PHOTOGRAPHIC POLICIES

NEU Guidance for Members, Reps and Local Officers

Introduction

It is common for school employers to have photographic policies in order to comply with:

- ***The Data Protection Act 2018;***
- ***The General Data Protection Regulations; and***
- ***Child Protection legislation and regulations.***

The Information Commissioner, who is responsible for compliance with data protection legislation, has published advice on taking photographs in schools and colleges, and the advice set out in this briefing is drawn from that, together with guidance from the DfE and the Welsh Government.

This briefing sets out:

- ***the legal obligations upon schools and colleges;***
- ***the role of head teachers;***
- ***the implications for staff.***

PHOTOGRAPHS IN SCHOOLS

Photographic policies will usually cover some or all the following:

- individual or group portraits for parents/carers;
- publicity photographs produced by the school for handbooks/websites;
- parents/carers recording school events i.e. sports' day;
- press/media photography;
- the use of CCTV cameras.

Relevant guidance on each is set out below.

What is personal data?

The General Data Protection Regulations define personal data as any information which are related to an identified or identifiable natural person (i.e. a human being). Personal data is caught by data protection legislation if it is processed wholly or partly by automated means, or forms part of a relevant filing system. Furthermore, Section 68 of the Freedom of Information Act extends the definition of data to include "recorded information held by a public authority" which includes all data held and processed *manually* even if it does not form part of a relevant filing system.

Individual/group pupil photographs

Schools and colleges should use professional photographers to take individual/group pupil photographs. This will ensure compliance with the data protection legislation and that:

- material is used only for the school's/college's own purposes;
- photographs are not used for any other purpose without seeking the data subject's consent first;
- the photographer does not share the photographs with any other party unless specifically required to do so under the contract with the school/college or where written permission has been given by the school/college;
- the photographer/agency retains evidence that they have followed the steps set out above.

Some schools/colleges make use of individual student portraits for security purposes, for example storing electronic images with other personal data. Images stored in this way fall within the definition of personal data and school/college management must therefore ensure that:

- parents/carers/guardians of students are informed that images are to be retained by the school/college; and
- images will be securely stored and only used by those authorised to do so.

Publicity photographs produced by the schools/colleges for handbooks and/or websites

The Information Commissioner's Good Practice note on 'taking photographs in schools' provides the following example:

> *'A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the Act as long as the children and/or their guardians are aware this is happening and of the context in which the photo will be used.'*

The DfE is not prescriptive on this point although they do advise (contrary to the Information Commissioner's guidance) as follows:

> *'Schools and local authorities are free to decide on their own policies relating to the use of such images or the release of associated information for their own publicity purposes. We do, however, advise that the photographs and video images of pupils and staff are classed as personal data……'*

The Union supports the DfE guidance and would expect schools/colleges to draw up their own policies on photography.

The NEU advises that if schools/colleges use images of students or staff in publicity material, such as school/college prospectuses, handbooks and websites, consent must be given by the individuals concerned or, in the case of pupils under the age of sixteen, by their

parents/carers/guardians. Pupils/students must be advised of the purpose for which the photos are being taken.

If the images are to be retained for further use, the individual or legal guardian concerned must be informed and assured that the images are securely stored and only used by those authorised to do so.

The NEU view is that where photographs of students are used in school publications, including the website, **the students should not be named**. Conversely, if a student's name appears, the student's image should not.

There may be some circumstances where it would be appropriate for the school/college to publicise a student's name with a photograph, for example, Head Girls and Head Boys, but the parents must be asked for their permission before such information is publicised if the student is not old enough to give consent on their own behalf. For the purposes of compliance with the DPA, a `fair processing' notice should be issued by the school/college setting out:

- the identity of the data controller (usually the governing body);
- the purpose or purposes for which the photographs are intended to be processed;
- any other organisations to which the photographs may be distributed; and
- when the photographs are likely to be destroyed.

A school/college may decide to do this when a student first starts at the school/college or on an annual basis.

Parents/carers photographing school events

The Information Commissioner's guidance gives the following example and advice:

> *'A parent takes a photo of their child and some friends taking part in the school sports day. These images are for personal use and the Data Protection Act does not apply.*
>
> *Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply.'*

The DfE advises that schools and local authorities are free to develop and implement their own policies regarding the use of cameras and videos by parent/carers at school events. This would include a parent member of the PTA who videos an event and then sells copies to parents who may not have such recording equipment or school staff wanting to record events involving their students or their form group. Such material may not be for school publication use, but might be used later in the classroom, e.g. video, photos/slides/PowerPoint presentation of a geography field trip, history site study. As long as parents are notified of the purposes for which the photographs or images will be used there will be no conflict with data protection legislation.

