



Chiltern Way Academy

Turning Futures Around

ICT Acceptable Use Policy

Responsibility for this policy (job title): Director of Schools

Responsibility for its review: CEO

Approved: 13/06/2019

Next Review Date: Summer 2020

CONTENTS

Developing safe school websites	3
Use of still and moving images	3
Procedures	4
Technical	4
Education	5
CWA Statement	5
Social networking and personal publishing	6
CWA Statement	6

General

Use of digital and video images in school websites

Developing safe school web sites

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety. A senior member of staff needs to oversee / authorise the website's content and check suitability. It should be clear who has authority to upload content into sections of the website. This is also true if images/videos of students are uploaded to third party websites.

Use of still and moving images

Most importantly, take care when using photographs or video footage of students on the school website. Consider using group photographs rather than photos of individual children. Preferably use photos that do not clearly identify students. Do not use the first name and last name of individuals in a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the school. An easy rule to remember is:

- **If the student is named, avoid using their photograph / video footage.**
- **If a photograph /video is used, avoid naming the student.**

If the school website is using a webcam – then this must be checked and monitored to ensure misuse does not occur accidentally or otherwise.

If showcasing school-made digital video work, take care to ensure that students aren't referred to by name on the video, and that students' full names aren't given in credits at the end of the film

If showcasing examples of students work consider using only their first names, rather than their full names.

Only use images of students in suitable dress to reduce the risk of inappropriate use.

In many cases, it is unlikely that the Data Protection Act will apply to the taking of images e.g. photographs taken for personal use, such as those taken by parents or grandparents at a school play or sports day. However, photographs taken for official school use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, staff and students should be advised why they are being taken.

Parental permission should be obtained before publishing any photographs, video footage etc of students on the school website, in a DVD or in any other high profile public printed media. This ensures that parents are aware of the way the image of their child is representing the school; a printed copy of the specific image should be attached to this form. A Parental Permission Form is an appropriate way of achieving this.

Procedures:

Use excerpts of students' work such as from written work, scanned images of artwork or photographs of items designed and made in technology lessons. This allows students to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of students.

Links to any external websites should be thoroughly checked before inclusion on a school website to ensure that the content is appropriate both to the school and for the intended audience. Remember that the content of websites can change substantially, even in a short space of time. Check all links regularly, not only to ensure that they are still active, but that the content remains suitable too.

Text written by students should always be reviewed before publishing it on the school website. Make sure that the work does not include the full name of the student, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them. Although it may seem obvious, check that students' work does not contain any statements that could be deemed defamatory.

Ensure also that the school is not infringing copyright or intellectual property rights through any content published on the website. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought.

If a school's website contains any guestbook, noticeboard or blog, they need to be monitored to ensure they do not contain personal details of staff or students.

If the school website is using a webcam – then this must be checked and monitored to ensure misuse does not occur accidentally or otherwise.

If showcasing school-made digital video work, take care to ensure that students aren't referred to by name on the video, and that students' full names aren't given in credits at the end of the film.

Digital images - photographs and video clips - can now readily be taken using mobile phones. Extreme abuse is the so called 'happy slapping' incidents sent to others or posted onto a website, e.g. a recent case of a posting on [YouTube](#). It is therefore important to ensure that the risk of inappropriate use is minimised. Are camera/video phones allowed in the school? How is this monitored and enforced? Staff should be advised not to use their personal phone or camera without permission e.g. for a school field trip. If personal equipment is being used it should be registered with the school and a clear undertaking that photographs will be transferred to the school network and will not be stored at home or on memory sticks and used for any other purpose than school approved business.

Technical:

Digital images / video of students need to be stored securely on the school network. Old images are kept no longer than is necessary for the purposes for which they were processed.

When saving pictures, ensure that the image file is appropriately named. Do not use students' names in image file names or in <ALT> tag references when published on the web.

[An ALT tag is the HTML text describing a displayed image, used mostly for reasons of accessibility, since the tag can be voiced by screen readers]

Many schools are now using video as part of their Visual Literacy work. It is important that staff do not use software to 'rip-out' sections of copyrighted movies without permission.

Education:

Ensure staff and students know who to report any inappropriate use of images to and understand the importance of safe practice. Staff and students also need to understand how to consider an external 'audience' when publishing or presenting work.

Chiltern Way Academy Policy statement:

In this Academy:

- The CEO takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to ICT technicians and those the CEO delegates to;
- The school web site complies with the school's guidelines for publications;
- 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;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- Digital images /video of students are stored in the Academy's shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- We do not use students' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not include the full names of students in the credits of any published school produced video materials / DVDs;
- Staff automatically agree to the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of students;
- Students are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Students are taught about how images can be abused in their e-Safety education programme;

General

Social networking and personal publishing

Parents and staff need to be aware that the Internet has online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Students should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.

Examples include: blogs, wikis, Facebook, Snapchat, Instagram, WhatsApp, twitter, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

Chiltern Way Academy Policy statement:

- The schools will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Students should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Staff official blogs or wikis should be password protected and run from the school website. Staff should be advised not to run social network spaces for student use on a personal basis.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.