

ONLINE SAFETY- INC. USE OF MEDIA POLICY

ADO Services C.I.C

Incorporating ADO River Valley

Version 3.2 ©2023

Current Version Valid from 1st February 2023

Next Scheduled Review February 2024

Reviewed by the ADO Management Committee March 2023

2023-2024

1. Online Safety and Use of Media Policy Overview

It is the policy of ADO to address the Online Safety and the taking of photographic images or video for media purposes at their sites. Every student in our care deserves to be protected from the misuse of the online dangers or photographic and video images of themselves, whilst they attend school. The internet forms an integral part of learning within programmes and to ensure ADO conform to the minimum requirements we use the Department of Education's, '**Teaching Online Safety**' as a guidance. This policy focuses on the impact of online and media access by the student.

This policy is closely linked to the **Privacy Policy** and the **Mobile Phone and Smart Device Policy**.

2. Types of Devices and Scope

The types and devices and their scope of use is covered in detail within the **Mobile Phone and Smart Device Policy**. This document is regularly updated as and when new technologies pose a change in policy or require a new set of procedures when in use. A full technical specification of internal systems, email and data storage can be found within the **Privacy Policy**.

3. Internet & Internal Networks Overview.

ADO has installed standard broadband services but with their own, not supplier proprietary, ADSL routers. This allows us to add additional levels of controls to accessing our main data network attached storage systems. Our two main sites are connected via a secure VPN connection. Each user (staff member) has their own unique username and password. Each site has its own internet connection, monitored centrally. Our outdoor site has clear line of sight boosters, all individually secured with their own passwords. Internal data is stored and accessed through an additional password layer and access rights are user restricted dependent on the authorisation levels within the company. All systems are protected by both anti-virus and malware software.

For this moment in time, the current technology and the size of our operation, these network controls provide ADO with all the security we require. As the company grows and new systems are implemented, the policies and procedures will be updated accordingly.

3.1 Student Access

Students who require ADO devices or computers to access the internet do not have their own individual usernames and passwords. Instead, they are given generic usernames and passwords with the basic access to either software programmes, installed Apps or restricted internet access. Staff are not allowed to let students use their own username and passwords. Students do not have any access to ADO email or filesystems. Students are only allowed to use their own devices under agreements as noted below in 3.2.

Students are allowed the wireless network password for our outdoor site, but not for the main head office.

3.2 Student Agreements

Each student is restricted by the policies as set out in the **Mobile Phone and Smart Device Policy**. If they want to bring to site their mobile phone or smart device, they must, in addition, be prepared to sign **The Mobile Phone & Smart Device Agreement Form**. There are strict regulations set out in the aforementioned policy and although we expect a level of trust if they are learning online, there are also many safeguards to stop them gaining access to any ADO internal networks or data. In fact, the access they are allowed is quite often restricted to Apps rather than carte blanche internet access.

4. Media Arrangements

Media plays an important part in recording service users progress and achievements. ADO complies with the GDPR guidelines on all data that is kept on ADO networks. A complete guide to this and our compliance can be found in our **Privacy Policy**.

4.1 Photographic Images and Purpose

These are taken solely for the purpose of ADO or our students with full permission. We never share images with third party or partner organisations, except in exceptional circumstances and only when agreed with all parties involved. It is our policy to only use photographic images or video taken to support, but not limiting to;

- The visibility of ADO as a brand
- Marketing purposes
- Media presence
- Highlight good work in the community.

In addition, our students and stakeholders benefit from images for the purposes of record keeping as part of OFSTED regulations, or supportive evidence for learning. Images may be taken and stored on secure software and company devices for any one of these reasons;

- For the benefit of parent-carers to view their children or young person (CYPs) progress.
- Support the learning of each CYP individual record.
- To highlight our students' activities and experiences.
- A record of outcomes, or any other recorded analysis that are agreed to.
- Supportive and evidence-based learning records for qualifications
- Supportive and evidence-based learning records for authorities

These images or videos are then subject to Release Management to ensure that full permissions are given before publishing. The Office Administration team hold a record of those students with agreed permissions to publish.

4.2 Image Use Permissions

All students will at some point agree to terms, or contractual agreements with the choice of allowing photographs or video to be used or refuse permission accordingly.

Permission for standard photographic images or video is obtained in a number of ways via Online Referral Forms, as part of the 'New Starter Process' or through paper records. Parent-carers can advise at this stage that they do not provide permission for any photographic images or video to be used for marketing or social media purposes, for example, which forms part of our data protection policy ongoing.

For ADO River Valley, the default stance on permission to use images is set to prohibited. This is to say that no images will be used of children and young people by default unless express permission is gained from the parent-carers or authorities and for reasons of special conditions or for supportive-educational circumstances.

In the case of the ADO staff team or outside agencies taking photographs for promotional and marketing purposes at outside one –off trips, the company will seek written, parental-carer-organisation permission to agree for students to be included at the time. Should a Parent-Carer prefer their CYP not to take part, then any images taken will be deleted within 24 hours. Individual CYP will not be included in a group image if written permission is not given by the CYPs designated guardian.

4.3 Storage and Security of Images

The Staff team operate ADO controlled smart devices capable of taking photographic images or video. These are locked away when not in use within the company demise in an offline position. Images are taken using official company equipment only. Once a month all images or video on these devices is removed and backed-up on the ADO data network. The devices are then returned cleaned of old images.

4.4 Security Images and Purpose

There is no CCTV security system currently installed on any sites. If CCTV is ever installed, this policy will be updated accordingly.

4.5 Retractions

If a Parent-Carer-organisation would like to retract their permission for the use of images or video, they should do so in writing to the main office, details to be found in the General Terms and Conditions of ADO.

5. Secure Image Capture and Storage

ADO uses **Arbor** software for its record keeping imagery for the River Valley School Parent-carers can view the images remotely but are unable to then copy them or download them for distribution.

Arbor software is secure from third party distribution of images or abuse of duplication. It is cloud based, therefore not on the ADO network.

6. Review

All ADO policies and procedures follow ITIL guidelines to ensure version control, change control and release management of any documents. As a matter of policy, documents can be updated at any time to reflect changes to ADO procedures, legal changes, OFSTED directives or any other reason to ensure the policies and procedures are accurate and correct. This involves consultation with stakeholders and approval from the directors and the ADO Management Committee. All policies and procedures are reviewed at the very least on an annual basis. Regular communication through newsletters, social media, text systems and through our website within the ADO Library is part of our Release Management.

7. Contact

This document was produced by the ADO Operations Consultancy Team. This version supersedes any previous versions and will be reviewed annually.

All correspondence with regard to this policy, or any other operational policy and procedure should be directed to the ADO Business Operations and Support Executive by e-mailing gmp@adoservices.co.uk or calling 0208 855 6778, requesting to speak to Gary McHolland-Pilcher or in writing, ADO Services CIC, Head Office, 126 Upper Wickham Lane, Welling, Kent, DA16 3DP.