Although data protection is not applicable here, there are two other considerations; practicalities and child protection issues.

The NEU advises that some or all the following suggestions could be incorporated into schools' policies on parents/carers photographing school events:

- Include in the schools' admission form, a section for parents/carers to sign to indicate that any images they take of school activities will not be used inappropriately;

- Include in letters inviting parents to school events a returnable slip for parents to sign indicating that any photographs taken will not be used inappropriately;

- Give written confirmation that photography only takes place in designated areas, for example during sports days on the sports fields;

- Where schools create their own photographic record of events, such arrangements should be announced in the letter inviting parents to the event.

Media Photography

The Information Commissioner's Good Practice note provides the following example:

> *'A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act.'*

If local newspapers sell such images the school is not the data controller and cannot be held responsible for the actions of the press.

The concerns here are likely to fall within the area of child protection. If press photographers do record school events, any published photographs should not identify individual students by name.

CCTV

Increasingly, schools/colleges are introducing CCTV cameras for the purposes of security and to address concerns about student behaviour. The NEU has reservations about the introduction of CCTV cameras and the balance between surveillance of students and potential overt or covert surveillance of staff, must be paramount.

If a school/college is considering the introduction of a CCTV system, certain requirements under data protection and human rights legislation must be complied with both before the installation of the system and once it is up and running. The key requirements to ensure compliance are listed in Appendix One.

Action points for Safety Reps

In order to preclude covert surveillance of staff, the following safeguards should be sought by NEU health and safety representatives at school level (or health and safety advisers at LA level) before CCTV systems are installed:

- that the purpose of the CCTV system is school security and/or monitoring pupils' behaviour;
- that data storage conforms to the requirements of the Data Protection Act;
- that the process for disclosing data about individuals is transparent and available to all staff;
- that the operation and maintenance of the system is subject to regular reviews which are made available to Safety Reps (or Health and Safety Advisers);

CCTV can be a useful resource for schools/colleges provided there are requisite safeguards.

CCTV cameras should be positioned outside classrooms/lecture theatres/computer suites which will ensure that there is no potential for misuse, i.e. covert surveillance of staff. The Information

Commissioner advises that 'continuous videoing of particular individuals is only likely to be justified in rare circumstances.'

If management in a school/college do not consider that siting a camera outside a classroom/suite will be sufficient to prevent theft or vandalism, the health and safety representative/adviser should seek written assurances that the CCTV will only be activated when the room is not being used for teaching and that any footage will not be used for staff disciplinaries or for performance management.

There are circumstances where covert monitoring may be lawful. Regional/Wales office advice should always be sought in these cases.

IRIS Connect

The IRIS Connect system essentially enables trainees and experienced teachers alike to video and audio record their lessons. After a recording has taken place, the video is uploaded directly to the individual's personal password protected account in the IRIS Connect online platform where they may watch it back for their own personal reflection or share with a colleague for feedback.

The providers of IRIS Connect purport that each video recorded will be stored in the individual's personal library and that no-one can access any video located in another user's personal library without permission. Furthermore, access to a user's personal library may be revoked at any time, and the person with whom videos are shared will not be able to share them with anyone else.

It is also possible to receive 'in-ear coaching' with IRIS Connect, where the lesson is viewed remotely by a coach who communicates privately with the teacher using a 'LiveView camera' and a discreet wireless earpiece.

AV1 Robots in the classroom

AV1 robots are used increasingly in classrooms to support the education of children and young adults who are unable to attend class in person. This may be because they have long-term or chronic illnesses. AV1 robots incorporate visual and audio systems to enable students to see, hear and talk to classmates remotely.

Safety features

The equipment does not record video/sound – it only streams it live to the viewer. However, members may rightly be concerned of the possibility that it could be recorded on other equipment e.g. a mobile phone, and then uploaded unto social media. Parents and students are usually asked to sign some sort of agreement not to misuse the robot, but this requires the teacher whose sessions will be viewed to depend only on the trustworthiness of those involved.

Is speech and appearance 'personal data?

Yes, it is. It is 'special category data' if it can identify a person's race and/or ethnic origin. Special category data is personal data which the GDPR says is more sensitive and so needs more protection. In order to lawfully process special category data, a school or college must identify both the lawful basis for processing it under Article 6, and a separate condition for processing special category data under Article 9.

Is 'livestreaming' images and sounds processing?

When a camera is being used to film people this entails processing of their personal data. It does not matter that AV1 robot is live streaming and not recording.

What is the NEU's position on the use of AV1 robots and IRIS Connect in classrooms?

