manager is the e-Safety Officer, who is responsible for ensuring that the policy is implemented, updated and complied
- The e-Safety Officer will ensure that the Club community is kept up to date with e-safety issues and guidance in collaboration with the LA and Child Protection authorities.
- Security strategies will be discussed with the Local Authority.
- Virus protection will be updated regularly in conjunction with the Club technician.
- The Club will work in partnership with Newcastle LA to ensure that filtering systems are effective as possible. Esafe is also currently installed to provide monitoring and reporting of user activity. The Club will be notified if any inappropriate material is found on the Club network or portable devices. A report is sent to the Club Manager / Owner each week or immediately if an issue arises.
- The e-safety team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable and a feedback email will be sent to the Club regularly.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Officer or member of the e-safety team.
- All users must observe password protocols for network and internet access.
- Passwords should be kept secret and never shared.
- PC/laptop screens should be sited so they can be monitored by the teaching and support staff.
- The Club maintains the right to regularly monitor internet traffic, the Club's network and user email. We are obliged to monitor to fulfil our responsibilities with regard to UK law.
- All cameras and electronic devices which have pictures of our children on must be stored in the staffroom which is locked securely overnight.
- Double point access must be security must be used when logging on to Cpoms

## **Communication Systems**

### **Learning Platform and Email**

- Only approved Email accounts may be accessed on the Club network.
- Work emails should only be used for professional correspondence.

### **Managing approved Email Accounts**

- All users who log on to the learning platform and Club email system at home or at any other location, must only use these systems for educational use and those deemed reasonable by the Club Manager and are bound by the acceptable use guidelines.
- Email sent to an external organisation should be written carefully in the same way as a letter sent on Club headed paper.
- No users should ever use the Club's communication systems to access or send inappropriate materials such as pornographic, racist or offensive material or to send or forward anonymous messages and chain letters.
- Users should not access public chat rooms and messaging systems (e.g. MSN Messenger). These sites should be blocked by the filtering solution.
- Users should not use the Club's communication technologies for personal financial gain, gambling, political purposes or advertising.
- Any inappropriate communications received must be reported to the head teacher immediately.

## **Accessing Internet Sites**

- Users should not visit sites that contain illegal, obscene, hateful or other objectionable material.
- Users should use the Club's internet for professional/educational purposes only and not for personal reasons, without the permission of the e-Safety Officer.
- Teaching staff should always research potential sites before directed pupil activities.
- Staff will endeavour to use a child friendly safe search engine when accessing the web with children, supported by the filtering systems through the cache-pilot.
- You Tube may be used only after it has been checked prior by a member of staff for inappropriate contents.

## **Club Web Site**

- Staff and children contact information will not be published. The contact information given will be that of the Club office.
- The Club Manager, supported by the Club technician, will take overall editorial responsibility to ensure that content is accurate and appropriate.
- Photographs that include pupils will be carefully selected.
- The permission of parents will be sought, before photographs or work is published on the Club website.

## **Social networking, instant messaging and personal publishing**

The term 'social networking' refers to online communities where typically text, photos, music, video are shared by users. Instant messaging refers to online chatting to others in 'real time'.

- The Club will not allow users access to social networking and instant messaging sites.
- Newsgroups will be blocked unless a specific use is approved.
- The Club will have a Facebook page which will be set up and monitored by John Hymus.
- Staff will not be friends with any current parents and have their setting set at Private
- Staff must not post anything which brings the Club into disrepute

## **Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

## **Copyright and Plagiarism**

- The Club will ensure that copyright and intellectual property right laws are not infringed.

## **Managing Emerging Technologies**

The technology available to the Club is constantly evolving and the range of data and ICT services and products ever increasing. The Club will therefore:-

- Examine emerging technologies for educational benefit and a risk assessment will be carried out before use in Club is allowed.
- The staff should note that technologies such as mobile phones with wireless Internet access can bypass Club filtering systems and present a new route to undesirable material and communications.

## **Mobile Devices**

### **Taking digital images using cameras and videos**

It is recognised that the taking of digital images is an integral part of the teaching and learning experience, but there must be a clear educational reason for creating, storing, distributing and/or manipulating images of members of the Club community.

- Staff and children may take digital photographs or videos using Club equipment, providing that they support educational activities.
- Images/video should not be taken with personal mobile phone cameras or personal cameras (e.g. whilst on Club visits).
- All images of children stored on the Club computers should be placed in a folder (Staff Shared Area) with a clear explanation of the intended use of the images, not in the personal areas of staff or other users of the systems.
- Images should be stored on the external drive from laptops and PCs at the end of the academic year.

### **Mobile phones**

- Parents and other visitors to the Club will be advised to switch off mobile phones, taking calls only once they are out of the Club. This will be go on regular newsletters as a reminder.

### **Laptops and other hardware/software**

- Staff should store Club laptops in a secure location overnight.
- If Club laptops are taken home, staff are responsible for their security.
- Club laptops are for sole use of the staff member to which they are loaned.
- The Club IT technician is responsible for maintenance of Club laptops and no other person should tamper with them.
- All laptops are encrypted.

### **Portable Storage Devices**

- All users should ensure that data stored on pen drives, disks, CD Rom etc has been downloaded using antivirus software and are encrypted.
- All users are responsible for the security of mobile storage devices.
- Images of children should not be stored on pen drives.
- Pen drives should be encoded.

### **Video, DVD and Video Games e.g. Nintendo Wii and DS**

- These should be age appropriate, as outlined by the film and gaming classification authority.