The NEU does not believe the use of innovative technology in schools is intrinsically good or bad. We do, however, stress the importance of informed consent and the need for schools to engage in consultation with parents, students and school/college staff before introducing potentially intrusive technology of this kind. If students and staff wish to opt out of having their image and speech captured by these devices, they should be able to do so.

The NEU's redlines on the use of AV1 robots and IRIS Connect

- The equipment must not be introduced to the school/college in the absence of consultation with pupils, parents and staff;
- The equipment should remain under the control of the individual teacher at all stages and in all circumstances;
- Staff with responsibility for the equipment must receive appropriate training, including training on the data protection and human rights obligations of the school/college governing body to pupils/students and to staff;
- Permission to share video and audio footage with peers and other third parties must first be sought from the teacher whose lessons are being recorded and from parents/students of pupils/students who appear in the recording;
- Neither system should be used for surveillance;
- Teachers should not be directed to use the technology. Its use must be voluntary;
- Students who do not want their image to be captured by the equipment should have the option to opt out of lessons where video footage of the entire class will or may be captured.

ID badges for staff

Some schools have introduced identity badges for staff as part of school security policies.

To amount to 'fair processing', the introduction of identity badges must be a proportionate response to the security needs of the school/college and the safety of staff and students. This may well be a proportionate response where the school/college has experienced breaches of security in the past or where a risk assessment has identified weaknesses in school security. Staff should be consulted fully about the introduction of name badges.

The legal framework

There are four pieces of legislation/regulation relevant to CCTV/monitoring equipment in the workplace.

These are:

- The Data Protection Act 2018
- The General Data Protection Regulations

- The Human Rights Act 1998

- The Regulation of Investigatory Powers Act 2000 (as amended) (and accompanying regulations)

There are two relevant Codes of Practice published by the Information Commissioner; CCTV and Monitoring at Work (Part 3 of the Employment Practices Data Protection Code).

The Human Rights Act 1998
(came into force in October 2000)

The Act incorporates into UK law the provisions of the European Convention of the Protection of Human Rights and Fundamental Freedoms.

The section of the Convention which is relevant to workplace privacy is article 8(1):

> *'Everyone has the right to respect for his private and family life, his home and his correspondence'.*

Data protection

Persons or institutions processing personal data must comply with a number of data protection principles.

Personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept longer than necessary;
- Processed in accordance with the data subject's rights (the right to access and to prevent processing);
- Secure (who can access the data as well as protection against loss, damage or destruction); and
- Not transferred to countries outside the European Economic Area.

The **Code of Practice: CCTV** (available from www.ico.gov.uk) sets out the following **standards** which must be met by users installing and using CCTV systems:

A. Initial Assessment Procedure;
B. Siting the Cameras;
C. Quality of the Images;
D. Processing the Images;
E. Access and Disclosure of Images to Third Parties;
F. Access by Data Subjects; and
G. Monitoring Compliance with this Code of Practice.

The standards are set out in full at Appendix One. See also the 2012 ICO report referred to in 'Further Information and Related Guidance' below, which includes a section summarising CCTV considerations.

Further Information and Related Guidance

The NEU Health and Safety briefing 'Mobile Phone Photography' is available on the NEU website at www.neu.org.uk.

The NEU Health and Safety briefing 'Security and Violence' is available on the NEU website at www.neu.org.uk.

The Information Commissioners website, which includes the Code of Practice on Photography in Schools as well as other information on data protection is to be found at https://ico.org.uk/

The ICO's report on data protection guidance given to schools in 2012 (as amended), which includes advice on CCTV, photographs and websites, can be downloaded from https://ico.org.uk/media/for-organisations/documents/1132/report_dp_guidance_for_schools.pdf

Kent County Council's 'The use of cameras and images within educational settings'

The website for the Welsh Assembly Government is: https://gov.wales/

August 2019

APPENDIX ONE

Summary of the Information Commissioner's Code of Practice on CCTV Systems

A. Initial Assessment Procedure

1. Users will need to establish the purpose or purposes for which they intend to use the equipment.

2. Establish who is the person or organisation legally responsible for the proposed scheme and who is responsive for the day to day compliance.

3. Assess the appropriateness of, and reasons for, using CCTV or similar surveillance equipment (First Data Protection Principle).

4. Document this assessment process and the reasons for the installation of the scheme.

5. Ensure that the notification lodged with the Information Commissioner's Office covers the purposes for which this equipment is used.

6. Establish and document security and disclosure policies.

B. Siting the Cameras

1. The equipment should be sited in such a way that it only monitors those spaces which are intended to be covered by the equipment.

2. Operators must be aware of the purpose(s) for which the scheme has been established.

3. Operators must be aware that they are only able to use the equipment in order to achieve the purpose(s) for which it has been installed.

4. Signs should be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment.

5. The size of signs will vary according to circumstances:

   For example *– a sign on the entrance door to a building society office may only need to be A4 size because it is at eye level of those entering the premises.*

   For example *– signs at the entrances of car parks alerting drivers to the fact that the car park is covered by such equipment will usually need to be large, for example, probably A3 size as they are likely to be viewed from further away, for example by a driver sitting in a car.*

6. The signs should contain the following information:

   a) Identity of the person or organisation responsible for the scheme.
   b) The purposes of the scheme.
   c) Details of whom to contact regarding the scheme.

C. Quality of the Images

1. If tapes are used, it should be ensured that they are good quality tapes.

2. The medium on which the images are captured should be cleaned so that the images are not recorded on top of images recorded previously.

3. A maintenance log should be kept.

4. If a camera is damaged, there should be clear procedures for:

    a) Defining the person responsible for making arrangements for ensuring that the camera is fixed
    b) Monitoring the quality of the maintenance work.

D. Processing the Images

1. Images should not be retained for longer than is necessary.

2. Once the retention period has expired, the images should be removed or erased.

3. If the images are retained for evidential purposes, they should be retained in a secure place to which access is controlled.

4. On removing the medium on which the images have been recorded for the use in legal proceedings, the operator should ensure that they have documented:

    a) The date on which the images were removed from the general system for use in legal
    proceedings.
    b) The reason why they were removed from the system.
    c) Any crime incident number to which the images may be relevant.
    d) The location of the images.
    e) The signature of the collecting police officer, where appropriate (see below).

5. All operators and employees with access to images should be aware of the procedure which needs to be followed when accessing the recorded images.

6. All operators should be trained in their responsibilities under this Code of Practice i.e. they should be aware of:

    a) The user's security policy e.g. procedures to have access to recorded images.
    b) The user's disclosure policy.
    c) Rights of individuals in relation to their recorded images.

E. Access to and Disclosure of Images to Third Parties

All employees should be aware of the restrictions set out in this code of practice in relation to access to, and disclosure of, recorded images.

1. Access to recorded images should be restricted to those staff who need to have access in order to achieve the purpose(s) of using the equipment.

2. All access to the medium on which the images are recorded should be documented.

3. Disclosure of the recorded images to third parties should only be made in limited and prescribed circumstances.

4. All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented.

5. If access to or disclosure of the images is allowed, then the following should be documented:

    a) The date and time at which access was allowed or the date on which disclosure was made.
    b) The identification of any third party who was allowed access or to whom disclosure was made.
    c) The reason for allowing access or disclosure.
    d) The extent of the information to which access was allowed or which was disclosed.

F. Access by Data Subjects

1. All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects.

2. *Data subjects should be provided with a standard subject access request form which:*

    a) Indicates the information required in order to locate the images requested.
    b) Indicates the information required in order to identify the person making the request.

3. *All subject access requests should be dealt with by a manager or designated member of staff.*

4. *The manager or designated member of staff should locate the images requested.*

5. If the manager or designated member of staff decides that a subject access request from an individual is not to be complied with, the following should be documented:

    a) The identity of the individual making the request
    b) The date of the request
    c) The reason for refusing to supply the images requested
    d) The name and signature of the manager or designated member of staff making the decision.

6. All staff should be aware of individuals' rights under this section of the Code of Practice.

G. Monitoring Compliance with this Code of Practice

1. The contact point indicated on the sign should be available to members of the public during office hours. Employees staffing that contact point should be aware of the policies and procedures governing the use of this equipment.

2. *Enquiries should be provided on request with one or more of the following:*

    a) The leaflet which individuals receive when they make a subject access request as general information
    b) A copy of this Code of Practice
    c) A subject access request form if required or requested

d) The complaints procedure to be followed if they have concerns about the use of the system

e) The complaints procedure to be followed if they have concerns about non-compliance with the provisions of this Code of Practice

- *A complaints procedure should be clearly documented.*
- *A record of the number and nature of complaints or enquiries received should be maintained together with an outline of the action taken.*
- *A report on those numbers should be collected by the manager or designated member of staff in order to assess public reaction to and opinion of the use of the system.*

3. *A report on those reviews should be provided to the data controller(s) in order that compliance with legal obligations and provisions of this Code of Practice can be monitored.*

4. *An internal annual assessment should be undertaken which evaluates the effectiveness of the system.*

5. *The results of the report should be assessed against the stated purpose of the scheme. If the scheme is not achieving its purpose, it should be discontinued or modified.*

The result of those reports should be made publicly available.