### **Assessing Risks and Handling e-Safety Issues**

#### **Assessing Risks**

The Club will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the Club network. Neither the Club nor South Tyneside Council can accept liability for any material accessed, or any consequences of Internet access.

- The Club will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

### **Reporting Procedures**

#### **Reporting Accidental Access to Inappropriate Material**

Any user of the Club network who accidentally comes across inappropriate or offensive material should do the following:

1. Inform the Club's E-Safety Officer of the incident and give the website address.

2. Ask the E-Safety Officer to log the web address, time and username in the Club web log book.
3. The Club's E-Safety Officer should ring the ICT in the Club's team who will make appropriate changes to the filtering system.
5. Discuss the possibility of counselling for pupils and the need for further education on a group or Club basis.

### **Reporting Accidental Access to Illegal Material**

Any User of the Club Network who accidentally comes across illegal material should do the following:-

1. Report the incident to the E-Safety Officer or senior manager.
2. Do not show anyone the content or make public the URL.
3. Do not log off or shutdown but simply unplug the machine, quarantine and make secure.
4. Make sure a reference is made of the incident in a log-book.
5. If reporting a URL, do not use copy and paste, type the URL.
6. Report issue to LA before taking any further actions.
7. Inform Police and LA team
8. Consider the possible need for counselling/training.

### **Reporting Suspected Deliberate Abuse or Misuse**

Any person suspecting another of deliberate misuse or abuse of the regional broadband network should take the following action:

1. Report the incident to the E-Safety Officer or senior manager.
2. Do not show anyone the content or make public the URL.
3. Do not log off or shutdown but simply unplug the machine, quarantine and make secure.
4. Make sure a reference is made of the incident in a log-book.
5. If reporting a URL, do not use copy and paste, type the URL.
6. Report issue to LA before taking any further actions.
7. Consider the possible need for counselling/training.
8. Follow disciplinary procedures against staff if appropriate, in conjunction with all relevant parties, including the Local Authority, Police and Governors.

### **Examples of Inappropriate Use or Material:**

- Visiting pornographic sites (adult top shelf materials)
- Inappropriate images being viewed, not suitable for age of children
- Causing offence to religious groups
- Inappropriate use of email
- Deliberate sabotage of the network; i.e. hacking, mail bombing etc.

### **Access to Illegal Material**

If this investigation results in confirmation of access to illegal materials police will be informed and a criminal investigation may follow.

### **Examples of Illegal Acts:**

- Accessing any child abuse images.
- Incitement to racial hatred
- Incitement to violence
- Software media counterfeiting or illegitimate distribution of copied software.

## **Sanctions**

- Sanctions for the abuse or misuse of Club ICT systems will be determined by the Club Manager/e-Safety Officer and governors of the Club, as deemed appropriate.

## **Authorising Access**

### **Authorising access to the Internet and other ICT resources**

- All staff must read and sign an Acceptable Use Policy before using any Club ICT resource.
- Parents will be asked to sign and return a consent form relating internet access and the taking of digital images.
- The Club will maintain a current record of all staff and pupils who are granted access to Club ICT systems.
- Any person not directly employed by the Club will be asked to sign an acceptable use of Club ICT resources before being allowed to access the internet from the Club site.

### **Community use of the Internet**

- The Club will liaise with local organisations to establish a common approach to e-safety.

## **Communicating this Policy**

### **Staff and other adults and the e-Safety policy**

- All staff will be given the Club E-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT will work with management and the LEA to establish clear procedures for reporting issues.

SIGNATURE OF OWNER: .....

SIGNATURE OF CLUB MANAGER: \_\_\_\_\_

Date \_\_\_\_\_

**DATE OF NEXT REVIEW:     August 25**

## Appendices

### **Mr H Out of School Club for Staff and other adult users of Club ICT systems**

- I have received (have access to a central copy held with all Club policy documents) a copy of the Club's E-Safety/acceptable use policy.
- I will only use the Club's e-mail / Internet / Network / Personal e-mail for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will only log onto the Club Network / Internet using an assigned user account, set up by the Club technician by prior request and will not log on with anyone else's individual details. I will log off from my account when it is not in use to prevent access by unauthorized pupils/staff.
- I will not allow unauthorized individuals to access Email / Internet / the Network.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to inappropriate materials to a member of the e-safety team.
- I will not download any software or resources from the Internet that can compromise the network, or is not adequately licensed. Any downloads should be approved by the Club technician.
- I will ensure all documents are saved, accessed and deleted in accordance with the Club's network security and confidentiality protocols.
- I will not connect a computer or laptop to the network / Internet that does not have up-to-date version of anti-virus software.
- I will not use personal digital cameras.
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.
- I will not have in my possession at anytime in the Club a mobile phone. Mobile phones MUST be kept in the staffroom or with the secretary in the event of an emergency
- I understand that all Internet usage will be logged and this information could be made available to my Head Teacher on request.
- I understand that I must not be Friends with any current parents
- I understand that all social media should be set to private
- I understand that if I put inappropriate or illegal content on my social media it may have the consequence of disciplinary. This include photos which are seen as lewd and written content which brings the reputation of the Club down

- I agree and accept that any computer or laptop loaned to me by the Club, is provided solely to support my professional responsibilities and that I will notify the Club of any “significant personal use” as defined by HM Revenue & Customs.
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.

Signed \_\_\_\_\_

Date \_\_\_\_\_